SEC – February 2016 Consultation (showing changes in mark-up from last published version of the relevant section)

Dated: 23 September 2013

Smart Energy Code

[Note: This document is a consolidated consultation version of the SEC for February 2016 with the section 88 changes being consulted upon shown in mark-up.]

CONTENTS

SMART ENERGY CODE CONTENTS

		Page No.
Introduction		1
Section A:	**Definitions and Interpretation**	
A1	Definitions	2
A2	Interpretation	104
Section B:	**Accession**	
B1	Accession	107
B2	DCC User and RDP Identifiers	111
Section C:	**Governance**	
C1	SEC Objectives	114
C2	Panel	118
C3	Panel Members	122
C4	Elected Members	127
C5	Proceedings of the Panel	132
C6	Sub-Committees	137
C7	Code Administrator, Secretariat and SECCo	140
C8	Panel Costs and Budgets	144
Section D:	**Modification Process**	
D1	Raising Modification Proposals	150
D2	Modification Paths	155
D3	Initial Consideration of Modification Proposals	157
D4	Authority Determinations	162
D5	Withdrawal by Proposer	165
D6	Refinement Process	166
D7	Report Phase	172
D8	Change Board and Change Board Decision	176
D9	Modification Proposal Decision	183

D10 Implementation 186

Section E: Registration Data

E1 Reliance on Registration Data 188
E2 Provision of Data 190
E3 DCC Gateway Connections for Registration Data Providers 197

Section F: Smart Metering System Requirements

F1 Technical Sub-Committee 200
F2 Certified Products List 203
F3 Panel Dispute Resolution Role 206
F4 Operational Functionality, Interoperability and Access for the DCC 208
F5 Communications Hub Forecasts & Orders 211
F6 Delivery and Acceptance of Communications Hubs 219
F7 Installation and Maintenance of Communications Hubs 223
F8 Removal and Return of Communications Hubs 231
F9 Categories of Communications Hubs Responsibility 236
F10 Test Communications Hubs 243

Section G: Security

G1 Security: General Provisions 247
G2 System Security: Obligations on the DCC 250
G3 System Security: Obligations on Users 262
G4 Organisational Security: Obligations on Users and the DCC 269
G5 Information Security: Obligations on the DCC and Users 272
G6 Anomaly Detection Thresholds: Obligations on the DCC and Users 282
G7 Security Sub-Committee 286
G8 User Security Assurance 296
G9 DCC Security Assurance 315

Section H: DCC Services

H1 User Entry Process 321
H2 Registered Supplier Agents 326
H3 DCC User Interface 328
H4 Processing Service Requests 338

H5	Smart Metering Inventory and Enrolment Services	340
H6	Decommissioning, Withdrawal and Suspension of Devices	342
H7	Elective Communication Services	345
H8	Service Management, Self-Service Interface and Service Desk	351
H9	Incident Management	359
H10	Business Continuity	369
H11	Parse and Correlate Software	373
H12	Intimate Communications Hub Interface Specification	378
H13	Performance Standards and Reporting	381
H14	Testing Services	384
H15	DCC Gateway Connections	399

Section I: Data Privacy

I1	Data Protection and Access to Data	407
I2	Other User Privacy Audits	411

Section J: Charges

J1	Payment of Charges	424
J2	Payment Default and Disputes	428
J3	Credit Cover	431
J4	Review and Forecasting of Charges	438

Section K: Charging Methodology

K1	Introduction	440
K2	Estimated Revenues	441
K3	Fixed Charge and Fixed CH Charge Calculations	443
K4	Determining Fixed Charges Before the UITMR Period	452
K5	Determining Fixed Charges During the UITMR Period	454
K5A	Determining Fixed Alt Han Charges During the UITMR Period	459
K6	Determining Fixed Charges After the UITMR Period (Enduring)	461
K6A	Determining Fixed CH Charges	465
K6B	Determining Fixed Alt Han Charges After the UITMR Period (Enduring)	469
K7	Determining Explicit Charges	471
K8	Determining Elective Charges	479

K9 Within-Year Adjustments 482
K10 Calculating Monthly Payments 486
K11 Definitions 493

Section L: Smart Metering Key Infrastructure and DCC Key Infrastructure

L1 SMKI Policy Management Authority 499
L2 SMKI Assurance 507
L3 The SMKI Services 511
L4 The SMKI Service Interface 521
L5 The SMKI Repository Service 525
L6 The SMKI Repository Interface 528
L7 SMKI and Repository Entry Process Tests 531
L8 SMKI Performance Standards and Demand Management 533
L9 The SMKI Document Set 537
L10 The SMKI Recovery Procedure 544
L11 The Subscriber Obligations 556
L12 Relying Party Obligations 560
L13 DCC Key Infrastructure 562

Section M: General

M1 Commencement and Duration 579
M2 Limitations of Liability 580
M3 Services FM and Force Majeure 587
M4 Confidentiality 591
M5 Intellectual Property Rights 599
M6 Party Details 604
M7 Dispute Resolution 605
M8 Suspension Expulsion and Withdrawal 610
M9 Transfer of DCC Licence 616
M10 Notices 618
M11 Miscellaneous 620

Section N: SMETS1 Meters

N1 Definitions for this Section N 624
N2 SMETS1 Enrolment Projects Generally 627

N3 Initial Enrolment 631
N4 Initial Enrolment Project Feasibility Report 635
N5 Initial Enrolment Code Amendments 640

Section T: Testing During Transition

T1 Device Selection Methodology 641
T2 Systems Integration Testing 645
T3 Interface Testing 655
T4 End-to-End Testing 667
T5 SMKI and Repository Testing 673
T6 Development of Enduring Testing Documents 683
T7 Ending of the Application of this Section T 686

Section X: Transition

X1 General Provisions Regarding Transition 687
X2 Effective Provisions at Designation 694
X3 Provisions to Become Effective Following Designation 700
X4 Governance Set-up Arrangements 707
X5 Incorporation of Certain Documents into this Code 710
X6 Transitional Variations 713
X7 Transitional Incident Management Procedures 715
X8 Developing CH Support Materials 718
X9 Interim Device and User System Testing 720
X10 Threshold Anomaly Detection Procedures 724

Section Z: The Alt HAN Arrangements

Z1 The Alt HAN Forum 726
Z2 The Alt HAN Company 740
Z3 Alt HAN Secretariat 750
Z4 Alt HAN Costs and Budgets 751
Z5 Transitional Provisions 760
Z6 Definitions 763

Schedules:

Schedule 1: Framework Agreement 777

Schedule 2: Specimen Accession Agreement 783
Schedule 3: Specimen Bilateral Agreements 789
Schedule 4: SECCo 798
Schedule 5: Accession Information 824
Schedule 6: Specimen Form of Letter of Credit 826
Schedule 7: Specimen Enabling Services Agreement 830

Appendices:

Appendix A: SMKI Device Certificate policy
Appendix B: SMKI Organisation Certificate Policy
Appendix C: SMKI Compliance Policy
Appendix D: SMKI Registration Authority Policies and Procedures
Appendix E: DCC User Interface Services Schedule
Appendix F: Minimum Communication Services For SMETS1 Meters
Appendix G: DCC Gateway Connection Code of Connection
Appendix H: CH Handover Support Materials
Appendix I: CH Installation and Maintenance Support Materials
Appendix J: Enduring Testing Approach Document
Appendix K: SMKI and Repository Test Scenarios Document
Appendix L: SMKI Recovery Procedure

INTRODUCTION

A) This Code has been designated by the Secretary of State pursuant to the DCC Licence, and is subject to modification in accordance with the Secretary of State's statutory powers and the DCC Licence.

B) The Parties comprise the DCC, Users (or prospective Users) of DCC's Services, and persons holding certain Energy Licences that are obliged by those licences to accede to this Code (some of whom are Users of DCC's Services).

C) The Original Parties have agreed to give effect to, and to be bound by, this Code in accordance with the Framework Agreement.

D) The other Parties have agreed to give effect to, and to be bound by, this Code in accordance with an Accession Agreement.

E) SECCo is a company established to facilitate the operation of this Code. SECCo is not a Party (as defined), and only has rights and obligations under this Code where specified.

SECTION A: DEFINITIONS AND INTERPRETATION

A1 DEFINITIONS

A1.1 In this Code, except where the context otherwise requires, the expressions in the left hand column below shall have the meanings given to them in the right hand column below:

Acceptance Testing	means testing of a software release undertaken by Users in order to determine whether the required specification for that software is met.
Accession Agreement	means an accession agreement entered into pursuant to Section B1 (Accession).
Acknowledgement	means, in respect of a communication sent by a User to the DCC over the DCC User Interface, a communication by the DCC to the User via the DCC User Interface acknowledging receipt of the User's communication.
Additional Interface Testing	has the meaning given to that expression in Section T3.34 (Additional Interface Testing).
Additional Interface Testing Objective	has the meaning given to that expression in Section T3.35 (Additional Interface Testing).
Additional Release Services	has the meaning given to that expression in Section X1.17 (Testing in respect of Additional Release Services).
Additional SIT	has the meaning given to that expression in Section T2.25 (Additional Systems Integration Testing).
Additional SIT Objective	has the meaning given to that expression in Section

	T2.26 (Additional Systems Integration Testing).
Additional SMKI and Repository Testing	has the meaning given to that expression in Section T5.30 (Additional SMKI and Repository Testing).
Additional SR Tests	has the meaning given to that expression in Section X1.17 (Testing in respect of Additional Release Services).
Additional SRT Objective	has the meaning given to that expression in Section T5.31 (Additional SMKI and Repository Testing).
Affected Party	has the meaning given to that expression in the definition of Force Majeure.
Affiliate	means, in relation to any person, any holding company of that person, any subsidiary of that person or any subsidiary of a holding company of that person, in each case within the meaning of section 1159 of the Companies Act 2006.
Agency for the Co-operation of Energy Regulators	means the agency of that name established under Regulation 2009/713/EC of the European Parliament and of the Council of 13 July 2009 establishing an Agency for the Co-operation of Energy Regulators.
Alert	has the meaning given to 'Alert' in the GB Companion Specification.
Alt HAN Arrangements	has the meaning given to that expression in condition 22.20(e) (Principal contents within the Smart Energy Code) of the DCC Licence.
Alt HAN Charges	means the Fixed Alt HAN Charges calculated in accordance with Section K5A or K6B (as applicable) taken together with the Explicit Charges in respect of

	the Explicit Charging Metrics at Section K7.5(t) and (u).
Alternate	has the meaning given to that expression in Section C5.19 (Alternates).
Alternative Proposal	has the meaning given to that expression in Section D6.15 (Alternative Proposals).
Anomalous Event	means, in relation to any System, an activity or event that is not expected to occur in the course of the ordinary operation of that System.
Anomaly Detection Threshold	means: (a) in respect of a User, a number of communications within a period of time, where both that number and the period of time are set by the User; (b) in respect of the DCC, either: (i) a number of communications within a period of time, where both that number and the period of time are set by the DCC; or (ii) a maximum or minimum data value within a communication, where that value is set by the DCC, in each case in accordance with the requirements of Section G6 applying (respectively) to the User or the DCC.
Applicant	has the meaning given to that expression in Section B1.1 (Eligibility for Admission).

Application Fee	has the meaning given to that expression in Section B1.5 (Application Fee).
Application Form	means a form requesting the information set out in Schedule 5 (and which must not request any further information), in such format as the Code Administrator may determine from time to time.
Application Guidance	has the meaning given to that expression in Section B1.4 (Application Form and Guidance).
Application Server	means a software framework that enables software applications to be installed on an underlying operating system, where that software framework and operating system are both generally available either free of charge or on reasonable commercial terms.
Appropriate Permission	means, in respect of a Communication Service or Local Command Service to be provided to a User in respect of a Smart Metering System at a premises that will result in the User obtaining Consumption Data, either: (a) (where that User is the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) that the User does not need consent to access that Consumption Data in accordance with its Energy Licence, or that the User has consent (whether explicit or implicit) in accordance with the requirements of its Energy Licence; or (b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity

Distributor or Gas Transporter for that Smart Metering System) that the Energy Consumer has given the User ~~e~~Explicit ~~e~~Consent to obtain that Consumption Data and such consent has not been withdrawn.

Approved Budget has the meaning given to that expression in Section C8.13 (Approval of Budgets).

Approved Finance Party means, in respect of each Communications Hub Finance Facility, the person to whom the DCC accepts payment obligations under the Direct Agreement relating to that facility, and which has (from time to time) been notified by the DCC to the Authority and the Panel as meeting the requirements of this definition.

Associated means:

(a) in respect of a Smart Meter, that the Smart Meter is identified in the Smart Metering Inventory as being associated with a Communications Hub Function; and

(b) in respect of any Device other than a Smart Meter or a Communications Hub Function, that the Device is identified in the Smart Metering Inventory as being associated with a Smart Meter or with a Gas Proxy Function,

and the expression "**Associate**" shall be interpreted accordingly.

Assurance Certificate has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).

Assurance Certification Body	has the meaning given to that expression in Section F2.3 (Background to Assurance Certificates).
Authorised Business	in relation to the DCC, has the meaning given in the DCC Licence.
Authorised Subscriber	means SECCo, a Party or an RDP which is an Authorised Subscriber for the purposes of (and in accordance with the meaning given to that expression in) any of the Certificate Policies.
Authority	means the Gas and Electricity Markets Authority as established under section 1 of the Utilities Act 2000.
Back-Up	means, in relation to Data which is held on any System, the storage of a copy of that Data for the purpose of ensuring that the copy may be used (if required) to restore or replace the original Data; and "Backed-Up" is to be interpreted accordingly.
Bank Guarantee	means an on demand bank guarantee in a form reasonably acceptable to the DCC from a bank with the Required Bank Rating which guarantee has not been breached or disclaimed by the provider and has at least one month left until it expires.
Batched Certificate Signing Request	has the meaning given to that expression in Section L8.2 (SMKI Services: Target Response Times).
BCDR Procedure	means the Business Continuity and Disaster Recovery Procedure.
Bilateral Agreement	means an agreement entered into pursuant to Section H7 (Elective Communication Services) between the DCC and a User.

Business Architecture	means the business architecture which is designed to enable Parties to use the Services and/or to enable Parties, Energy Consumers and those acting on behalf of Energy Consumers to access the functionality described in the Technical Specifications.
Business Architecture Document	means a document that describes the Business Architecture.
Business Continuity and Disaster Recovery Procedure	means that part of the Incident Management Policy which describes the business continuity and disaster recovery procedures applicable to the Services.
Cash Deposit	means a deposit of funds by or on behalf of the User into a bank account in the name of the DCC, such that title in such funds transfers absolutely to the DCC.
Certificate	means a Device Certificate, DCA Certificate, Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate.
Certificate Policy	means the Device Certificate Policy, the Organisation Certificate Policy, or the IKI Certificate Policy.
Certificate Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.
Certified Products List	has the meaning given to that expression in Section F2.1 (Certified Products List).
CESG	means the UK Government's national technical authority for information assurance.
CESG CHECK	means the scheme of that name which is administered by CESG, or any successor to that scheme.

CESG Listed Advisor Scheme (CLAS)	means the scheme of that name which is administered by CESG, or any successor to that scheme.
CESG Tailored Assurance Service (CTAS)	means the scheme of that name which is administered by CESG, or any successor to that scheme.
CH Batch Fault	has the meaning given to that expression in Section F9.20 (Liquidated Damages for CH Batch Faults).
CH Batch Fault Payment	has the meaning given to that expression in Section F9.21 (Liquidated Damages for CH Batch Faults).
CH Defect	means, in respect of a Communications Hub, any fault or defect in relation to the Communications Hub (including any failure: to conform in all respects with, and be fit for the purposes described in, the CHTS; to be free from any defect in design, manufacture, materials or workmanship; and to comply with all applicable Laws and/or Directives including with respect to product safety), which is not caused by a breach of this Code by a Party other than the DCC.
CH Fault Diagnosis	has the meaning given to that expression in Section F9.7 (CH Fault Diagnosis).
CH Handover Support Materials	means, in respect of each Region, the SEC Subsidiary Document of that name set out in Appendix H and applying to that Region, which document is originally to be developed pursuant to Section X8 (Developing CH Support Materials).
CH Installation and Maintenance Support Materials	means, in respect of each Region, the SEC Subsidiary Document of that name set out in Appendix [TBC] and applying to that Region, which document is originally to be developed pursuant to Section X8 (Developing

	CH Support Materials).
CH Order Management System	means that part of the CH Ordering System described as the 'Order Management System' in the CH Handover Support Materials.
CH Ordering System	has the meaning given to that expression in Section F5.20 (CH Ordering System).
CH Post-Installation DCC Responsibility	has the meaning given to that expression in Section F9.6 (Categories of Responsibility).
CH Pre-Installation DCC Responsibility	has the meaning given to that expression in Section F9.6 (Categories of Responsibility).
CH Support Materials	means the CH Handover Support Materials and the CH Installation and Maintenance Support Materials.
CH Type Fault	has the meaning given to that expression in Section F9.16 (Liquidated Damages for CH Type Faults).
CH Type Fault Payment	has the meaning given to that expression in Section F9.19 (Liquidated Damages for CH Type Faults).
CH User Responsibility	has the meaning given to that expression in Section F9.6 (Categories of Responsibility).
Change Board	has the meaning given to that expression in Section D8.1 (Establishment of the Change Board).
Change Board Member	has the meaning given to that expression in Section D8.4 (Membership of the Change Board).
Charges	means the charges payable to the DCC pursuant to this Code (including pursuant to Bilateral Agreements).
Charging Methodology	means the methodology for determining the Charges,

	as set out in Section K (Charging Methodology).
Charging Objectives	has the meaning given to that expression in Section C1 (SEC Objectives).
Charging Statement	means, from time to time, the statement prepared by DCC pursuant to Condition 19 of the DCC Licence that is in force at that time.
Check Cryptographic Protection	means, in respect of ~~a communication~~any electronic Data, to check the Digital Signature or Message Authentication Code within ~~the communication~~those Data (as applicable) using: (a) the Public Key contained in the certificate issued by the relevant Certificate Authority associated with the Private Key of the person or device that ~~the communication~~those Data ~~identifies~~identify, or ~~implies~~ imply has generated the Digital Signature; (b) where applicable, the recipient's relevant Private Key; and (c) the relevant algorithm identified in the certificate policy under which the relevant certificates were issued (or, where such certificate or certificate policy does not exist, the appropriate algorithm).
CHTS	means the Communications Hub Technical Specification.
Citizens Advice	means the National Association of Citizens Advice Bureaux.

Citizens Advice Scotland	means the Scottish Association of Citizens Advice Bureaux.
Code	means this Smart Energy Code (including its Schedules and the SEC Subsidiary Documents).
Code Administration Code of Practice	means the document of that name as approved by the Authority from time to time.
Code Administration Code of Practice Principles	means the principles set out as such in the Code Administration Code of Practice.
Code Administrator	has the meaning given to that expression in Section C7.1 (Code Administrator).
Code Performance Measure	means a performance measure set out in either Section H13.1 (Code Performance Measures) or Section L8.6 (Code Performance Measures).
Command	means a communication to a Device in the format required by the GB Companion Specification and which incorporates all Digital Signatures and/or Message Authentication Codes required by the GB Companion Specification.
Commercial Activities	includes, in particular, Energy Efficiency Services, Energy Management Services, Energy Metering Services, and Energy Price Comparison Services, in each case as defined in the DCC Licence and in relation to the Supply of Energy (or its use) under the Electricity Act and the Gas Act.
Commissioned	means, in respect of a Device, that: (a) the Device has been commissioned in accordance with the Smart Metering Inventory

Enrolment and Withdrawal Procedures; and

(b) the Device has not subsequently been Decommissioned, Withdrawn or Suspended,

and "**Commission**" is to be interpreted in accordance with (a) above. A Communications Hub shall be considered to be Commissioned where the Communications Hub Function that forms part of that Communications Hub is Commissioned.

Common Test Scenarios Document	means the SEC Subsidiary Document set out in Appendix [TBC], which is originally to be developed pursuant to Section T6 (Development of Enduring Testing Documents).
Communication Services	means the Core Communication Services or the Elective Communication Services.
Communications Hub	means a physical device that includes a Communications Hub Function together with a Gas Proxy Function; save that, when such expression is used in relation to the following provisions, such expression shall be interpreted in accordance with the definition of that expression in the DCC Licence: (a) the definitions of "CH Defect" and "Test Communications Hub"; and (b) Sections F5 (Communications Hub Forecasts & Orders), F6 (Delivery and Acceptance of Communications Hub Orders) and F10 (Test Communications Hubs).
Communications Hub Auxiliary Equipment	means any additional, replacement or spare equipment or packaging (not forming part of a Communications Hub) that may be required by a Supplier Party in

	relation to the installation, maintenance or return of a Communications Hub, as listed by the DCC on the CH Ordering System from time to time.
Communications Hub Charges	has the meaning given to the expression 'Fixed CH Charges' in Section K (Charging Methodology).
Communications Hub Finance Acceleration Event	means, in respect of each Communications Hub Finance Facility, that: (a) an acceleration of repayment of the indebtedness thereunder occurs such that it is immediately due and payable by the borrower in circumstances where the DCC is liable for the same under the Direct Agreement; or (b) the DCC becomes liable under the Direct Agreement to immediately pay the unamortised asset value (and any associated finance costs in respect) of the Communications Hubs to which that facility relates.
Communications Hub Finance Charges	means, in respect of each Communications Hub Finance Facility, the DCC's charge to recover the applicable Communications Hub Finance Costs (being a subset of the Communications Hub Charges), in an amount each month determined by the DCC at the time it produces an Invoice for that month (having regard to the requirements of Condition 36.5 of the DCC Licence).
Communications Hub Finance Costs	means, in respect of each Communications Hub Finance Facility, the costs the DCC incurs in procuring the provision (but not the maintenance) of the tranche of Communications Hubs to which that facility relates.

Communications Hub Finance Facility	means a facility arranged by a DCC Service Provider with an Approved Finance Party relating exclusively to the funding of the costs associated with acquiring a tranche of Communications Hubs, including by way of a loan facility, an equity subscription, or an assignment or sale of receivables.
Communications Hub Forecast	has the meaning given to that expression in Section F5.2 (Communications Hub Forecasts).
Communications Hub Function	means that part of a device installed (or to be installed) at a premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other requirements of, a version of the CHTS (but excluding those provisions that are described as applying only to 'Gas Proxy Functions') which was a Valid Technical Specification on the date on which the device was installed.
Communications Hub Hot Shoe	means equipment, other than a Smart Meter, to which a Communications Hub can be connected (provided the Communications Hub complies with the ICHIS).
Communications Hub Order	has the meaning given to that expression in Section F5.7 (Communications Hub Orders).
Communications Hub Products	means, in respect of a Valid Communications Hub Order, the Communications Hubs of the applicable Device Models that are the subject of that order and/or

	the Communications Hub Auxiliary Equipment that is the subject of that order.
Communications Hub Services	means those Services described in Sections F5 (Communications Hub Forecasts & Orders), F6 (Delivery and Acceptance of Communications Hub), F7 (Installation and Maintenance of Communications Hubs), F8 (Removal and Return of Communications Hubs), and F9 (Categories of Communications Hub Responsibility).
Communications Hub Technical Specification	means the document(s) set out in Schedule [TBC].
Competent Authority	means the Secretary of State, the Authority, and any local or regional or national agency, authority, department, inspectorate, minister, ministry, official or public or statutory person (whether autonomous or not) of the government of the United Kingdom or of the European Union (but only insofar as each has jurisdiction over the relevant Party, this Code or its subject matter).
Completion of Implementation	has the meaning given to that expression in Section X1 (General Provisions Regarding Transition).
Compromised	means: (a) in relation to any System, that the intended purpose or effective operation of that System is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity or availability of the System or of any Data that are stored on or communicated by means of it;

(b) in relation to any Device, that the intended purpose or effective operation of that Device is compromised by the occurrence of any event which has an adverse effect on the confidentiality, integrity or availability of the Device or of any Data that are stored on or communicated by means of it;

(c) in relation to any Data, that the confidentiality, integrity or availability of that Data is adversely affected by the occurrence of any event;

(d) in relation to any Secret Key Material, that that Secret Key Material (or any part of it), or any Cryptographic Module within which it is stored, is accessed by, or has become accessible to, a person not authorised to access it;

(e) in relation to any Certificate, that any of the following Private Keys is Compromised:

(i) the Private Key associated with the Public Key that is contained within that Certificate;

(ii) the Private Key used by the relevant Certification Authority to Digitally Sign the Certificate; or

(iii) where relevant, the Private Key used by the relevant Certification Authority to Digitally Sign the Certification Authority Certificate associated with the Private Key referred to in (ii); and

(f) in relation to any DCCKI Certificate, that any of the following Private Keys is Compromised:

(i) the Private Key associated with the Public Key that is contained within that DCCKI Certificate;

(ii) the Private Key used by the DCCKICA to Digitally Sign the DCCKI Certificate; or

(iii) where relevant, the Private Key used by the DCCKICA to Digitally Sign the DCCKICA Certificate associated with the Private Key referred to in (ii); and

(g) in relation to any process or to the functionality of any hardware, firmware or software, that the intended purpose or effective operation of that process or functionality is compromised by the occurrence of any event which has an adverse effect on its confidentiality, integrity or availability,

(and "**Compromise**" and "**Compromising**" are to be interpreted accordingly).

Confidential Information means, in respect of a Party other than DCC, the Data belonging or relating to that Party or that otherwise becomes available to the DCC as a result (whether directly or indirectly) of that Party being a party to this Code.

Confirm Validity means:

(a) where the person carrying out the check has not previously done so in relation to a particular certificate, to successfully confirm the certificate

path validation by using:

(i) the path validation algorithm specified in IETF RFC 5280; or

(ii) where the algorithm identified in IETF RFC 5280 is not appropriate for the certificate for which validity is being confirmed, such other certificate path validation as is appropriate in relation to that type of certificate; or

(b) where the person carrying out the check has previously carried out the check in paragraph (a) in relation to a particular certificate, that the certificate has not subsequently been revoked, and its validity period has not expired.

Consignment	has the meaning given to that expression in Section F5.9 (Communications Hub Orders).
Consultation Summary	has the meaning given to that expression in Section D6.14 (Working Group Consultation).
Consumer Data	has the meaning given to that expression in Section M5.6 (Consumer Data).
Consumer Member	has the meaning given to that expression in Section C3.1 (Panel Composition).
Consumer Prices Index	means, in respect of any month, the consumer prices index (CPI) published for that month by the Office of National Statistics.
Consumption Data	means, in respect of a premises, the quantity of

	electricity or gas measured by the Energy Meter as having been supplied to the premises.
Contingency Key Pair	has the meaning given to that expression in Section L10.30(e) (Definitions).
Contingency Private Key	has the meaning given to that expression in Section L10.30(e)(i) (Definitions).
Contingency Public Key	has the meaning given to that expression in Section L10.30(e)(ii) (Definitions).
Core Communication Services	means the provision of the Services set out in the DCC User Interface Services Schedule, but excluding the Enrolment Services and Local Command Services.
Correlate	means, in respect of one or more Pre-Commands received by a User from the DCC in respect of a Service Request sent by that User, carrying out a process to check that the relevant contents of the Pre-Command is substantively identical to that of the Service Request using either (at the User's discretion): (a) the Parse and Correlate Software; or (b) equivalent software procured or developed by the User in accordance with Good Industry Practice, and "**Correlated**" shall be interpreted accordingly.
CoS Party	means the DCC when performing the tasks ascribed to the CoS Party in the Service Request Processing Document.

CPA Assurance Maintenance Plan	means the document agreed with the CESG that describes the components of a device which, if changed, will require a new CPA Certificate to be issued.
CPA Certificates	has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).
CPL Requirements Document	means the SEC Subsidiary Document of that name set out as Appendix [TBC].
Credit Assessment Score	means, in respect of a User, a credit assessment score in respect of that User procured from one of the credit assessment companies named in Section J3.8 (User's Credit Cover Factor). Where more than one credit assessment product is listed in respect of that company, it shall be the score determined in accordance with the listed product that the DCC reasonably considers the most appropriate for the User.
Credit Cover Factor	has the meaning given to that expression in Section J3.4 (User's Credit Cover Factor).
Credit Cover Requirement	has the meaning given to that expression in Section J3.2 (Calculation of Credit Cover Requirement).
Credit Cover Threshold	means, in respect of each Regulatory Year, £2,000, multiplied by the Consumer Prices Index for the October preceding the start of that Regulatory Year, divided by the Consumer Prices Index for October 2014. The relevant amount will be rounded to the nearest pound.
Credit Support	means one or more of a Bank Guarantee, Cash Deposit

	and/or Letter of Credit procured by a User pursuant to Section J3 (Credit Cover).
CREST	means the not-for-profit company registered in the United Kingdom with company number 06024007.
Critical Command	has the meaning given to that expression in the GB Companion Specification.
Critical Service Request	means a Service Request which is identified as critical in the DCC User Interface Specification (or, in the case of Elective Communication Services, the relevant Bilateral Agreement).
Critical Service Response	means a Service Response in respect of a Critical Service Request.
Cryptographic Credential Token	means a token compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time) and containing Secret Key Material, as issued in accordance with the SMKI RAPP.
Cryptographic Hash Function	means an algorithm: (a) the inputs to which it would be computationally infeasible to determine from knowledge of its outputs; and (b) in relation to which it would be computationally infeasible to find an input which generates the same output as any other input.
Cryptographic Module	means a set of hardware, software and/or firmware that is Separated from all other Systems and that is designed for:

(a) the secure storage of Secret Key Material; and

(b) the implementation of Cryptographic Processing without revealing Secret Key Material.

Cryptographic Processing means the generation, storage or use of any Secret Key Material.

Data means any information, data, knowledge, figures, methodologies, minutes, reports, forecasts, images or sounds (together with any database made up of any of these) embodied in any medium (whether tangible or electronic).

Data Protection Act means the Data Protection Act 1998.

Data Retention Policy means a document developed and maintained by a Party which sets out, in relation to Data held by that Party, the periods for which such Data will be held by it for the purpose of ensuring that it is able to satisfy its legal, contractual and commercial requirements in respect of the Data.

DCA Certificate has the meaning given to that expression in Annex A of the Device Certificate Policy.

DCC means, subject to Section M9 (Transfer of DCC Licence), the holder from time to time of the DCC Licence. In accordance with Section A2.1(l), references to the DCC shall (where applicable) include references to the DCC Service Providers with whom the DCC has contracted in order to secure performance of its obligations under this Code.

DCC Alert has the meaning given to that expression in the DCC User Interface Specification.

DCC Gateway Bandwidth Option	means a DCC Gateway HV Connection or a DCC Gateway LV Connection.
DCC Gateway Connection	means, for a premises, the physical infrastructure by which a connection is (or is to be) made between that premises and the DCC Systems (and each DCC Gateway Connection shall form part of the DCC Systems).
DCC Gateway Connection Code of Connection	means the SEC Subsidiary Document set out in Appendix G.
DCC Gateway Equipment	means, for each premises and any DCC Gateway Connection provided at that premises, that part of the DCC Gateway Connection that is (or is to be) located within that premises.
DCC Gateway HV Connection	means the high-volume technology solution by which the DCC provides DCC Gateway Connections, as further described in the DCC Gateway Connection Code of Connection.
DCC Gateway LV Connection	means the low-volume technology solution by which the DCC provides DCC Gateway Connections, as further described in the DCC Gateway Connection Code of Connection.
DCC Gateway Party	means a Party that is seeking or has been provided with a DCC Gateway Connection at its premises, or to whom the right to use that connection has been transferred in accordance with Section H15.16 (Use of a DCC Gateway Connection).
DCC ID	means each identification number established by the DCC pursuant to Section H4.43 (DCC IDs).

DCC Independent Security Assessment Arrangements	has the meaning given to that expression in Section G9.1 (The DCC Independent Security Assessment Arrangements).
DCC Independent Security Assurance Service Provider	has the meaning given to that expression in Section G9.4 (The DCC Independent Security Assurance Service Provider).
DCC Interfaces	means each and every one of the following interfaces: (a) the DCC User Interface; (b) the Registration Data Interface; (c) the SMKI Repository Interface; (d) the SMKI Services Interface; (e) the Self-Service Interface; and (f) the communications interfaces used for the purposes of accessing those Testing Services designed to be accessed via DCC Gateway Connections.
DCC Internal Systems	means those aspects of the DCC Total System for which the specification or design is not set out in this Code.
DCC IT Supporting Systems	means, with regard to the DCC's duty to Separate parts of the DCC Total System, those parts of the DCC Total System which are used to support the DCC Live Systems and DCC IT Testing and Training Systems.
DCC IT Testing and Training Systems	means, with regard to the DCC's duty to Separate parts of the DCC Total System, those parts of the DCC

	Total System which are used to support the testing and training of DCC Personnel and third parties in relation to the provision of Services by the DCC.
DCC Key Infrastructure (or **DCCKI**)	means the public key infrastructure established by DCC to provide, amongst other things, transport layer security across DCC Gateway Connections.
DCC Licence	means the licences granted under section 6(1A) of the Electricity Act and section 7AB(2) of the Gas Act.
DCC Live Systems	means, with regard to the DCC's duty to Separate parts of the DCC Total System, those parts of the DCC Total System which are used for the purposes of: (a) (other than to the extent to which the activities fall within paragraph (b), (c) or (f) below) processing Service Requests, Pre-Commands, Commands, Service Responses and Alerts, holding or using Registration Data for the purposes of processing Service Requests and Signed Pre-Commands, and providing the Repository Service; (b) Threshold Anomaly Detection and (other than to the extent to which the activity falls within paragraph (d) or (f) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code; (c) discharging the obligations placed on the DCC in its capacity as CoS Party; (d) providing SMKI Services; (e) the Self-Service Interface; and (f) discharging the DCC's obligations under the

	SMKI Recovery Procedure, each of which shall be treated as an individual System within the DCC Live Systems.
DCC Member	has the meaning given to that expression in Section C3.1 (Panel Composition).
DCC Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the Authorised Business.
DCC Release Management Policy	has the meaning given to that expression in Section H8.9 (Release Management).
DCC Security Assessment Report	has the meaning given to that expression in Section G9.7(a) (DCC Security Assessment Reports and Responses).
DCC Security Assessment Response	has the meaning given to that expression in Section G9.7(b) (DCC Security Assessment Reports and Responses).
DCC Service Provider	means an External Service Provider, as defined in the DCC Licence (but always excluding the DCC itself).
DCC Service Provider Contract	means, as between the DCC and each DCC Service Provider, any arrangement (however described) pursuant to which the DCC procures services for the purpose of providing the Services.
DCC Systems	means the DCC Total System, including the SM WAN but excluding all Communications Hubs.
DCC Total System	means the Systems used by the DCC and/or the DCC Service Providers in relation to the Services and/or this

	Code, including the DCC User Interface, SM WAN and Communications Hubs except for those Communications Hubs which are: (a) neither installed nor in the possession of the DCC; or (b) installed, but are not Commissioned.
DCC User Interface	means the communications interface designed to allow the communications referred to in Section H3.3 (Communications to be sent via the DCC User Interface) to be sent between the DCC and Users.
DCC User Interface Code of Connection	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
DCC User Interface Services	means the Services described in the DCC User Interface Services Schedule.
DCC User Interface Services Schedule	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
DCC User Interface Specification	means the SEC Subsidiary Document set out in Appendix [TBC].
DCC Website	means the DCC's publicly available website (or, where the Panel and the DCC so agree, the Website).
DCCKI Authorised Subscriber	means a Party or RDP which is a DCCKI Authorised Subscriber for the purposes of (and in accordance with the meaning given to that expression in) the DCCKI Certificate Policy.
DCCKI Authority Revocation List (or **DCCKI ARL**)	has the meaning given to that expression in the DCCKI Certificate Policy.

DCCKI Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certificate Policy	means the SEC Subsidiary Document of that name set out in Appendix [TBD].
DCCKI Certificate Revocation List (or **DCCKI CRL**)	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certificate Signing Request	means a request for a DCCKI Certificate submitted by a DCCKI Eligible Subscriber in accordance with the DCCKI Certificate Policy and the DCCKI RAPP.
DCCKI Certification Authority (or **DCCKICA**)	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Certification Practice Statement (or **DCCKI CPS**)	has the meaning given to that expression in Section L13.37 (the DCCKI Certification Practice Statement).
DCCKI Code of Connection	means the SEC Subsidiary Document of that name set out in Appendix [TBD], which: (a) has the purpose described in Section L13.14 (DCCKI Code of Connection); and (b) is originally to be developed pursuant to Sections L13.15 to L13.16 (DCCKI Interface Document Development).
DCCKI Document Set	has the meaning given to that expression in Section L13.33 (the DCCKI Document Set).
DCCKI Eligible Subscriber	has the meaning given to that expression in Section L13.8 (DCCKI Eligible Subscribers).

DCCKI Infrastructure Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.
DCCKI Interface Design Specification	means the SEC Subsidiary Document of that name set out in Appendix [TBD], which: (a) has the purpose described in Section L13.13 (DCCKI Interface Design Specification); and (b) is originally to be developed pursuant to Sections L13.15 to L13.16 (DCCKI Interface Document Development).
DCCKI Participants	means the DCC (acting in its capacity as the provider of the DCCKI Services), all DCCKI Subscribers and all DCCKI Relying Parties.
DCCKI PMA Functions	has the meaning given to that expression in Section L13.54 (the DCCKI PMA Functions).
DCCKI Registration Authority	means the DCC, acting in its capacity as such for the purposes of (and in accordance with the meaning given to that expression in) the DCCKI Certificate Policy.
DCCKI Registration Authority Policies and Procedures (or **DCCKI RAPP**)	means the SEC Subsidiary Document of that name set out in Appendix [TBD], which is originally to be developed pursuant to Sections L13.35 to L13.36 (the DCCKI Registration Authority Policies and Procedures: Document Development).
DCCKI Relying Party	means a person who, pursuant to the Code, receives and relies upon a DCCKI Certificate.
DCCKI Repository	has the meaning given to that expression in Section L13.17 (the DCCKI Repository).

DCCKI Repository Code of Connection	means the SEC Subsidiary Document of that name set out in Appendix [TBD], which: (a) has the purpose described in Section L13.28 (DCCKI Repository Code of Connection); and (b) is originally to be developed pursuant to Sections L13.29 to L13.30 (DCCKI Repository Interface Document Development).
DCCKI Repository Interface	has the meaning given to that expression in Section L13.26 (the DCCKI Repository Interface).
DCCKI Repository Interface Design Specification	means the SEC Subsidiary Document of that name set out in Appendix [TBD], which: (a) has the purpose described in Section L13.27 (DCCKI Repository Interface Design Specification); and (b) is originally to be developed pursuant to Sections L13.29 to L13.30 (DCCKI Repository Interface Document Development).
DCCKI Repository Service	has the meaning given to that expression in Section L13.18 (the DCCKI Repository Service).
DCCKI SEC Documents	has the meaning given to that expression in Section L13.34 (the DCCKI SEC Documents).
DCCKI Service Interface	has the meaning given to that expression in Section L13.12 (the DCCKI Service Interface).
DCCKI Services	has the meaning given to that expression in Section L13.1 (the DCCKI Services).
DCCKI Subscriber	means, in relation to any DCCKI Certificate, a Party or RDP which has been Issued with and accepted that

	Certificate, acting in its capacity as the holder of the Certificate.
DCCKICA Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.
Decommissioned	means, in respect of a Device that has previously been Commissioned, that the Device has been decommissioned in accordance with Section H6.1 (Decommissioning).
Default Interest Rate	means, for any day, 8% above the base lending rate of the Bank of England at 13.00 hours on that day.
Defaulting Party	has the meaning given to that expression in Section M8.1 (Events of Default).
Delivery Batch	means all the Communications Hubs that were delivered pursuant to Section F6 (Delivery and Acceptance of Communications Hubs) to a single location during a month (regardless of whether they were delivered pursuant to more than one Communications Hub Order by more than one Party).
Delivery Date	has the meaning given to that expression in Section F5.8 (Communications Hub Orders).
Delivery Location	has the meaning given to that expression in Section F5.8 (Communications Hub Orders).
Delivery Month	has the meaning given to that expression in Section F5.8 (Communications Hub Orders).
Delivery Quantity	has the meaning given to that expression in Section F5.8 (Communications Hub Orders).

Delivery Window	means, for each delivery of Communications Hub Products to a Delivery Location, the time period on the applicable Delivery Date within which the DCC is to deliver the Communications Hub Products, as established in accordance with the CH Handover Support Materials.
Denial of Service Event	means any unauthorised attempt to make any part of a System wholly or partially unavailable for use for a period of time.
Designated Premises	means Non-Domestic Premises defined as Designated Premises within the meaning given to that expression in the Electricity Supply Licences or the Gas Supply Licences.
Detailed Evaluation	has the meaning given to that expression in Section H7.7 (Detailed Evaluation of Elective Communication Services).
Device	means one of the following individual devices: (a) an Electricity Smart Meter; (b) a Gas Smart Meter; (c) a Communications Hub Function; (d) a Gas Proxy Function; (e) a Pre-Payment Meter Interface Device; (f) a HAN Connected Auxiliary Load Control Switch; and (g) any Type 2 Device.
Device Alert	has the meaning given to that expression in the DCC User Interface Specification.
Device and User System Tests	has the meaning given to that expression in Section H14.31 (Device and User System Tests).
Device Certificate	has the meaning given to that expression in Annex A of the Device Certificate Policy.

Device Certificate Policy	means the SEC Subsidiary Document of that name set out in Appendix A.
Device Certification Authority (or **DCA**)	has the meaning given to that expression in Annex A of the Device Certificate Policy.
Device Certification Practice Statement (or **Device CPS**)	has the meaning given to that expression in Section L9.8 (the Device Certification Practice Statement).
Device ID	means the unique number by which an individual Device can be identified, as allocated to that Device in accordance with the applicable Technical Specification.
Device Log	means, in respect of a Device (excluding Type 2 Devices), the electronic record within that Device which records the other Devices from which that Device can receive Data via the HAN.
Device Model	means, in respect of a Communications Hub or a Device (other than a Communications Hub Function or a Gas Proxy Function), the Manufacturer, the model, the hardware version and the firmware version of the Communications Hub or Device.
Device Security Credentials	means, in respect of any Device (other than a Type 2 Device), the Device's active Device Certificates and the electronic record within that Device of information from any other Certificates required to be held on the Device in order to execute the functionality of that Device specified in the GB Companion Specification.
Device Selection Methodology	has the meaning given to that expression in Section T1.3 (Device Selection Methodology).

Device Type	means, in respect of a Device, a generic description of the category of Devices into which the Device falls.
Digital Signature	means, in respect of ~~a communication~~any electronic Data, a digital signature generated using: (a) the entirety of ~~that communication~~those Data (excluding the digital signature itself and, to the extent specified in the code, any other parts of ~~the communication~~those Data); (b) a Private Key; and (c) the signature algorithm defined in the certificate profile in the certificate policy under which the certificate associated with that Private Key was issued or (where such certificate policy does not exist) the signature algorithm relevant to that certificate.
Digitally Signed	means, in respect of ~~a communication~~any electronic Data, that such ~~communication~~ Data ~~has~~ have had the necessary Digital Signatures applied to ~~it~~ them (and "**Digitally Sign**" and "**Digitally Signing**" are to be interpreted accordingly).
Direct Agreement	means, in respect of each Communications Hub Finance Facility, any agreement entered into by the DCC in relation to that facility under which the DCC owes direct payment obligations.
Disaster	means an event that causes one or more of the 'DCC Disaster Impacts' listed in the BCDR Procedure.
Dispute	means any dispute or difference (of whatever nature)

	arising under, out of or in connection with this Code and/or any Bilateral Agreement.
DLMS Certificates	has the meaning given to that expression in Section F2.4 (Background to Assurance Certificates).
DLMS User Association	means the association of that name located in Switzerland (see - www.dlms.com).
Domestic Premises	means premises at which a Supply of Energy is or will be taken wholly or mainly for domestic purposes, which is to be interpreted in accordance with Condition 6 of the relevant Energy Supply Licence.
Draft Budget	has the meaning given to that expression in Section C8.11 (Preparation of Draft Budgets).
Due Date	has the meaning given to that expression in Section J1.5 (Payment of Charges).
EII DCCKICA Certificate	has the meaning given to that expression in the DCCKI Certificate Policy.
Elected Members	has the meaning given to that expression in Section C3.1 (Panel Composition).
Elective Communication Services	means the provision of communication services that are (or are to be) defined in a Bilateral Agreement (rather than the DCC User Interface Services Schedule) in a manner that involves communication via the SM WAN (provided that such services must relate solely to the Supply of Energy or its use).
Electricity Act	means the Electricity Act 1989.
Electricity Distribution	means a licence granted, or treated as granted, under

Licence	section 6(1)(c) of the Electricity Act.
Electricity Distributor	means, for a Smart Metering System or a Device, the holder of the Electricity Distribution Licence for the network to which the relevant premises are connected.
Electricity Meter	means any meter that conforms to the requirements of paragraph 2 of schedule 7 to the Electricity Act and is used for the purpose of measuring the quantity of electricity that is supplied to premises.
Electricity Network Party	means a Party that holds an Electricity Distribution Licence.
Electricity Smart Meter	means a device installed (or to be installed) at a premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other requirements of, the part(s) of the SMETS identified as applying to 'Electricity Smart Metering Equipment' (and, where applicable, the part(s) relevant to the Physical Device Type in question) in a version of the SMETS which was the Valid Technical Specification on the date on which the device was installed. Devices that meet the requirements of the version of the SMETS that was designated on 18 December 2012 (and amended and restated on 31 March 2014) are not currently included within this definition.

Electricity Supplier Party	means a Party that holds an Electricity Supply Licence (regardless of whether that Party also holds a Gas Supply Licence).
Electricity Supply Licence	means a licence granted, or treated as granted, pursuant to section 6(1)(d) of the Electricity Act.
Eligible Subscriber	has the meaning given to that expression in Section L3.15 (Eligible Subscribers).
Eligible User	means, in respect of a Service set out in the DCC User Interface Services Schedule or an Elective Communication Service and (in either case) a Smart Metering System (or a Device forming, or to form, part of a Smart Metering System), one of the Users eligible to receive that Service in respect of that Smart Metering System (or such a Device), as further described in Section H3.8 (Eligibility for Services).
Eligible User Role	means, in respect of a Service set out in the DCC User Interface Services Schedule or an Elective Communication Service, one of the User Roles that is capable of being an Eligible User in respect of that Service (determined without reference to a particular Smart Metering System or Device).
Enabling Services	means one or more of the Enrolment Service, the Communications Hub Service, and the Other Enabling Services.
Encrypt	means, in respect of Section H4 (Processing Service Requests), the process of encoding Data using the methods set out for that purpose in the GB Companion Specification; and "**Encrypted**" shall be interpreted

	accordingly.
End-to-End Security Architecture	means a document that describes how the security controls in respect of smart metering relate to the architecture of the End-to-End Smart Metering System.
End-to-End Smart Metering System	means the DCC Total System, all Enrolled Smart Metering Systems, all User Systems and all RDP Systems.
End-to-End Technical Architecture	means the DCC Systems and the Smart Metering Systems together, including as documented in the Technical Code Specifications.
End-to-End Testing	means the testing described in Section T4 (End-to-End Testing).
End-to-End Testing Approach Document	has the meaning given to that expression in Section T4.4 (End-to-End Testing Approach Document).
Enduring Testing Approach Document	means the SEC Subsidiary Document set out in Appendix J, which is originally to be developed pursuant to Section T6 (Development of Enduring Testing Documents).
Energy Code	means a multilateral code or agreement maintained pursuant to one or more of the Energy Licences.
Energy Consumer	means a person who receives, or wishes to receive, a Supply of Energy at any premises in Great Britain.
Energy Licence	means a licence that is granted, or treated as granted, under section 6 of the Electricity Act or under section 7, 7A or 7AB of the Gas Act.

Energy Meter	means an Electricity Meter or a Gas Meter.
Energy Supply Licence	means an Electricity Supply Licence or a Gas Supply Licence.
Enrolment	means, in respect of a Smart Metering System, the act of enrolling that Smart Metering System in accordance with the Enrolment Service (and the words "**Enrol**" and "**Enrolled**" will be interpreted accordingly). Enrolment of a Smart Metering System ends on its Withdrawal.
Enrolment Service	means the Service described in Section H5 (Enrolment Services and the Smart Metering Inventory).
EU Regulations	means: (a) Regulation 2009/714/EC of the European Parliament and of the Council of 13 July 2009 on conditions for access to the network for cross-border exchange in electricity and repealing Regulation 2003/1228/EC; and (b) Regulation 2009/715/EC of the European Parliament and of the Council of 13 July 2009 on conditions for access to the national gas transmission networks and repealing Regulation 2005/1775/EC, as amended by Commission Decision 2010/685/EU of 10 November 2010 amending Chapter 3 of Annex I to Regulation 2009/715/EC of the European Parliament and of the Council on conditions for access to the natural gas transmission networks.
EUI-64 Compliant	means a 64-bit globally unique identifier governed by

	the Institute of Electrical and Electronics Engineers.
Event of Default	has the meaning given to that expression in Section M8.1 (Events of Default).
Explicit Consent	means the explicit and informed consent of an Energy Consumer given to a User to undertake a specified action, and that consent shall not be treated as having been given explicitly unless the Energy Consumer has: (a) of his or her own volition, communicated to the User a request for it to undertake that action; or (b) in response to a specific request by the User for him or her to indicate consent to it undertaking that action, take a positive step amounting to a clear communication of that consent.
Export MPAN	means an MPAN for a Metering Point relating to the export of electricity from a premises.
Export Supplier	means, for a Smart Metering System or a Device and any period of or point in time, the Supplier Party Registered during that period of or at that point in time in respect of the Export MPAN relating to that Smart Metering System or Device (but excluding Smart Metering Systems or Devices for which there is no related Import MPAN, in which circumstance such Registered Supplier Party is deemed to be the Import Supplier in accordance with the definition thereof).
Fast-Track Modifications	has the meaning given to that expression in Section D2.8 (Fast-Track Modifications).

File Signing Certificate	has the meaning given to that expression in the IKI Certificate Policy.
Firmware Hash	means the result of the application of a hash function, such function being a repeatable process to create a fixed size and condensed representation of a message using the SHA-256 algorithm as specified in the US Government's Federal Information Processing Standards document 180-4.
Fixed Charges	has the meaning given to that expression in the Charging Methodology.
Follow-up Security Assessment	has the meaning given to that expression in Section G8.19 (Categories of Security Assurance Assessment).
Force Majeure	means, in respect of any Party (the **Affected Party**), any event or circumstance which is beyond the reasonable control of the Affected Party, but only to the extent such event or circumstance (or its consequences) could not have been prevented or avoided had the Affected Party acted in accordance with Good Industry Practice. Neither lack of funds nor strikes or other industrial disturbances affecting only the employees of the Affected Party and/or its contractors shall be interpreted as an event or circumstance beyond the Affected Party's control.
Forum Sub-Group	has the meaning given to that expression in Section Z6.1 (Definitions).
Framework Agreement	means an agreement in the form set out in Schedule 1.
Full Privacy Assessment	has the meaning given to that expression in Section I2.12 (Categories of Assessment).

Full User Security Assessment	has the meaning given to that expression in Section G8.16 (Categories of Security Assurance Assessment).
Future-Dated Services	has the meaning given to that expression in Section H3.11 (Categories of Services).
Gas Act	means the Gas Act 1986.
Gas Meter	means a meter that conforms to the requirements of section 17(1) of the Gas Act for the purpose of registering the quantity of gas supplied through pipes to premises.
Gas Network Party	means a Party that holds a Gas Transporter Licence.
Gas Proxy Function	means that part of a device installed (or to be installed) at a premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other requirements of, a version of the CHTS (but only those provisions that are described as applying to 'Gas Proxy Functions') which was a Valid Technical Specification on the date on which the device was installed.
Gas Smart Meter	means a device installed (or to be installed) at a premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability

specified by and complies with the other requirements of,

the part(s) of the SMETS identified as applying to 'Gas Smart Metering Equipment' in a version of the SMETS which was a Valid Technical Specification on the date on which the device was installed. Devices that meet the requirements of the version of the SMETS that was designated on 18 December 2012 (and amended and restated on 31 March 2014) are not currently included within this definition.

Gas Supplier	means, for a Smart Metering System or a Device and any period of or point in time, the Supplier Party Registered during that period of or at that point in time in respect of the MPRN relating to that Smart Metering System or Device.
Gas Supplier Party	means a Party that holds a Gas Supply Licence (regardless of whether that Party also holds an Electricity Supply Licence).
Gas Supply Licence	means a licence granted, or treated as granted, pursuant to section 7A(1) of the Gas Act.
Gas Transporter	means, for a Smart Metering System or a Device, the holder of the Gas Transporter Licence for the network to which the relevant premises are connected.
Gas Transporter Licence	means a licence granted, or treated as granted, under section 7 of the Gas Act (but not the licence in respect of the National Transmission System, as defined in the UNC).

GB Companion Specification (or "GBCS")	means the document of that name set out in Schedule [TBC].
GBCS Payload	means the content of a Pre-Command, Signed Pre-Command, Service Response or Device Alert which is set out in the format required by the GB Companion Specification.
General SEC Objectives	has the meaning given to that expression in Section C1 (SEC Objectives).
Good Industry Practice	means, in respect of a Party, the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in a similar type of undertaking as that Party under the same or similar circumstances.
Greenhouse Gas Emissions	means emissions of Greenhouse Gases, as defined in section 92 of the Climate Change Act 2008.
HAN	means, for each Smart Metering System, the home area network created by the Communications Hub Function forming part of that Smart Metering System.
HAN Connected Auxiliary Load Control Switch	means a device installed (or to be installed) at a premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other requirements of, a version of the HCALCS Technical Specification which was a Valid Technical Specification on the date

	on which the device was installed.
HAN Requirements	means the requirements with respect to the HAN provided for in the Energy Licences and this Code.
HAN Variants	means the variations of Communications Hub that are necessary to enable communication via each HAN Interface (as defined in the CHTS).
Hash	means the result of the application of a hash function, such function being a repeatable process to create a fixed size and condensed representation of a message using the SHA-256 algorithm as specified in the US Government's Federal Information Processing Standards document 180-4.
HCALCS	means a HAN Connected Auxiliary Load Control Switch.
HCALCS Technical Specification	means the part(s) of the SMETS identified as applying to 'HAN Connected Auxiliary Load Control Switches'.
ICA Certificate	has the meaning given to that expression in the IKI Certificate Policy.
ICHIS	means the Intimate Communications Hub Interface Specifications.
ID Allocation Procedure	means the document of that name developed and maintained in accordance with Section B2.2 (ID Allocation Procedure).
IETF RFC 5280	has the meaning given to that expression in the GB Companion Specification.
IHD	means a device provided (or to be provided) at a

	premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other requirements of, a version of the IHD Technical Specification which was a Valid Technical Specification on the date on which the device was provided, and which a User acting in the role of Import Supplier or Gas Supplier has joined, or is seeking to join, to an Electricity Smart Meter or Gas Proxy Function (as applicable).
IHD Technical Specification	means the part(s) of the SMETS identified as applying to 'IHDs'.
IKI Authority Revocation List (or **IKI ARL**)	has the meaning given to that expression in the IKI Certificate Policy.
IKI Certificate	has the meaning given to that expression in the IKI Certificate Policy.
IKI Certificate Policy	means the SEC Subsidiary Document of that name set out in Appendix [TBD].
IKI Certificate Revocation List (or **IKI CRL**)	has the meaning given to that expression in the IKI Certificate Policy.
IKI Certification Practice Statement (or **IKI CPS**)	has the meaning given to that expression in Section L9.20 (the IKI Certification Practice Statement).
Import MPAN	means an MPAN for a Metering Point relating to the import of electricity to a premises.

Import Supplier	means, for a Smart Metering System or a Device and any period of or point in time: (a) the Supplier Party Registered during that period of or at that point in time in respect of the Import MPAN relating to that Smart Metering System or Device; or (b) where there is no related Import MPAN for that Smart Metering System or Device, the Supplier Party Registered during that period of or at that point in time in respect of the Export MPAN relating to that Smart Metering System or Device.
Incident	means an actual or potential interruption to (or reduction in the quality or security of) the Services, as further described in the Incident Management Policy.
Incident Category	has the meaning given to that expression in Section H9.1 (Incident Management Policy).
Incident Management	means a framework of processes designed to identify, raise, allocate responsibility for, track and close Incidents.
Incident Management Log	has the meaning given to that expression in Section H9.3 (Incident Management Log).
Incident Management Policy	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
Incident Parties	has the meaning given to that expression in Section H9.1 (Incident Management Policy).
Independent Assurance	has the meaning given to that expression in Part 2.1 of

Scheme	the SMKI Compliance Policy (DCC: Duty to Submit to an Independent Assurance Scheme).
Independent Privacy Auditor	has the meaning given to that expression in Section I2.1 (Procurement of the Independent Privacy Auditor).
Independent SMKI Assurance Service Provider	has the meaning given to that expression in Part 3.1 of the SMKI Compliance Policy (DCC: Duty to Procure Independent Assurance Services).
Independent Time Source	has the meaning given to that expression in Section G2.~~38~~41(b) (Network Time).
Information Classification Scheme	means a methodology for: (a) the appropriate classification of all Data that are processed or stored on a System by reference to the potential impact of those Data being Compromised; and (b) determining the controls to be applied to the processing, storage, transfer and deletion of each such class of those Data.
Information Commissioner	means the Commissioner, as defined in the Data Protection Act.
Infrastructure Key Infrastructure (or IKI)	means the public key infrastructure established by the DCC for the purpose, among other things, of authenticating communications between: (a) Parties and the OCA and DCA; and (b) Parties and the DCC, where those Parties are required in accordance with this Code to provide files to the DCC that have been Digitally Signed using the Private Key

associated with the Public Key that is contained within a File Signing Certificate.

Insolvency Type Event means, in respect of a Party, that that Party:

(a) is unable to pay its debts as they fall due, or is deemed to be unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 (but as if the reference in such section to "£750" was replaced with "£10,000");

(b) calls a meeting for the purpose of passing a resolution for its winding-up, or such a resolution is passed;

(c) presents, or has presented in respect of it, a petition for a winding-up order;

(d) has an application to appoint an administrator made in respect of it, or a notice of intention to appoint an administrator is filed in respect of it;

(e) has an administrator, administrative receiver, or receiver appointed over all or a substantial part of its business, undertaking, property or assets;

(f) takes any steps in connection with proposing a company voluntary arrangement or a company voluntary arrangement is passed in relation to it; or

(g) suffers or undergoes any procedure analogous to any of those specified above, including in respect of a Party who is a natural person or in any jurisdiction outside the UK in which a Party is incorporated.

Intellectual Property Rights means patents, trade marks, trade names, service

	marks, rights in designs, copyright (including rights in computer software), logos, rights in internet domain names, and moral rights, database rights, rights in know-how, and other intellectual property rights (in each case, whether registered or unregistered or subject to an application for registration), and includes any and all rights or forms of protection having equivalent or similar effect anywhere in the world.
Interface Testing	means the testing described in Section T3 (Interface Testing).
Interface Testing Approach Document	has the meaning given to that expression in Section T3.8 (Interface Testing Approach Document).
Interface Testing Objective	has the meaning given to that expression in Section T3.2 (Interface Testing Objective).
Interim Election	has the meaning given to that expression in Section C4.2 (Election of Elected Members).
Intimate Communications Hub Interface Specifications	means the specifications described as such and originally developed by the DCC pursuant to schedule 3 of the DCC Licence, as amended from time to time in accordance with Section H12.9 (Amendments to the ICHIS).
Inventory Enrolment and Withdrawal Procedures	means the SEC Subsidiary Document of that name set out as Appendix [TBC].
Invoice	has the meaning given to that expression in Section J1.2 (Invoicing of Charges).
Issue	in relation to: (a) a Device Certificate or DCA Certificate, has the

meaning given to that expression in Annex A of the Device Certificate Policy;

(b) an Organisation Certificate or OCA Certificate, has the meaning given to that expression in Annex A of the Organisation Certificate Policy;

(c) an IKI Certificate or ICA Certificate has the meaning given to that expression in the IKI Certificate Policy;

(d) a DCCKI Certificate (including any DCCKICA Certificate) has the meaning given to that expression in the DCCKI Certificate Policy.

Issuing DCA has the meaning given to that expression in Annex A of the Device Certificate Policy.

Issuing DCA Certificate has the meaning given to that expression in Annex A of the Device Certificate Policy.

Issuing ICA has the meaning given to that expression in the IKI Certificate Policy.

Issuing ICA Certificate has the meaning given to that expression in the IKI Certificate Policy.

Issuing OCA has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Issuing OCA Certificate has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Key Pair means a Private Key and its mathematically related Public Key, where the Public Key may be used to Check Cryptographic Protection in relation to a communication that has been Digitally Signed using

	the Private Key.
Known Remote Party	has the meaning given to that expression in the GB Companion Specification.
Large Supplier Party	means a Supplier Party that is not a Small Supplier Party.
Laws and Directives	means any law (including the common law), statute, statutory instrument, regulation, instruction, direction, rule, condition or requirement (in each case) of any Competent Authority (or of any authorisation, licence, consent, permit or approval of any Competent Authority).
Lead Supplier	means, in respect of a Communications Hub: (a) where there is only one Responsible Supplier for the Communications Hub Function which forms part of that Communications Hub, that Responsible Supplier; or (b) where there is more than one Responsible Supplier for the Communications Hub Function which forms part of that Communications Hub, the Import Supplier for the Communications Hub Function.
Letter of Credit	means an unconditional irrevocable standby letter of credit in substantially the form set out in Schedule 6 from a bank with the Required Bank Rating which letter of credit has not been breached or disclaimed by the provider.
Liability	includes any loss, liability, damages, costs (including

	legal costs), expenses and claims.
Local Command Services	means the sending of Commands to a User via the DCC User Interface where the User has opted in the Service Request for the Command to be sent in that way.
Maintenance	includes repair, replacement, upgrade or modification.
Major Incident	means an Incident that is categorised as a major incident in accordance with the Service Management Standards, as further described in the Incident Management Policy.
Major Security Incident	means, in relation to any System, any event which results, or was capable of resulting, in that System being Compromised to a material extent.
Malicious Software	means any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on Data, software, files, programs or codes (whether or not its operation is immediate or delayed, and whether it is introduced wilfully, negligently or without knowledge of its existence).
Manufacturer	means, in respect of any Device Model, the person: (a) that manufactures some or all of the Devices of that Device Model; or (b) on whose behalf some or all of those Devices are manufactured for onward sale or other provision.
Manufacturer Image	has the meaning given to that expression in the GB Companion Specification.
Manufacturer Release	means, in respect of any hardware version or firmware version in a Device Model, the Manufacturer's notes

Notes	regarding the description of the features provided by that hardware version or firmware version (and, where relevant, how and why this differs from other Device Models where this difference arises only by virtue of having newer versions of hardware and/or firmware). Such description of differences shall include the reasons for the newer version(s), a description of any enhancements to the features provided by the newer version(s), a description of any fixes to existing features, and a statement on backwards and forwards compatibility of any new firmware version.
MA-S Registry Entry	means a publicly registered 36-bit identifier of that name issued by the Institute of Electrical and Electronics Engineers Standards Association.
Material Risk	means, in respect of any Maintenance of the DCC Systems, that such Maintenance poses either: (a) a material risk of disruption ~~to the Services~~; or (b) a risk of material disruption ~~to the Services~~.
Mesh Communications Hub	has the meaning given to that expression in the CH Support Materials.
Message Authentication Code	has the meaning given to that expression in the GB Companion Specification (or, where used in the context of a communication not specified by the GB Companion Specification, the meaning associated with the relevant cryptographic algorithm used to generate it).
Message Mapping	means the SEC Subsidiary Document of that name set

Catalogue	out in Appendix [TBC].
Meter Asset Manager	has the meaning given to that expression in the SPAA.
Meter Operator	has the meaning given to that expression in the MRA.
Metering Point	has the meaning given to that expression in the MRA.
Minimum Monthly Charge	means, in respect of each Regulatory Year, £25.00, multiplied by the Consumer Prices Index for the October preceding the start of that Regulatory Year, divided by the Consumer Prices Index for October 2014. The relevant amount will be rounded to the nearest pound.
Minimum Service Level	means, in respect of each Performance Measure, the number or percentage intended to represent the minimum level of performance for the activity which is the subject of the Performance Measure, as set out in: (a) Section H13.1 (Code Performance Measures); (b) the Reported List of Service Provider Performance Measures; or (c) Section L8.6 (Code Performance Measures).
Modification Proposal	has the meaning given to that expression in Section D1.2 (Modifications).
Modification Register	has the meaning given to that expression in Section D1.8 (Modification Register).
Modification Report	has the meaning given to that expression in Section D7.1 (Modification Report).
Modification Report	has the meaning given to that expression in Section

Consultation	D7.8 (Modification Report Consultation).
Monthly Service Metric	has the meaning set out in the DCC User Interface Services Schedule.
Monthly Service Threshold	has the meaning set out in the DCC User Interface Services Schedule.
MPAN	means, in respect of a Smart Metering System (or Electricity Meter), the Supply Number (or each of the Supply Numbers) allocated under the MRA to the Metering Point(s) at which the import or export of electricity is recorded by that Smart Metering System (or Electricity Meter).
MPRN	means, in respect of a Smart Metering System (or Gas Meter), the Supply Meter Point Reference Number allocated by the relevant Gas Network Party to the Supply Meter Point at which the supply of gas is recorded by that Smart Metering System (or Gas Meter).
MRA	means the Master Registration Agreement established pursuant to the Electricity Distribution Licences.
Network Enhancement Plan	means a plan by the DCC to undertake works to improve SM WAN connectivity for a cohort of Communications Hubs installed within a particular geographic area (in either the south Region or the central Region), where the DCC has obtained reasonable evidence to justify that the works are required in order to improve SM WAN connectivity.
Network Party	means a Party that is either an Electricity Network Party or a Gas Network Party.

Network Time	has the meaning given to that expression in Section G2.~~38~~41(a) (Network Time).
New Party	means a Party that is a Party pursuant to an Accession Agreement.
Non-Critical Service Request	means a Service Request which is not identified as critical in the DCC User Interface Services Schedule (or, in the case of Elective Communication Services, the relevant Bilateral Agreement).
Non-Critical Service Response	means a Service Response in respect of a Non-Critical Service Request.
Non-Default Interest Rate	means, for any day, the base lending rate of the Bank of England at 13.00 hours on that day.
Non-Device Service Request	means a Service Request in respect of a Service identified as a non-device service in the DCC User Interface Services Schedule (or, in the case of Elective Communication Services, the relevant Bilateral Agreement).
Non-Domestic Premises	means premises other than Domestic Premises.
Notification	means, in respect of a Modification Proposal, notification of that modification to the EU Commission pursuant to EU Directive 98/34/EC.
NSA Suite B Cryptographic Algorithm	means a cryptographic algorithm that meets the standards required by the US National Security Agency's suite B cryptography standards (www.nsa.gov/ia/programs/suiteb_cryptography/).
OCA Certificate	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

On-Demand Services	has the meaning given to that expression in Section H3.11 (Categories of Services).
Organisation Authority Revocation List (or Organisation ARL)	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.
Organisation Certificate	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.
Organisation Certificate Policy	means the SEC Subsidiary Document of that name set out in Appendix B.
Organisation Certificate Revocation List (or **Organisation CRL**)	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.
Organisation Certification Authority (or **OCA**)	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.
Organisation Certification Practice Statement (or **Organisation CPS**)	has the meaning given to that expression in Section L9.14 (the Organisation Certification Practice Statement).
Original Party	means a Party that is a Party pursuant to the Framework Agreement.
OTA Header	has the meaning given to that expression in the GB Companion Specification.
Other Enabling Services	means the Services other than the Enrolment Services, the Communications Hub Services and the Communication Services.
Other SEC Party	means a Party that is not the DCC, is not a Network Party, and is not a Supplier Party.

Other User	means, for a Smart Metering System or a Device and any period of or point in time, a User that is not acting in the User Role of Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter or Registered Supplier Agent (regardless of whether in fact that User is a Responsible Supplier or the Electricity Distributor or the Gas Transporter or the Registered Supplier Agent during that period of or at that point in time).
Panel	means the body established as such in accordance with Section C2.1 (Establishment of the Panel).
Panel Chair	has the meaning given to that expression in Section C3.1 (Composition of the Panel).
Panel Member	has the meaning given to that expression in Section C3.1 (Composition of the Panel).
Panel Objectives	has the meaning given to that expression in Section C2.2 (Panel Objectives).
Panel Release Management Policy	has the meaning given to that expression in Section D10.7 (Release Management).
Parent Company Guarantee	means a guarantee in such form as the DCC may reasonably approve from an Affiliate of the User in question which guarantee has not been breached or disclaimed by the guarantor and has at least one month left until it expires. Where the guarantor is incorporated outside of the United Kingdom, the guarantee will only be validly given where supported by a legal opinion regarding capacity and enforceability in a form reasonably satisfactory to the

	DCC.
Parse and Correlate Software	has the meaning given to that expression in Section H11.1 (Provision of Parse and Correlate Software).
Party	means, from time to time, a person that has agreed to be bound by this Code (either pursuant to the Framework Agreement or an Accession Agreement), and (without prejudice to Section M8.14 (Consequences of Ceasing to be a Party)) that has not at that time ceased to be so bound in accordance with Section M8 (but excluding SECCo).
Party Category	means, as the context requires, one of the following categories: (a) the Large Supplier Parties collectively; (b) the Small Supplier Parties collectively; (c) the Electricity Network Parties collectively; (d) the Gas Network Parties collectively; and (e) the Other SEC Parties collectively.
Party Data	has the meaning given to that expression in Section M5.10 (Party Data).
Party Details	means, in respect of each Party, the information relating to that Party and corresponding to the heads of information set out in the Application Form from time to time.
Party Signifier	means an identification number allocated to a Party by the Code Administrator pursuant to Section B1.17 (Party Signifiers), which uniquely identifies that Party under the Code.

Path 1 Modification	has the meaning given to that expression in Section D2.4 (Path 1 Modification: Authority-led).
Path 2 Modification	has the meaning given to that expression in Section D2.6 (Path 2 Modification: Authority Determination).
Path 3 Modification	has the meaning given to that expression in Section D2.7 (Path 3 Modification: Self-Governance).
Performance Measurement Methodology	means a documented methodology for establishing the performance against each Performance Measure, which may include sampling and/or test communications.
Performance Measurement Period	means, in respect of each Performance Measure, the applicable period over which the Service Level for that Performance Measure is to be measured, as set out in: (a) Section H13.1 (Code Performance Measures); (b) the Reported List of Service Provider Performance Measures; or (c) Section L8.6 (Code Performance Measures).
Performance Measures	means the Code Performance Measures and such Service Provider Performance Measures as are specified in the Reported List of Service Provider Performance Measures.
Permitted Communication Service	means, in respect of a User and a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System): (a) a service that results in the sending of a Command to a Device (other than the Communications Hub Function) for which the

User is the Responsible Supplier (except where, were the Command to be sent as a Core Communication Service, it would be a Critical Command requiring another User's Digital Signature);

(b) a service that only results in the sending of a Command to a Device which is the same as a Command which results from a Service listed in the DCC User Interface Services Schedule for which that User is an Eligible User; or

(c) a service which the Panel has (on the application of the User) approved as a permitted communication service.

Personal Data means personal data, as defined in the Data Protection Act.

Physical Device Type means, in respect of a device, its type which may be only one of: a Communications Hub; a Single Element Electricity Metering Equipment (as defined in SMETS); a Twin Element Electricity Metering Equipment (as defined in SMETS); a Polyphase Electricity Metering Equipment (as defined in SMETS), a Gas Smart Meter; a Pre-Payment Meter Interface Device; a HAN Connected Auxiliary Load Control Switch; an IHD; or a Type 2 Device (Other).

Planned Maintenance means, in respect of a month, Maintenance of the DCC Systems planned prior to the start of that month and which will disrupt, or poses a Material Risk of disruption to, provision of the Services (and, where it will disrupt, or poses a Material Risk of disruption to, the provision of the Services in relation to Devices

	associated with Communications Hubs, at least 100,000 Communications Hubs are affected).
Point-to-Point Alt HAN Equipment	has the meaning given to that expression in accordance with standard condition 55 of the Electricity Supply Licence (Smart Metering – The Alt HAN Arrangements) and standard condition 49 of the Gas Supply Licence (Smart Metering – The Alt HAN Arrangements).
Post Commissioning Information	has the meaning given to that expression in the Inventory Enrolment and Withdrawal Procedures.
PPMID	means a Prepayment Meter Interface Device.
PPMID Technical Specification	means the part(s) of the SMETS identified as applying to 'Pre-Payment Meter Interface Devices'.
Pre-Command	means a communication (other than a Service Response or Device Alert) to be sent from the DCC to a User or to the CoS Party that includes a GBCS Payload and which has been Digitally Signed by the DCC in accordance with the DCC User Interface Specification.
Preliminary Assessment	has the meaning given to that expression in Section H7.4 (Preliminary Assessment of Elective Communication Services).
Pre-Payment Meter Interface Device	means a device installed (or to be installed) at a premises, which: (a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other

	requirements of, a version of the PPMID Technical Specification which was a Valid Technical Specification on the date on which the device was installed.
Principal User Security Obligations	has the meaning given to that expression in Section G1.7 (Obligations on Users).
Privacy Assessment	means a Full Privacy Assessment, Random Sample Privacy Assessment or User Privacy Self-Assessment.
Privacy Assessment Report	has the meaning given to that expression in Section I2.19 (The Privacy Assessment Report).
Privacy Assessment Response	has the meaning given to that expression in Section I2.21 (The Privacy Assessment Response).
Privacy Controls Framework	means the document of that name developed and maintained by the Panel in accordance with Section I2.15 (The Privacy Controls Framework).
Privacy Self-Assessment	has the meaning given to that expression in Section I2.14 (Categories of Assessment).
Privacy Self-Assessment Report	has the meaning given to that expression in Section I2.26 (The User Privacy Self-Assessment Report).
Private Key	means the private part of an asymmetric Key Pair used for the purposes of public key encryption techniques
Privileged Person	means a member of DCC Personnel who is authorised to carry out activities which involve access to resources, or Data held, on the DCC Total System and which are capable of being a means by which the DCC Total System, any User Systems, any RDP Systems or

	any Device are Compromised to a material extent.
Problem	means the underlying cause of one or more Incidents, as further described in the Incident Management Policy.
Process	means, in respect of any Personal Data, to 'process' that Personal Data, as defined in the Data Protection Act (and "**Processing**" shall be interpreted accordingly).
Product Recall or Technology Refresh	has the meaning given to that expression in Section F9.6 (Categories of Responsibility).
Projected Operational Service Levels	[TBC] [*For a discussion of this term, please refer to the SEC3 Consultation Document.*]
Proposer	has the meaning given to that expression in Section D1.3 (Persons Entitled to Propose Modification Proposals).
Prototype Communications Hub	means a device that as closely achieves compliance with the CHTS as is reasonably practicable from time to time, which is provided (or to be provided) for the purpose of testing as described in Section F10 (Test Communications Hubs).
Public Key	means the public part of an asymmetric Key Pair used for the purposes of public key encryption techniques.
Random Sample Privacy Assessment	has the meaning given to that expression in Section I2.13 (Categories of Assessment).
RDP	means Registration Data Provider.
RDP ID	means, in respect of an RDP acting in its capacity as such (including a Network Party where it is deemed to

have nominated itself for that role), one of the unique identification numbers accepted by the DCC in respect of that RDP under Section E2.16 (Security Obligations and RDP IDs).

RDP Signifier means an identification number allocated to an RDP by the Code Administrator pursuant to Section B1.19 (RDP Signifiers), which uniquely identifies that RDP under the Code.

RDP Systems means any Systems:

(a) which are operated by or on behalf of an Electricity Distributor or Gas Transporter responsible for providing (or procuring the provision of) Registration Data in respect of a particular MPAN or MPRN; and

(b) which are used in whole or in part for:

(i) the collection, storage, Back-Up, processing or communication of that Registration Data prior to, or for the purposes of, its provision to the DCC over the Registration Data Interface;

(ii) generating Data for communication to the OCA, DCA, ICA or DCCKICA, or receiving Data from the OCA, DCA, ICA or DCCKICA (including any Systems which store or use Secret Key Material for such purposes); and/or

(iii) generating Data for the purposes of lodging in the SMKI Repository or DCCKI Repository, or retrieving Data from the SMKI Repository or DCCKI

	Repository, and any other Systems from which the Systems described in paragraphs (a) and (b) are not Separated.
Recoverable Costs	has the meaning given to that expression in Section C8.2 (SEC Costs and Expenses).
Recovery Certificate	has the meaning given to that expression in Section L10.30(d)(ii) (Definitions).
Recovery Costs	has the meaning given to that expression in Section L10.17 (Recovery Costs).
Recovery Event	has the meaning given to that expression in Section L10.14 (Recovery Events).
Recovery Key Pair	has the meaning given to that expression in Section L10.30(d) (Definitions).
Recovery Private Key	has the meaning given to that expression in Section L10.30(d)(i) (Definitions).
Refinement Process	has the meaning given to that expression in Section D6 (Refinement Process).
Region	means each of the regions of Great Britain that are subject to different DCC Service Provider Contracts, and the region into which a premises (or future potential premises) falls shall be: (a) identified insofar as reasonably practicable in a document published by the DCC (or the Panel on behalf of the DCC) from time to time; or (b) where a premises (or future potential premises) is not so identified, confirmed by the DCC on application of any Party or in response to the

resolution of an Incident regarding the fact that a premises (or future potential premises) is not so identified,

and once a premises has been identified by the DCC as being in a particular region, the DCC shall not identify that premises as being in a different region (unless agreed by the Supplier Party or Supplier Parties Registered for the MPAN and/or MPRN at the premises and the Network Party or Network Parties for the network(s) to which the premises is, or is intended to be, connected).

Registered means Registered, as defined in the MRA or the SPAA, as applicable (and "**Registration**" shall be interpreted accordingly).

Registered Supplier Agent means, for a Smart Metering System or a Device and any period of or point in time, the User that is:

(a) in the case of electricity, appointed as the Meter Operator in respect of the MPAN relating to that Smart Metering System or Device; or

(b) in the case of gas, appointed as the Meter Asset Manager in respect of the MPRN relating to that Smart Metering System or Device,

(in either case) during that period of or at that point in time.

Registration Authority means the DCC, acting in its capacity as such for the purposes of (and in accordance with the meaning given to that expression in any) of the Certificate Policies.

Registration Data	has the meaning given to that expression in Section E1 (Reliance on Registration Data).
Registration Data Interface	means the communications interface designed to allow the communications referred to in Section E (Registration Data) to be sent between the DCC and the Registration Data Providers.
Registration Data Interface Code of Connection	means the SEC Subsidiary Document of that name to be incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).
Registration Data Interface Documents	means the Registration Data Interface Code of Connection and Registration Data Interface Specification.
Registration Data Interface Specification	means the SEC Subsidiary Document of that name to be incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).
Registration Data Provider	means, in respect of each Network Party, the person nominated as such in writing to the DCC from time to time by that Network Party, on the basis that more than one Party may specify the same Registration Data Provider, and that the Network Party shall be deemed to have so nominated itself in the absence of any other nomination.
Regulatory Year	means a period of twelve months beginning at the start of 1 April in any calendar year and ending at the end of 31 March in the next following calendar year.
Related Person	means, in relation to an individual, that individual's spouse, civil partner, parent, grandparent, sibling, child, grandchild or other immediate family member;

	any partner with whom that individual is in partnership; that individual's employer; any Affiliate of such employer; any person by whom that individual was employed in the previous 12 months; and any company (or Affiliate of a company) in respect of which that individual (individually or collectively with any member of his immediate family) controls more than 20% of the voting rights.
Release Management	means the process adopted for planning, scheduling and controlling the build, test and deployment of releases of IT updates, procedures and processes.
Relevant Device	has the meaning given to that expression in Section L10.30(a) (Definitions).
Relevant Instruments	means: (a) the Electricity Act and the Gas Act; (b) the Data Protection Act; (c) the Energy Licences; and (d) the Energy Codes.
Relevant Private Key	has the meaning given to that expression in Section L10.30(c) (Definitions).
Relevant Subscriber	has the meaning given to that expression in Section L10.30(b).
Relying Party	means a person who, pursuant to the Code, receives and relies upon a Certificate.
Relying Party Obligations	means the provisions in respect of Relying Parties set out at Section L12 of the Code (the Relying Party Obligations).

Remote Party Role	has the meaning given to that expression, and comprises the values allowed for the ASN.1 type RemotePartyRole identified, in the GB Companion Specification.
Report Phase	has the meaning given to that expression in Section D7.1 (Modification Report).
Reported List of Service Provider Performance Measures	means the document which: (a) is initially provided to Parties, the Panel and the Authority by the Secretary of State, bears the title 'Reported List of Service Provider Performance Measures' and identifies itself as being produced for the purposes of Section H13 (Performance Standards and Reporting); and (b) specifies a number of Service Provider Performance Measures together (in each case) with the applicable Service Level Requirement, Target Service Level, Minimum Service Level and Performance Measurement Period, as it may be modified from time to time in accordance with Section H13.2 (Service Provider Performance Measures).
Required Bank Rating	means that a person has one or more long-term Recognised Credit Ratings of at least (based, where the person has more than one such rating, on the lower of the ratings): (a) "A-" by Standard & Poor's Financial Services LLC; (b) "A3" by Moody's Investors Services Inc; and/or

(c) "A-" by Fitch Ratings Limited; and/or

(d) "A(low)" by DBRS Ratings Limited.

Response has the meaning given to that expression in the GB Companion Specification.

Responsible Supplier means, in respect of a Smart Metering System (or any Device forming, or intended to form, part of a Smart Metering System) which relates to:

(a) an MPAN, the Import Supplier for that Smart Metering System; and/or

(b) an MPRN, the Gas Supplier for that Smart Metering System.

Restricted Communication Service means, in respect of any User requesting an Elective Communication Service, a service which is not a Permitted Communication Service.

Risk Treatment Plan has the meaning given to that expression in Section G7.16(e) (Duties and Powers of the Security Sub-Committee).

Root DCA has the meaning given to that expression in Annex A of the Device Certificate Policy.

Root DCA Certificate has the meaning given to that expression in Annex A of the Device Certificate Policy.

Root DCCKICA Certificate has the meaning given to that expression in the DCCKI Certificate Policy

Root ICA has the meaning given to that expression in the IKI Certificate Policy.

Root ICA Certificate has the meaning given to that expression in the IKI

	Certificate Policy.
Root OCA	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.
Root OCA Certificate	has the meaning given to that expression in Annex A of the Organisation Certificate Policy.
Scheduled Election	has the meaning given to that expression in Section C4.2 (Election of the Elected Members).
Scheduled Services	has the meaning given to that expression in Section H3.11 (Categories of Services).
SEC Arrangements	has the meaning given to that expression in the DCC Licence.
SEC Materials	has the meaning given to that expression in Section M5.1 (SEC Materials).
SEC Objectives	means, in respect of the Charging Methodology only, the Charging Objectives and, in all other cases, the General SEC Objectives.
SEC Subsidiary Documents	means each of the documents set out as such in the appendices to this Code.
SECCo	has the meaning given to that expression in Schedule 4.
Secret Key Material	means any Private Key, Shared Secret, Symmetric Key or other functionally equivalent cryptographic material (and any associated input parameter) that is generated and maintained by a Party or RDP for the purposes of complying with its obligations under, or in relation to, this Code, but excluding:

(a) any such material (and associated input parameters) to the extent that it is maintained on Devices;

(b) any Digital Signature; and

(c) any output of a Cryptographic Hash Function operating on an input communication.

Secretariat has the meaning given to that expression in Section C7.6 (Secretariat).

Secretary of State has the meaning given to that expression in the Interpretation Act 1978.

Security Check means the vetting of personnel, carried out to a level that is identified by that name, under and in accordance with the HMG National Security Vetting Procedures.

Security Controls Framework has the meaning given to that expression in Section G7.16(a) (Duties and Powers of the Security Sub-Committee).

Security Obligations and Assurance Arrangements means:

(a) in the case of the DCC Total System, those requirements set out in Sections G2, G4 to G7 and G9;

(b) in the case of User Systems, those requirements set out in Sections G3 to G8;

(c) in the case of Smart Metering Systems, those requirements set out in the Security Characteristics (as defined in the relevant Technical Specification); and

(d) in the case of RDP Systems, those

	requirements set out in Section E2.14 (Security Obligations).
Security Requirements	means a document that: (a) identifies the security controls that are considered appropriate to mitigate the security risks relating to the End-to-End Smart Metering System; and (b) indicates those provisions having effect (or being proposed to have effect) in or under the Security Obligations and Assurance Arrangements or any Energy Licences which require that such security controls are established and maintained.
Security Risk Assessment	means a document that identifies, analyses and evaluates the security risks which relate to the End-to-End Smart Metering System.
Security Sub-Committee	means the Sub-Committee established pursuant to Section G7 (Security Sub-Committee).
Security Sub-Committee (Network) Members	has the meaning given to that expression in Section G7.8 (Membership of the Security Sub-Committee).
Security Sub-Committee (Other User) Member	has the meaning given to that expression in Section G7.10 (Membership of the Security Sub-Committee)
Security Sub-Committee (Supplier) Members	has the meaning given to that expression in Section G7.6 (Membership of the Security Sub-Committee).
Security Sub-Committee Chair	has the meaning given to that expression in Section G7.5 (Membership of the Security Sub-Committee).
Security Sub-Committee Member	has the meaning given to that expression in Section G7.3 (Membership of the Security Sub-Committee).

Self-Service Interface	has the meaning given to that expression in Section H8.15 (Self-Service Interface).
Self-Service Interface Code of Connection	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
Self-Service Interface Design Specification	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
Separate	means, in relation to any System, software or firmware, to establish controls which are appropriately designed to ensure that no communication may take place between it and any other System, software or firmware (as the case may be) except to the extent that such communication is for a necessary purpose having regard to the intended operation of the System, software or firmware (and "**Separated**" and "**Separation**" are to be interpreted accordingly).
Sequenced Services	has the meaning given to that expression in Section H3.13 (Sequenced Services).
Service Desk	has the meaning given to that expression in Section H8.19 (Service Desk).
Service Level	means, in respect of each Performance Measure and each Performance Measurement Period: (a) where that Performance Measure relates to an activity that is performed on a number of separate occasions: (i) the number of occasions during the Performance Measurement Period on which that activity was performed in accordance with the relevant Service

Level Requirement,

expressed as a percentage of, or a number in relation to:

(ii) the total number of occasions during the Performance Measurement Period on which that activity was performed;

(b) where that Performance Measure relates to an activity that is performed over a period of time:

(i) the period of time during the Performance Measurement Period on which that activity was performed,

expressed as a percentage of:

(ii) the period of time during the Performance Measurement Period on which that activity would have been performed if it had been performed in accordance with the relevant Service Level Requirement,

provided that in each case the DCC may establish the Service Level for a Performance Measure in accordance with the Performance Measurement Methodology.

Service Level Requirements means:

(a) in respect of each Code Performance Measure, the Target Response Time, Target Resolution Time or Target Availability Time (applicable in accordance with the table at Section H13.1 (Code Performance Measures) or at Section L8.6 (Code Performance Measures)); or

	(b) in respect of each Service Provider Performance Measure, the standard to which the relevant DCC Service Provider is obliged by its DCC Service Provider Contract to perform the activity that is the subject of the Service Provider Performance Measure.
Service Management Standards	means the Information Technology Infrastructure Library (ITIL®) standards for IT services management, as issued and updated by the Cabinet Office from time to time.
Service Provider Performance Measures	means the performance measures (however described and from time to time) for each DCC Service Provider under each DCC Service Provider Contract.
Service Request	means a request for one of the Services listed in the DCC User Interface Services Schedule (or, in the case of Elective Communication Services, provided for in the relevant Bilateral Agreement).
Service Request Processing Document	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
Service Response	means, in respect of a Service Request sent by a User, one or more communications in response to that Service Request from the DCC to the User (not being a Pre-Command).
Services	means the services provided, or to be provided, by the DCC pursuant to Sections F5 (Communications Hub Forecasts and Orders) to F10 (Test Communications Hubs), Section H (DCC Services), or Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure), including pursuant to Bilateral

	Agreements.
Services FM	means, in respect of any Services, the occurrence of any of the following: (a) war, civil war, riot, civil commotion or armed conflict; (b) terrorism (being the use or threat of action designed to influence the government or intimidate the public or for the purpose of advancing a political, religious or ideological cause and which involves serious violence against a person or serious damage to property, endangers a person's life, creates a serious risk to the public or is designed to seriously interfere with or disrupt an electronic system); (c) nuclear, chemical or biological contamination; (d) earthquakes, fire, storm damage or severe flooding (if in each case it affects a significant geographical area); and/or (e) any blockade or embargo (if in each case it affects a significant geographical area).
Services IPR	has the meaning given to that expression in Section M5.14 (Services IPR).
Shared Resources	in relation to any User Systems, has the meaning given to that expression in Section G5.25 (Shared Resources).
Shared Secret	means a parameter that is (or may be) derived from a Private Key and a Public Key which are not from the same Key Pair in accordance with the GB Companion

	Specification.
Shared Solution Alt HAN Equipment	has the meaning given to that expression in accordance with standard condition 55 of the Electricity Supply Licence (Smart Metering – The Alt HAN Arrangements) and standard condition 49 of the Gas Supply Licence (Smart Metering – The Alt HAN Arrangements).
Signed Pre-Command	means a communication containing the Digitally Signed GBCS Payload of a Pre-Command that has been Digitally Signed by a User or the CoS Party.
Significant Code Review	means a review of one or more matters by the Authority which the Authority considers is: (a) related to this Code (whether on its own or together with other Energy Codes); and (b) likely to be of significance in relation to the Authority's principal objective and/or general duties (as set out in section 3A of the Electricity Act and section 4AA of the Gas Act), statutory functions and/or relevant obligations arising under EU law, and concerning which the Authority has issued a notice that the review will constitute a significant code review.
Significant Code Review Phase	means, in respect of each Significant Code Review, the period from the date on which the Authority issues the notice stating that the matter is to constitute a Significant Code Review, and ending on the earlier of: (a) the date on which the DCC submits a Modification Proposal in respect of any

	variations arising out of a Significant Code Review that the DCC is directed to submit by the Authority; (b) the date on which the Authority issues a conclusion that no modification is required to this Code as a result of the Significant Code Review; or (c) the date 28 days after the date on which the Authority issues its conclusion document in respect of the Significant Code Review.
SIT Approach Document	has the meaning given to that expression in Section T2.5 (SIT Approach Document).
SIT Objective	has the meaning given to that expression in Section T2.2 (SIT Objective).
SM WAN	means the means by which the DCC sends, receives and conveys communications to and from Communications Hub Functions.
SM WAN Coverage Database	means the information made available via the SSI pursuant to Section H8.16(f) (and which is also available via the CH Ordering System).
Small Supplier Party	means a Supplier Party which, at the time at which it is necessary to assess the status of the Party, supplies electricity and/or gas to fewer than 250,000 (two hundred and fifty thousand) Domestic Premises.
Smart Meter	means either an Electricity Smart Meter or a Gas Smart Meter (as the context requires).
Smart Metering Equipment	means the document(s) set out in Schedule [TBC].

Technical Specification

Smart Metering Inventory means an electronic database of Devices which records (as a minimum) the following information in respect of each Device:

(a) its Device Type;

(b) its Device ID;

(c) its Device Model (provided that no firmware version is needed for Type 2 Devices);

(d) for Devices other than Type 2 Devices, its SMI Status, and the date from which that status has applied;

(e) for Devices other than Type 2 Devices, its SMI Status history;

(f) where it is a Smart Meter which has been installed, the related MPAN or MPRN and the Communications Hub Function with which that Smart Meter is associated; and

(g) where it is a Device (other than a Smart Meter or a Communications Hub Function), the Smart Meter or Gas Proxy Function with which that Device is associated.

Smart Metering Key Infrastructure (or SMKI) means the public key infrastructure established by DCC for the purpose, among other things, of providing secure communications between Devices and Users.

Smart Metering System means either:

(a) an Electricity Smart Meter together with the Communications Hub Function with which it is Associated, together with the Type 1 Devices (if

any) that may from time to time be Associated with that Electricity Smart Meter; or

(b) a Gas Smart Meter together with the Communications Hub Function with which it is Associated and an Associated Gas Proxy Function, together with the Type 1 Devices (if any) that may from time to time be Associated with that Gas Proxy Function.

SMETS means the Smart Metering Equipment Technical Specification.

SMI Status means the status indicator of each Device recorded within the Smart Metering Inventory, which indicator may (as a minimum) be set to any one of the following:

(a) 'pending', indicating that the Device has not yet been Commissioned;

(b) 'installed not commissioned', indicating that the Device is ready to be Commissioned, but has not yet been Commissioned;

(c) 'commissioned', indicating that the Device has been Commissioned;

(d) 'decommissioned', indicating that the Device has been Decommissioned;

(e) 'withdrawn', indicating that the Device has been Withdrawn;

(f) 'suspended', indicating that the Device has been Suspended; or

(g) 'whitelisted', indicating that a Device has been added to the Device Log of a Communications

	Hub Function but that communications between the Device and the Communications Hub Function may not yet have been established.
SMKI and Repository Entry Process Tests	means the tests described in Section H14.22 (SMKI and Repository Entry Process Tests).
SMKI and Repository Test Scenario Document	means the SEC Subsidiary Document of that name set out in Appendix K, which is originally to be developed pursuant to Section T6 (Development of Enduring Testing Documents).
SMKI and Repository Testing	means the testing described in Section T5 (SMKI and Repository Testing).
SMKI Code of Connection	means the SEC Subsidiary Document of that name set out in Appendix [TBC], which: (a) has the purpose described in Section L4.5 (SMKI Code of Connection); and (b) is originally to be developed pursuant to Sections L4.6 to L4.7 (SMKI Interface Document Development).
SMKI Compliance Policy	means the SEC Subsidiary Document of that name set out in Appendix C.
SMKI Document Set	has the meaning given to that expression in Section L9.3 (the SMKI Document Set).
SMKI Independent Assurance Scheme	has the meaning given to that expression in Part 2.1 of the SMKI Compliance Policy (DCC: Duty to Submit to an SMKI Independent Assurance Scheme).
SMKI Interface Design Specification	means the SEC Subsidiary Document of that name set out in Appendix [TBC], which:

	(a) has the purpose described in Section L4.4 (SMKI Interface Design Specification); and (b) is originally to be developed pursuant to Sections L4.6 to L4.7 (SMKI Interface Document Development).
SMKI Participants	means the DCC (acting in its capacity as the provider of the SMKI Services), all Authorised Subscribers and all Relying Parties.
SMKI PMA	means the Sub-Committee of that name established pursuant to Section L1 (SMKI Policy Management Authority).
SMKI PMA (Network) Member	has the meaning given to that expression in Section L1.8 (Membership of the SMKI PMA).
SMKI PMA (Supplier) Members	has the meaning given to that expression in Section L1.6 (Membership of the SMKI PMA).
SMKI PMA Chair	has the meaning given to that expression in Section L1.5 (Membership of the SMKI PMA).
SMKI PMA Member	has the meaning given to that expression in Section L1.3 (Membership of the SMKI PMA).
SMKI Recovery Key Guidance	has the meaning given to that expression in Section L10.9 (The SMKI Recovery Key Guidance).
SMKI Recovery Procedure	means the SEC Subsidiary Document of that name set out in Appendix [TBC], which: (a) has the purpose described in Section L10.1 (The SMKI Recovery Procedure); and (b) is originally to be developed pursuant to Sections L10.7 to L10.8 (SMKI Recovery

	Procedure: Document Development).
SMKI Registration Authority Policies and Procedures (or **SMKI RAPP**)	means the SEC Subsidiary Document of that name set out in Appendix D, which is originally to be developed pursuant to Sections L9.5 to L9.6 (the Registration Authority Policies and Procedures: Document Development).
SMKI Repository	has the meaning given to that expression in Section L5.1 (the SMKI Repository).
SMKI Repository Code of Connection	means the SEC Subsidiary Document of that name set out in Appendix [TBC], which: (a) has the purpose described in Section L6.5 (SMKI Repository Code of Connection); and (b) is originally to be developed pursuant to Sections L6.6 to L6.7 (SMKI Repository Interface Document Development).
SMKI Repository Interface	has the meaning given to that expression in Section L6.3 (the SMKI Repository Interface).
SMKI Repository Interface Design Specification	means the SEC Subsidiary Document of that name set out in Appendix [TBC], which: (a) has the purpose described in Section L6.4 (SMKI Repository Interface Design Specification); and (b) is originally to be developed pursuant to Sections L6.6 to L6.7 (SMKI Repository Interface Document Development).
SMKI Repository Service	has the meaning given to that expression in Section L5.2 (the SMKI Repository Service).

SMKI SEC Documents	has the meaning given to that expression in Section L9.4 (the SMKI SEC Documents).
SMKI Service Interface	has the meaning given to that expression in Section L4.3 (the SMKI Service Interface).
SMKI Services	has the meaning given to that expression in Section L3.1 (the SMKI Services).
SMKI Specialist	means an individual (rather than a body corporate, association or partnership) to be appointed and remunerated under a contract with SECCo, who: (a) has experience and expertise in public key infrastructure arrangements; (b) is sufficiently independent of any particular Party or RDP, or class of Parties or RDPs, and of the Independent SMKI Assurance Service Provider; and (c) is chosen by the SMKI PMA Chair from time to time.
SOC2	means the Service Organisation Control 2 standard, as defined by the American Institute of Certified Public Accountants.
Solution Architecture Information	means a description of the overall technical architecture of the DCC Systems (or any part thereof) in more detail than the Technical Architecture Document so as to describe the individual components of the DCC Systems (including hardware and software) and how they interface with the User Systems.

SPAA	means the Supply Point Administration Agreement established pursuant to the Gas Supply Licences.
Special Installation Mesh Communications Hub	means a WAN Variant (in the central Region and the southern Region) which is distinguishable from a standard Mesh Communications Hub by the existence of an additional external aerial port.
Special Second-Fuel Installation	means, in the case of a premises for which there is both an Electricity Smart Meter and a Gas Smart Meter, where on the installation of the second of those two meters to be installed it was necessary to replace the Communications Hub relating to the first of those two meters to be installed because that Communications Hub was not able to serve the second of those two meters to be installed (with the consequence that the Communications Hub that is replaced is removed from the premises and returned to the DCC).
Special WAN-Variant Installation	means that the DCC requests (in accordance with the Incident Management Policy) that a Supplier Party replaces an installed Communications Hub with a Communications Hub of a different WAN Variant to the installed Communications Hub, with the consequence that the Communications Hub that is replaced is removed from the premises and returned to the DCC.
Specimen Accession Agreement	means the specimen form of agreement set out in Schedule 2.
Specimen Bilateral Agreement	means the specimen form of agreement set out in Schedule 3.

Specimen Enabling Services Agreement	means the form of specimen agreement set out in Schedule 7 (Specimen Enabling Services Agreement).
SRT Approach Document	has the meaning given to that expression in Section T5.5 (SRT Approach Document).
SRT Objective	has the meaning given to that expression in Section T5.2 (SRT Objective).
Stage 1 Assurance Report	has the meaning given to that expression in Part 4.4 of the SMKI Compliance Policy (Nature of the Initial Assessment).
Stage 2 Assurance Report	has the meaning given to that expression in Part 4.6 of the SMKI Compliance Policy (Nature of the Initial Assessment).
Statement of Service Exemptions	means a statement of that name developed by the DCC in accordance with Condition 17 of the DCC Licence.
Sub-Committee	has the meaning given to that expression in Section C6 (Sub-Committees).
Subject	in relation to a Certificate, has the meaning given to that expression in the relevant Certificate Policy.
Subscriber	means, in relation to any Certificate, SECCo, a Party or an RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.
Subscriber Obligations	means the provisions in respect of Subscribers set out at Section L11 of the Code (the Subscriber Agreement Obligations).
Successfully Executed	means:

(a) in respect of a Command and a Device, that the action that a Command of the relevant type is designed to effect in respect of a Device of the relevant Device Type has been effected on the Device; or

(b) in respect of a Service Request and a Device, that the associated Command has been Successfully Executed on the Device as described in (a) above (or, in the case of Service Requests that are not designed to result in a Command, that the action that a Service Request of the relevant type is designed to effect has been effected).

Successor Licensee	has the meaning given to that expression in Section M9.2 (Application and Interpretation of Section M9).
Supplementary Remote Party	has the meaning given to that expression in the GB Companion Specification.
Supplier Party	means a Party that is an Electricity Supplier Party and/or a Gas Supplier Party.
Supply Meter Point	has the meaning given to that expression in the UNC.
Supply Meter Point Reference Number	has the meaning given to that expression in the UNC.
Supply Number	has the meaning given to that expression in the MRA.
Supply of Energy	means either or both of the supply of gas pursuant to the Gas Act and the supply of electricity pursuant to the Electricity Act (in each case within the meaning that is given to the expression "supply" in the

	respective Act).
Supply Sensitive Check	means a check carried out by a User in relation to a Supply Sensitive Service Request in order to confirm the intention of the User that the associated Command should be executed on the relevant Device, having regard to the reasonably foreseeable effect that the Command could have on the quantity of gas or electricity that is supplied to a consumer at premises.
Supply Sensitive Service Request	means any Service Request in respect of which it is reasonably foreseeable that the associated Command, if it were to be executed on the relevant Device, could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises.
Suspended	means, in respect of a Device, that the Device has been suspended (or deemed suspended) in accordance with Section H6.10 (Suspension); and the word "**Suspension**" shall be interpreted accordingly.
Symmetric Key	means any key derived from a Shared Secret in accordance with the GB Companion Specification
System	means a system for generating, sending, receiving, storing (including for the purposes of Back-Up), manipulating or otherwise processing electronic communications, including all hardware, software, firmware and Data associated therewith.
System Development Lifecycle	means, in relation to any System, the whole of the life of that System from its initial concept to ultimate disposal, including the stages of development, design, build, testing, configuration, implementation,

operation, maintenance, modification and decommissioning.

Systems Integration Testing means the testing described in Section T2 (Systems Integration Testing).

Target Availability Period means, in relation to the Self-Service Interface, a period of time in respect of each month, expressed in minutes and calculated as:

(a) the total number of minutes in that month,

minus

(b) the number of minutes during which the relevant DCC Service Provider has, acting in compliance with Sections H8.2 and H8.3 (Maintenance of the DCC Systems), arranged for the Self-Service Interface to be unavailable during that month for the purposes of Planned Maintenance.

Target Resolution Time has the meaning given to that expression in Section H9.1 (Incident Management Policy).

Target Response Time has the meaning given to that expression in Section H3.14 (Target Response Times) or L8 (SMKI Performance Standards and Demand Management).

Target Service Level means, in respect of each Performance Measure, the number or percentage intended to represent a reasonable level of performance for the activity which is the subject of the Performance Measure, as set out in:

(a) Section H13.1 (Code Performance Measures);

(b) the Reported List of Service Provider Performance Measures; or

(c) Section L8.6 (Code Performance Measures).

TCH Participant	has the meaning given to that expression in Section F10.5 (Provision of Test Communications Hubs).
Technical Architecture and Business Architecture Sub-Committee	means the Sub-Committee established pursuant to Section F1 (Technical Architecture and Business Architecture Sub-Committee).
Technical Architecture Document	means a document setting out a representation of the End-to-End Technical Architecture.
Technical Code Specifications	means the Technical Specifications, the DCC Gateway Connection Code of Connection, the DCC User Interface Code of Connection, the DCC User Interface Specification, the Self-Service Interface Design Specification, the Self-Service Interface Code of Connection, the Registration Data Interface Documents, the Message Mapping Catalogue, the Incident Management Policy, the DCC Release Management Policy, the Panel Release Management Policy, the SMKI Interface Design Specification, the SMKI Code of Connection, the SMKI Repository Interface Design Specification and the SMKI Repository Code of Connection.
Technical Specification	means each of the CHTS and the SMETS.
Test Certificate	means a certificate that simulates the function of a Certificate for the purpose of testing pursuant to this Code.
Test Communications Hub	means: (a) until such date as the DCC may determine (or such earlier date as the Secretary of State may

designate for the purposes of this definition), a Prototype Communications Hub; and

(b) after such date, a device that is equivalent to a Communications Hub but which contains such variations in functionality as the DCC reasonably considers appropriate to enable the device to be used for the purposes of testing, which device is provided (or to be provided) for the purpose of testing as described in Section F10 (Test Communications Hubs).

Test Repository means a repository that simulates the function of the SMKI Repository for the purpose of testing pursuant to this Code.

Test Stubs means Systems and actions which simulate the behaviour of Devices and User Systems.

Testing Issue means, in respect of any tests:

(a) anything that is preventing the execution of the tests; or

(b) once commenced or executed, the test has an unexpected or unexplained outcome or response.

Testing Objectives means one or more of the SIT Objective and the Interface Testing Objective.

Testing Participant means, in respect of each Testing Service, the persons (whether or not they are Parties) who are entitled to undertake such tests, as described in Section H14 (Testing Services), together with any other persons identified as such in Section T (Testing During Transition).

Testing Service	has the meaning given to that expression in Section H14.1 (General Testing Requirements).
Threshold Anomaly Detection	means the DCC processes which: (a) in respect of any User, detect whether the total number of communications (in general or of a particular type) sent, received or processed by the DCC in relation to that User exceeds the relevant Anomaly Detection Threshold; (b) in respect of the DCC, detect whether: (i) the total number of communications of a particular type sent, received or processed by the DCC in relation to all Users and the CoS Party exceeds the relevant Anomaly Detection Threshold; and (ii) a data value within a communication of a particular type sent, received or processed by the DCC in relation to a User exceeds or is less than the relevant Anomaly Detection Threshold; and (c) quarantine those communications that, in the case of paragraph (a) or (b)(i) above, are in excess of the relevant Anomaly Detection Threshold or, in the case of paragraph (b)(ii) above, contain a data value that exceeds or is less than the relevant Anomaly Detection Threshold.
Threshold Anomaly Detection Procedures	means the SEC Subsidiary Document of that name set out in Appendix [TBC], which: (a) has the purpose described in Section G6.1

	(Threshold Anomaly Detection Procedures); and (b) is originally to be developed pursuant to Section X10 (Threshold Anomaly Detection Procedures).
Transform	means, in respect of a Service Request in relation to a Device, the conversion of that Service Request into one or more corresponding Commands (less any required Message Authentication Code or Digital Signatures), where such correspondence is identified in the DCC User Interface Specification in respect of particular types of Service Request and particular Device Types; and "**Transformed**" shall be interpreted accordingly.
Transition Objective	has the meaning given to that expression in Section X1 (General Provisions Regarding Transition).
Type 1 Device	means a HAN Connected Auxiliary Load Control Switch or a Pre-Payment Meter Interface Device.
Type 2 Device	has the meaning given to that expression in the SMETS.
Type 2 Device (Other)	means a Type 2 Device that is not an IHD.
UKAS	means the United Kingdom Accreditation Service
UNC	means the Uniform Network Code established pursuant to the Gas Transporter Licences.
Unique Transaction Reference Number	has the meaning given to that expression in the GB Companion Specification.
Unknown Remote Party	has the meaning given to that expression in the GB Companion Specification.

Unplanned Maintenance	means, in respect of a month, Maintenance of the DCC Systems that was not planned prior to the start of that month and which disrupts, will disrupt, or poses a Material Risk of disruption to, provision of the Services (and, where it disrupts, will disrupt, or poses a Material Risk of disruption to, the provision of the Services in relation to Devices associated with Communications Hubs, at least 100,000 Communications Hubs are affected).
UPRN	means the unique property reference number (if any) recorded in respect of a premises so as to link the MPAN(s) and MPRN for that premises.
Urgent Proposal	has the meaning given to that expression in Section D4.6 (Urgent Proposals).
User	means a Party that has completed the User Entry Process (and, in respect of Services available in accordance with this Code to Users acting only in one or more User Roles, a Party that has completed the User Entry Process for that User Role).
User Entry Process	means the process described in Section H1 (User Entry Process).
User Entry Process Tests	means the tests described in Section H14.13 (User Entry Process Tests).
User ID	means, in respect of a User and a User Role, one of the unique identification numbers accepted by the DCC in respect of that User and that User Role under Section H1.6 (User Roles and User IDs).
User Independent Security	has the meaning given to that expression in Section

Assurance Service Provider	G8.1 (Procurement of the Independent Security Assurance Service Provider).
User Personnel	means those persons who are engaged by a User, in so far as such persons carry out, or are authorised to carry out, any activity in relation to the business of the User in the exercise of rights and compliance with obligations under this Code.
User Privacy Self-Assessment	has the meaning given to that expression in Section I2.12 (Categories of Assessment).
User Privacy Self-Assessment Report	has the meaning given to that expression in Section I2.24 (The User Privacy Self-Assessment Report).
User Role	means, in respect of the Service set out in the DCC User Interface Services Schedule and Elective Communication Services, one of the categories of User that is capable of being an Eligible User in respect of those Services (determined without reference to a particular Smart Metering System), and which comprise the following categories (construed without reference to a particular Smart Metering System): Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent and Other User.
User Security Assessment	means either a Full User Security Assessment or a Verification User Security Assessment.
User Security Assessment Methodology	means a methodology to be applied (as the case may be): (a) by the User Independent Security Assurance Service Provider in carrying out any User

Security Assessment; or

(b) by a User, in carrying out any User Security Self-Assessment,

in each case in accordance with the provisions of the Security Controls Framework applicable to the relevant category of security assurance assessment.

User Security Assessment Report has the meaning given to that expression in Section G8.22 (User Security Assessments: General Procedure).

User Security Assessment Response has the meaning given to that expression in Section G8.24 (User Security Assessments: General Procedure).

User Security Self-Assessment has the meaning given to that expression in Section G8.18 (Categories of Security Assurance Assessment).

User Systems means any Systems (excluding any Devices) which are operated by or on behalf of a User and used in whole or in part for:

(a) constructing Service Requests;

(b) sending Service Requests over the DCC User Interface;

(c) receiving, sending, storing, using or otherwise carrying out any processing in respect of any Pre-Command or Signed Pre-Command;

(d) receiving Service Responses or Alerts over the DCC User Interface;

(e) generating Data for communication to the OCA, DCA, ICA or DCCKICA, or receiving Data from the OCA, DCA, ICA or DCCKICA (including

any Systems which store or use Secret Key Material for such purposes); ~~and/or~~

(f) generating Data for the purposes of lodging in the SMKI Repository or DCCKI Repository, or retrieving Data from the SMKI Repository or DCCKI Repository; and/or

~~(f)~~(g) generating any Unique Transaction Reference Number,

and any other Systems from which the Systems used in whole or in part for the purposes set out in paragraphs (a) to (~~f~~g) are not Separated.

Valid Communications Hub Order means the Consignment or Consignments which arise from a Communications Hub Order that has been accepted by the DCC under Section F5.16 or F5.17 (DCC: Duties in relation to Communications Hub Orders), and which have not been cancelled by the ordering Party in accordance with Section F5.19 (Non-Standard Cancellation of Consignments).

Valid Technical Specification means, in respect of a Technical Specification and a device which was installed at a particular point in time, one of the versions of that Technical Specification that has (or had) a validity period including that point in time (where validity period is the period identified as such within that version of the Technical Specification).

Validity Period has the meaning given to that expression in any of the Certificate Policies or the DCCKI Certificate Policy.

Value at Risk has the meaning given to that expression in Section J3.3 (User's Value at Risk).

VAT	means VAT, as defined in the Value Added Tax Act 1994, and any tax of a similar nature which may be substituted for or levied in addition to it.
Verification User Security Assessment	has the meaning given to that expression in Section G8.17 (Categories of Security Assurance Assessment).
Verify	means, in respect of a Service Request, to confirm that it meets all the applicable requirements of the DCC User Interface Specification.
Volume Scenarios	means the capacity levels to which the DCC Systems will be tested.
Voting Group	means, in respect of each Party Category, each Party that falls into that Party Category collectively with that Party's Affiliates (if any) who also fall into that Party Category.
WAN Variants	means the variations of Communications Hub that are necessary to enable communications via the SM WAN in each Region (and each part thereof that is not subject to the Statement of Service Exemptions).
Website	means a dedicated website established at the direction of the Panel for the purposes of this Code.
Withdrawal	means, in respect of a Smart Metering System (or a Device), the act of ending that Smart Metering System's Enrolment (or, in the case of a Device, of ending the Enrolment of the Smart Metering System of which that Device forms part) in accordance with Section H6.7 (Withdrawal); and the words "**Withdraw**" and "**Withdrawn**" shall be interpreted accordingly.

Working Day	means any day other than a Saturday, a Sunday, Christmas Day, Good Friday, or a day that is a bank holiday within the meaning of the Banking and Financial Dealings Act 1971.
Working Group	has the meaning given to that expression in Section D6.2 (Establishment of a Working Group).
Zigbee Alliance	means the association of that name administered by ZigBee Alliance Inc (2400 Camino Ramon, Suite 375, San Ramon, CA 94583, USA) (see - www.zigbee.org).

A2 INTERPRETATION

A2.1 In this Code, unless the context otherwise requires, any reference to:

(a) a "person" includes a reference to an individual, a body corporate, an association, a partnership or a Competent Authority;

(b) the singular includes the plural, and vice versa;

(c) a gender includes every gender;

(d) a Section or Schedule is a reference (respectively) to the section of, or schedule to, this Code which bears the relevant letter, number or letter and number;

(e) a numbered Paragraph or a numbered Clause is a reference to the paragraph or clause of the Schedule or Appendix in which such reference occurs;

(f) a numbered Condition (with or without a letter) is a reference to the licence condition bearing that number (and, where relevant, letter) in the Energy Licence indicated (and, save in the case of the DCC Licence, is a reference to the standard licence conditions of that Energy Licence);

(g) writing (or similar) includes all methods of reproducing words in a legible and non-transitory form (including email);

(h) a day, week or month is a reference (respectively) to a calendar day, a week starting on a Monday, or a calendar month;

(i) a time is a reference to that time in the UK;

(j) any statute or statutory provision includes any subordinate legislation made under it, any provision which it has modified or re-enacted, and any provision which subsequently supersedes or re-enacts it (with or without modification);

(k) an agreement, code, licence or other document is to such agreement, code, licence or other document as amended, supplemented, novated or replaced from time to time;

(l) a Party shall include reference to that Party's respective successors, (in the case of the DCC) to the person to whom the DCC may novate its rights and obligations pursuant to Section M9 (Transfer of DCC Licence), and (as the context permits) reference to the respective persons to whom that Party may sub-contract or otherwise delegate its rights and/or obligations under this Code in accordance with Section M11.8 and M11.9 (which shall include, in the case of the DCC, reference to the DCC Service Providers);

(m) any premises of a Party shall include references to any premises owned or occupied by that Party and (as the context permits) by the respective persons to whom that Party may sub-contract or otherwise delegate its rights and/or obligations under this Code in accordance with Section M11.8 and M11.9 (which shall include, in the case of the DCC, reference to the DCC Service Providers);

(n) a Competent Authority or other public organisation includes a reference to its successors, or to any organisation to which some or all of its functions and responsibilities have been transferred; and

(o) an expression that is stated to have the meaning given to it in an Energy Licence (other than the DCC Licence) is a reference to that expression as defined in the standard licence conditions for the Energy Licence indicated.

A2.2 The headings in this Code are for ease of reference only and shall not affect its interpretation.

A2.3 In this Code, the words preceding "include", "including" or "in particular" are to be construed without limitation to the generality of the words following those expressions.

A2.4 The language of this Code is English. All notices and other communications sent between any of the Parties, the Panel, SECCo, the Code Administrator and the Secretariat shall be in English.

A2.5 Except where expressly stated to the contrary, in the event of any conflict between the provisions of this Code, the following order of precedence shall apply:

(a) the Sections, as among which Section X (Transition) shall take precedence; then

(b) the Schedules; then

(c) the SEC Subsidiary Documents.

A2.6 Except to the extent that any provision of Section T (Testing During Transition) otherwise provides (in which case that provision shall take precedence), Section A2.7 shall apply, during the period prior to Completion of Implementation, where initial capital letters are used for any expression in this Code that either is not defined in this Code or the definition of which cannot be given effect by reference to the provisions of this Code.

A2.7 Any expression of the type referred to in Section A2.6 shall be interpreted as having the meaning given to that expression in the decision or consultation document concerning the intended future definition of such expression most recently published by the Secretary of State prior to the date on which this Section A2.7 comes into force.

A2.8 Where no time period is specified for performance of any obligation under this Code, the obligation shall be performed as soon as reasonably practicable.

SECTION B: ACCESSION

B1 ACCESSION

Eligibility for Admission

B1.1 Any person who applies to be admitted as a Party (an **Applicant**) shall be entitled to be admitted as a Party, subject to and in accordance with the provisions of this Section B1.

B1.2 An Applicant may not be admitted as a Party if:

(a) it is already a Party; or

(b) it was expelled from this Code in accordance with Section M8 (Suspension, Expulsion and Withdrawal) within the 12 months preceding the date of its application (or such shorter period as the Panel may determine from time to time).

Application Form and Guidance

B1.3 The Code Administrator shall create an Application Form, and publish such form on the Website.

B1.4 The Code Administrator shall establish and publish on the Website a guide for Applicants describing, and providing guidance in respect of, the process set out in this Section B1 (the **Application Guidance**).

Application Fee

B1.5 The Panel shall determine (and publish on the Website) a fee from time to time (the **Application Fee**) to be payable by Applicants to SECCo. The Panel shall set the Application Fee at a level intended to recover the reasonable costs incurred by or on behalf of the Panel (including amounts payable to the Code Administrator) in administering the process set out in this Section B1.

B1.6 The Code Administrator shall include within the Application Guidance details of the

methods by which the Application Fee may be paid.

Accession Process

B1.7 An Applicant shall submit to the Code Administrator a duly completed Application Form (together with any supporting documents required by that form), and the Application Fee (by a method of payment provided for in the Application Guidance).

B1.8 As soon as reasonably practicable following receipt of an Application Form and the Application Fee from an Applicant, the Code Administrator shall:

(a) notify the Applicant if it is ineligible to be admitted as a Party in accordance with Section B1.2;

(b) where the Applicant is not ineligible, check that the Application Form has been duly completed and that any supporting documentation requested has been provided, and notify the Applicant of any omissions; and

(c) where there are no such omissions, notify the Applicant and the Panel that the Applicant is to be admitted as a Party subject to execution of an Accession Agreement.

Accession Agreement

B1.9 Where an Applicant is to be admitted as a Party in accordance with Section B1.8(c), the Code Administrator shall prepare two counterparts of the Accession Agreement for the Applicant (in substantially the form of the Specimen Accession Agreement), and send them to the Applicant.

B1.10 An Applicant that wishes to proceed with its accession to this Code should sign (but not date) both counterparts of the Accession Agreement, and return them to the Code Administrator.

B1.11 Upon return to the Code Administrator of the two counterparts of the Accession Agreement as envisaged by Section B1.10, the Panel shall procure that (as soon as reasonably practicable thereafter) SECCo:

(a) signs each counterpart on behalf of itself and all the Parties (as it is authorised

to do under Section B1.14); and

(b) dates each counterpart with the date of such execution.

B1.12 The Code Administrator shall return one signed and dated counterpart of the Accession Agreement to the Applicant, and retain the other counterpart for the Panel's records.

Accession

B1.13 An Applicant will accede to this Code and become a Party with effect from the date of its executed Accession Agreement. The Code Administrator shall give notice of each Applicant's accession to the Applicant, to each other Party and to the Authority. Such notice will confirm the Applicant's Party Details.

SECCo Authority to enter into Accession Agreements

B1.14 Subject to and in accordance with this Section B1, each Party hereby irrevocably and unconditionally authorises SECCo to execute and deliver, on behalf of such Party, any and all Accession Agreements that are substantially in the form of the Specimen Accession Agreement and that have been signed by an Applicant.

Disputes Regarding Admission

B1.15 Where an Applicant disagrees with any decision of the Code Administrator pursuant to Section B1.8, the Applicant may refer the matter to the Panel for determination.

B1.16 Where an Applicant disagrees with any decision of the Panel made pursuant to Section B1.15, the Applicant may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Party Signifiers

B1.17 On an Applicant acceding to this Code and becoming a Party, the Panel shall as soon as reasonably practicable thereafter issue to it a Party Signifier.

B1.18 The Code Administrator shall notify the DCC of each Party Signifier issued to a Party in accordance with Section B1.17.

RDP Signifiers

B1.19 The Panel shall issue to a Registration Data Provider (other than a Gas Network Party or Electricity Network Party which is deemed to be an RDP, acting in its capacity as such) an RDP Signifier:

(a) as soon as reasonably practicable after receipt of a request from that RDP for it to do so; or

(b) in any event prior to issuing an RDP ID, following receipt of an application from that RDP for it to do so.

B1.20 The Code Administrator shall notify the DCC of each RDP Signifier issued to an RDP in accordance with Section B1.19.

MRA and UNC Identifiers

B1.21 The Panel shall, as soon as reasonably practicable after a person becomes a Party, notify the DCC of the unique identifiers (if any) by which such person is identified under the MRA or the UNC, as set out in the Party Details contained in the relevant Accession Agreement. The Panel shall, as soon as reasonably practicable after a Party notifies any change or addition to such unique identifiers under Section M6 (Party Details), notify the DCC of such change or addition.

B2 DCC, USER AND RDP IDENTIFIERS

Panel: Duty to Obtain MA-S Registry Entries

B2.1 The Panel shall obtain one or more MA-S Registry Entries to the extent necessary for the purpose of establishing and issuing EUI-64 Compliant identifiers for use as User IDs, RDP IDs and/or DCC IDs in accordance with the provisions of this Section B2.

ID Allocation Procedure

B2.2 The Panel shall develop and maintain a document to be known as the "**ID Allocation Procedure**", which shall:

(a) make provision for the Panel to establish and issue Party and RDP Signifiers, each of which must be unique under this Code but which need not be EUI-64 Compliant;

(b) make provision for the Panel to establish EUI-64 Compliant identifiers by the concatenation of:

(i) the assigned value of an MA-S Registry Entry obtained by it; and

(ii) a unique extension identifier created by it;

(c) describe the numbering convention to be used by the Panel for the purpose of creating those unique extension identifiers;

(d) set out the application procedure to be followed by any Party which wishes to be issued with an EUI-64 Compliant identifier for use as a User ID or DCC ID, or by any RDP which wishes to be issued with an EUI-64 Compliant identifier for use as an RDP ID; and

(e) set out the procedure to be followed by the Panel in issuing an EUI-64 Compliant identifier to any Party or RDP for such purposes.

B2.3 In developing the ID Allocation Procedure, the Panel shall act in conjunction with the DCC and such other Parties and RDPs as have indicated a wish to be involved, and shall consult with and have regard to the views of all Parties and RDPs.

B2.4 The Panel shall keep the ID Allocation Procedure under review from time to time, and in particular when requested to do so by any Party or RDP, in order to ensure that it remains fit for purpose. Before making any change to the ID Allocation Procedure the Panel shall consult with and have regard to the views of all Parties and RDPs.

Issue of DCC, User and RDP IDs

B2.5 Where:

(a) the DCC wishes to be issued with an EUI-64 Compliant identifier for use as a DCC ID;

(b) another Party wishes to be issued with an EUI-64 Compliant identifier for use as a User ID; or

(c) an RDP wishes to be issued with an EUI-64 Compliant identifier for use as an RDP ID,

it shall, in accordance with the provisions of the ID Allocation Procedure, apply to the Panel for the issue of that identifier.

B2.6 No Party or RDP may apply to the Panel for the issue of an EUI-64 Compliant identifier other than for one of the purposes specified in Section B2.5.

B2.7 On receiving an application from a Party or RDP in accordance with Section B2.5, the Panel shall issue an EUI-64 Compliant identifier in accordance with the provisions of the ID Allocation Procedure.

Issue of Party and RDP Signifiers

B2.8 The Panel shall issue Party and RDP Signifiers to the Code Administrator from time to time, in accordance with the provisions of the ID Allocation Procedure, for their allocation by the Code Administrator to new Parties pursuant to Section B1.17 (Party Signifiers) and to RDPs pursuant to Section B1.19 (RDP Signifiers).

Record of Signifiers and IDs Issued

B2.9 The Panel shall:

(a) maintain an up to date record of the Party and RDP Signifiers and the EUI-64 Compliant identifiers issued by it pursuant to this Section B2 (and, where applicable, the mapping between them), and make that record available to all Parties and RDPs; and

(b) notify the DCC of any EUI-64 Compliant identifier that it has issued to:

(i) a Party for use as a User ID and the corresponding Party Signifier of that Party; or

(ii) an RDP for use as an RDP ID and the corresponding RDP Signifier of that RDP.

SECTION C – GOVERNANCE

C1 SEC OBJECTIVES

General SEC Objectives

C1.1 The objectives of this Code otherwise than in respect of the Charging Methodology are set out in Condition 22 of the DCC Licence (such objectives being the **General SEC Objectives**). For ease of reference, the General SEC Objectives are set out below using the terminology of this Code (but in the case of any inconsistency with the DCC Licence, the DCC Licence shall prevail):

(a) the first General SEC Objective is to facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain;

(b) the second General SEC Objective is to enable the DCC to comply at all times with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence;

(c) the third General SEC Objective is to facilitate Energy Consumers' management of their use of electricity and gas through the provision to them of appropriate information by means of Smart Metering Systems;

(d) the fourth General SEC Objective is to facilitate effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy;

(e) the fifth General SEC Objective is to facilitate such innovation in the design and operation of Energy Networks (as defined in the DCC Licence) as will best contribute to the delivery of a secure and sustainable Supply of Energy;

(f) the sixth General SEC Objective is to ensure the protection of Data and the security of Data and Systems in the operation of this Code;

(g) the seventh General SEC Objective is to facilitate the efficient and transparent

administration and implementation of this Code;

(h) the eighth General SEC Objective is to facilitate the establishment and operation of the Alt HAN Arrangements.

Transition Objective

C1.2 As provided for in Condition 22 of the DCC Licence, during the period prior to the Completion of Implementation, the General SEC Objectives must be read and given effect (so far as it is possible to do so) in a way that is compatible with achieving the Transition Objective.

Charging Objectives

C1.3 The objectives of this Code in respect of the Charging Methodology only (such objectives being the **Charging Objectives**) comprise the "**First Relevant Policy Objective**", the "**Second Relevant Policy Objective**" and the "**Third Relevant Policy Objective**" as set out in Condition 18 of the DCC Licence. For ease of reference, the First Relevant Policy Objective, the Second Relevant Policy Objective and the Third Relevant Policy Objective are set out in Sections C1.4, C1.5 and C1.6 using the terminology of this Code (but in the case of any inconsistency with the DCC Licence, the DCC Licence shall prevail).

C1.4 The First Relevant Policy Objective**:**

(a) applies in relation to Smart Metering Systems installed (or to be installed) at Domestic Premises; and

(b) requires the Charging Methodology to ensure that Charges (other than Charges for Elective Communication Services) in respect of such Smart Metering Systems do not distinguish (whether directly or indirectly) between Energy Consumers at Domestic Premises in different parts of Great Britain.

C1.5 The Second Relevant Policy Objective applies in relation to SMETS1 Meters. The Second Relevant Policy Objective is that, subject to compliance with the First Relevant Policy Objective, the Charging Methodology must (other than in respect of Elective Communication Services) (in each of the following cases, as far as is

reasonably practicable in all of the circumstances of the case, having regard to the costs of implementing the Charging Methodology):

(a) result in Charges that are the same for SMETS1 Meters as they are for Smart Metering Systems, save that no Charges for Communications Hub Services will apply to SMETS1 Meters;

(b) notwithstanding (a) above (where the Costs of Communications for a SMETS1 Meter exceeds the Costs of Communications for a Smart Metering System, and where an Original Supplier for the Energy Supplier Contract relating to that SMETS1 Meter is (and has at all times since the adoption of the Energy Supplier Contract been) a supplier of electricity and/or gas to the premises at which that SMETS1 Meter is installed), result in Charges that ensure that the excess Costs of Communications are recovered from the Original Supplier from time to time (in addition to the Charges referred to in (a) above),

and, for the purposes of this Section C1.5, the terms "**SMETS1 Meters**", "**Costs of Communications**", "**Original Supplier**" and "**Energy Supplier Contract**" shall have the meaning given to those terms in the DCC Licence.

C1.6 The Third Relevant Policy Objective is that, subject to compliance with the First and Second Relevant Policy Objectives, the Charging Methodology must result in Charges that**:**

(a) facilitate effective competition in the Supply of Energy (or its use) under the Electricity Act and the Gas Act;

(b) do not restrict, distort, or prevent competition in Commercial Activities that are connected with the Supply of Energy under the Electricity Act and the Gas Act;

(c) do not deter the full and timely installation by Energy Suppliers of Smart Metering Systems at Energy Consumers' premises in accordance with their obligations under the Energy Supply Licence; and

(d) do not unduly discriminate in their application and are reflective of the costs

incurred by the DCC, as far as is reasonably practicable in all of the circumstances of the case, having regard to the costs of implementing the Charging Methodology.

C1.7 The Charging Methodology will achieve the Third Relevant Policy Objective if it is compliant with the provisions of Section C1.6 in the round, weighing them as appropriate in each particular case.

C2 PANEL

Establishment of the Panel

C2.1 The Panel is hereby established. The Panel shall:

(a) pursue the objectives, undertake the duties, and have the powers, set out in Sections C2.2 to C2.4;

(b) be composed of the Panel Members described in Section C3 (Panel Members), some of whom will be elected in accordance with Section C4 (Elected Members); and

(c) conduct its activities in accordance with the procedures set out in Section C5 (Proceedings of the Panel).

Panel Objectives

C2.2 The Panel shall, in all its activities, always act in a manner designed to achieve the following objectives (the **Panel Objectives**):

(a) that this Code is given full and prompt effect in accordance with its terms and conditions;

(b) that this Code is given effect in such a manner as will facilitate achievement of the SEC Objectives;

(c) that this Code is given effect in a fair manner without undue discrimination between the Parties or any classes of Party; and

(d) that the Panel conducts its affairs in an open and transparent manner.

Panel Duties

C2.3 Without prejudice to any other tasks, duties or obligations imposed on the Panel in this Code, the Panel shall, subject to and in accordance with the other provisions of this Code:

(a) oversee the process by which Applicants apply to become a Party, as set out in

Section B (Accession);

(b) manage the Code Administrator and Secretariat, and oversee their performance;

(c) develop, consult upon, and report upon its performance against three-year budgets and work plans in accordance with Section C8 (Panel Costs and Budgets);

(d) oversee and co-ordinate the process for assessing Modification Proposals, and implement successful Modification Proposals, each as set out in Section D (Modification Process);

(e) manage and co-ordinate arrangements for the resolution of certain Disputes under or in relation to this Code, as set out in Section M7.3 (Reference to the Panel or its Sub-Committees);

(f) manage and co-ordinate the suspension of Parties' rights under this Code, as set out in Section M8 (Suspension, Expulsion and Withdrawal);

(g) manage and co-ordinate the withdrawal or expulsion of Parties from this Code, as set out in Section M8 (Suspension, Expulsion and Withdrawal);

(h) by no later than 30 Working Days following the end of each Regulatory Year prepare and publish a report on the implementation of this Code and the activities of the Panel during that Regulatory Year, including so as to evaluate whether this Code continues to meet the SEC Objectives;

(i) at the written request of the Authority at any time, undertake a review of such parts of this Code as the Authority may specify to evaluate whether this Code continues to meet the SEC Objectives;

(j) at the written request of the Authority, collect and provide to the Authority (or publish in such manner as the Authority may direct) such information regarding the SEC Arrangements as the Authority may reasonably request (and each Party shall provide to the Panel such information as the Panel reasonably requires in order to enable the Panel to comply with any such

request of the Authority);

(k) hold a general meeting during the month of July each year, which each Panel Member will (subject to unforeseen circumstances) attend, at which a representative of each Party shall be entitled to attend and speak, and at which the Panel will endeavour to answer any reasonable questions submitted to the Secretariat in advance of the meeting;

(l) establish (and, where appropriate, revise from time to time) joint working arrangements with the panels, committees and administrators responsible for the governance and operation of other Energy Codes, in order to facilitate the timely:

(i) identification, co-ordination, making and implementation of changes to other Energy Codes consequent on a Modification Proposal (and vice versa); and

(ii) identification and coordinated resolution of Disputes and disputes under other Energy Codes (in circumstances where there is an interaction between the Dispute and one or more disputes under the other Energy Codes);

(m) establish joint working arrangements with the Information Commissioner pursuant to which the Panel shall notify the Information Commissioner of matters in which the Panel believes the Information Commissioner may have an interest; and

(n) periodically commission a review of the effectiveness of the End-to-End Technical Architecture and the Business Architecture by the Technical Architecture and Business Architecture Sub-Committee, as further described in Section F1 (Technical Architecture and Business Architecture Sub-Committee).

Panel Powers

C2.4 Without prejudice to any other rights or powers granted to the Panel in this Code, the

Panel shall, subject to and in accordance with the other provisions of this Code, have the power to:

(a) appoint and remove the Code Administrator and the Secretariat in accordance with Section C7 (Code Administrator, Secretariat and SECCo);

(b) appoint and remove professional advisers;

(c) consider, approve and authorise the entering into by SECCo of contracts in accordance with Section C7 (Code Administrator, Secretariat and SECCo);

(d) constitute Sub-Committees in accordance with Section C6 (Sub-Committees);

(e) consider, approve and authorise the licensing, sub-licensing, or any other manner of dealing with the Intellectual Property Rights in the SEC Materials, for any use which does not hinder, delay or frustrate, in any way whatsoever, the SEC Objectives;

~~(e)~~(f) direct SECCo to become a Subscriber for IKI Certificates, on behalf of the Panel and for the purpose of Digitally Signing the Certified Products List; and

~~(f)~~(g) do anything necessary for, or reasonably incidental to, the discharge of its duties under this Code.

C3 PANEL MEMBERS

Panel Composition

C3.1 The Panel shall be composed of the following categories of persons (each a **Panel Member**, and the Panel Members referred to in Sections C3.1(a) to (e) being the **Elected Members**):

(a) two persons elected by the Large Supplier Parties;

(b) two persons elected by the Small Supplier Parties;

(c) one person elected by the Electricity Network Parties;

(d) one person elected by the Gas Network Parties;

(e) two persons elected by the Other SEC Parties;

(f) one person nominated by the DCC in accordance with Section C3.3 (the **DCC Member**);

(g) two persons nominated in accordance with Section C3.4 (the **Consumer Members**);

(h) one person appointed in accordance with Section C3.5 (the **Panel Chair**); and

(i) any additional person appointed by the Panel Chair in accordance with Section C3.6.

C3.2 Each Panel Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Panel Member.

DCC Member

C3.3 The DCC Member shall be one person nominated by the DCC by notice to the Secretariat. The DCC may replace such person from time to time by prior notice to the Secretariat.

Consumer Members

C3.4 The Consumer Members shall be two persons nominated by Citizens Advice or Citizens Advice Scotland by notice to the Secretariat from time to time. Citizens Advice or Citizens Advice Scotland may replace each such person from time to time by prior notice to the Secretariat.

Appointment of the Panel Chair

C3.5 The first Panel Chair to be appointed following the designation of this Code shall be appointed in accordance with the appointment process developed in accordance with Section X (Transition). Thereafter, each Panel Chair shall be appointed in accordance with the same process, as modified from time to time by the Panel; provided that such process as modified must be designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the appointment is conditional on the Authority approving the candidate;

(c) the Panel Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(d) the Panel Chair is remunerated at a reasonable rate;

(e) the Panel Chair's appointment is subject to Section C3.8 and terms equivalent to those set out in Section C4.6 (Removal of Elected Members); and

(f) provision is made for the Panel Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

Panel Chair Appointee

C3.6 Where at any time:

(a) no person is currently appointed as a Panel Member pursuant to this Section C3.6; and

(b) the Panel Chair (having consulted with the other Panel Members) considers

that there is a class or category of person having an interest in the SEC Arrangements whose interests are not adequately represented in the composition of the Panel at that time, and whose interests would be better represented if a particular person were appointed as an additional Panel Member,

the Panel Chair may (having consulted with the other Panel Members) appoint that particular person as a Panel Member by notice to the Secretariat. The Panel Chair may (having consulted with the other Panel Members), at any time thereafter by notice to the Secretariat, remove that person from the office of Panel Member.

Duties of Panel Members

C3.7 A person appointed as Panel Member, when acting in that capacity, shall:

(a) act independently, not as a delegate, and without undue regard to the interests, of any Related Person;

(b) exercise reasonable skill and care to the standard reasonably expected of a director of a company under the Companies Act 2006; and

(c) act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

Panel Member Confirmation

C3.8 Each Panel Member must confirm in writing to SECCo (for the benefit of SECCo and each Party) that that person:

(a) agrees to act as a Panel Member in accordance with this Code, including the requirements of Section C3.7; and

(b) agrees to accept appointment as a director of SECCo, and to act in such capacity in accordance with this Code; and

(c) will be available as reasonably required throughout his or her term of office, both to attend Panel meetings and to undertake work outside those meetings as may reasonably be required,

and must further complete any and all forms required to be completed by law in order for that person to become a director of SECCo.

C3.9 The appointment of a person who would otherwise be a Panel Member shall lapse (and the relevant office shall become vacant) if that person does not comply with the requirements of Section C3.8 within 20 Working Days after a request from the Secretariat to do so.

Notification of Related Persons

C3.10 Each Panel Member shall, at the time of his appointment and upon any relevant change in circumstance, disclose, in writing to the Panel, the name of each Related Person who is a Party, a DCC Service Provider or is otherwise likely to be materially affected by the SEC Arrangements (other than in the capacity of Energy Consumer).

C3.11 Without prejudice to the generality of Section C3.10, where a Panel Member changes employer, the Panel Member shall (as soon as reasonably practicable after such change) notify the Secretariat of such change in writing. The Secretariat shall then notify the Parties of such change in employer.

Protections for Panel Members and Others

C3.12 SECCo shall indemnify, and keep indemnified:

(a) each Panel Member (whether as a Panel Member or as a director of SECCo);

(b) each Reserve (whether acting as an Alternate or otherwise);

(c) each person who serves on a Sub-Committee or Working Group; and

(d) each Party, or an Affiliate of a Party, as employer of any person referred to in Sections C3.12(a) to (c),

from and against any and all costs (including legal costs), charges, expenses, damages or other liabilities properly incurred or suffered by that person or employer in relation to the exercise of the person's powers duties or responsibilities under this Code, including where such powers duties or responsibilities are exercised

negligently. The persons and employers shall be entitled to enforce their rights under this Section C3.12 pursuant to Section M11.5 (Third Party Rights).

C3.13 The indemnity set out in Section C3.12 shall not apply to any costs, charges, expenses, damages or other liabilities that are:

(a) costs and expenses expressly stated to be incapable of recovery by the Panel under Section C8 (Panel Costs and Budgets); or

(b) suffered or incurred or occasioned by the wilful default, fraud or bad faith of~~, or breach of contract by,~~ the relevant person.

C4 ELECTED MEMBERS

Elected Members

C4.1 The first Elected Members to be appointed on the designation of this Code shall be appointed in accordance with Section X (Transition). All other Elected Members shall be elected in accordance with the process set out in Section C4.2. Each Elected Member shall serve as a Panel Member until his or her retirement in accordance with Section C4.4, or until he or she is removed from office in accordance with Section C3.9, C4.5 or C4.6.

Election of Elected Members

C4.2 The process set out in this Section C4.2 shall apply in respect of the election of each Elected Member. This process shall apply in respect of Elected Member vacancies arising by virtue of a Panel Member's retirement in accordance with Section C4.4 (a **Scheduled Election**), or a Panel Member being removed from office in accordance with Section C3.9, C4.5 or C4.6 (an **Interim Election**). In each case, the following process shall apply:

(a) each Elected Member is to be elected by a Party Category as described in Section C3.1;

(b) each Voting Group within a Party Category is entitled to cast one vote in the election of the Panel Member(s) to be elected by that Party Category;

(c) the Secretariat shall publish on the Website and send to each Party within the relevant Party Category an invitation for nominations for candidates for the role of Elected Member for that Party Category;

(d) in the case of Scheduled Elections, the invitation for nomination of candidates shall be published and sent by the Secretariat at least 35 Working Days ahead of the date on which the relevant Panel Member's term of office expires;

(e) in the case of Interim Elections, the invitation for nomination of candidates shall be published and sent by the Secretariat by no later than 5 Working Days after the date on which the relevant Panel Member was removed from office;

(f) the invitation for nomination of candidates shall request nominations within 15 Working Days after the date of the invitation;

(g) the eligible candidates for election shall be those persons who are (at the time of their nomination) capable of becoming and remaining Panel Members in accordance with Sections C3.2 and C4.6, and whose nominations (whether nominated by themselves or a third party) are received by the Secretariat within the period of time set out in the request for nominations;

(h) where the Secretariat receives a nomination for a candidate that the Secretariat does not consider to be an eligible candidate in accordance with Section C4.2(g), the Secretariat shall notify that person that this is the case as soon as reasonably practicable after receipt of the nomination (and, in any event, by no later than 2 Working Days following the expiry of the period of time set out in the request for nominations);

(i) where a candidate disputes the Secretariat's notification under Section C4.2(h), the candidate shall have 2 Working Days following receipt of such notification to refer the matter to the Panel Chair for final determination (which determination shall be made by the Panel Chair by no later than 5 Working Days following the expiry of the period of time set out in the request for nominations);

(j) 6 Working Days following the expiry of the period of time set out in the request for nominations, the Secretariat shall give notice to each Party within the relevant Party Category of the names of each eligible candidate (together with any supporting information provided to the Secretariat with his or her nomination);

(k) at the same time as the Secretariat issues such notice, where there are more eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category, the Secretariat shall invite the Voting Groups comprising that Party Category to vote for their preferred eligible candidate;

(l) each such Voting Group shall be entitled to cast one vote, and shall cast such

vote by means of a system established by the Panel which ensures that each Voting Group casts only one vote, and which allows 10 Working Days following the invitation pursuant to Section C4.2(k) for such vote to be cast;

(m) the successful candidate or candidates elected as a result of the votes cast in accordance with this Section C4.2 shall be determined in accordance with Section C4.3;

(n) the Secretariat shall not publish details of the votes cast by each Voting Group, but shall disclose such details to the Panel Chair for scrutiny;

(o) as soon as reasonably practicable following the election of an Elected Member in accordance with this Section C4.2, the Secretariat shall publish on the Website and notify each Party of the identity of the person who has been so elected; and

(p) each person elected as a Panel Member in accordance with this Section C4.2 shall commence his or her office as a Panel Member: (i) in the case of Scheduled Elections, simultaneously with the retirement of the relevant Panel Member; or (ii) in the case of Interim Elections, simultaneously with the notification by the Secretariat pursuant to Section C4.2(o).

C4.3 As a result of the process set out in Section C4.2:

(a) where there are the same number of eligible candidates for a Party Category as there are positions to be filled as Elected Members for that Party Category, all of the eligible candidates shall be elected as Elected Members;

(b) where there are more eligible candidates for a Party Category than there are positions to be filled as Elected Members for that Party Category, the eligible candidate(s) that received the most votes in accordance with Section C4.2(l) shall be elected as Elected Members (and, in the case of a tie, the Secretariat shall determine the Elected Member by drawing lots, to be witnessed by the Panel Chair); or

(c) where there are fewer eligible candidates for a Party Category than there are

positions to be filled as Elected Members for that Party Category (including where there are no eligible candidates), the Authority will (at its discretion) be entitled to nominate an Elected Member for that Party Category. Where this Section C4.3(c) applies, the Panel shall be entitled (at any time thereafter) to determine that a further Interim Election should be held in accordance with Section C4.2 in respect of that Party Category.

Retirement of Elected Members

C4.4 Subject to earlier removal from office of an Elected Member in accordance with Section C3.9, C4.5 or C4.6 and without prejudice to his or her ability to stand for re-election, each Elected Member shall retire (at which point his or her office shall become vacant) as follows:

(a) the Elected Members elected in accordance with Section X (Transition) shall retire in accordance with that Section;

(b) the Elected Members elected in accordance with this Section C4.2, shall retire two years after the date on which they first took office; and

(c) any Elected Member nominated by the Authority pursuant to Section C4.3(c), shall retire on the Authority determining (at its discretion) that such person should be removed from office, or on the successful election of a replacement Elected Member in an election pursuant to Section C4.3(c).

Removal of Elected Members

C4.5 An Elected Member may:

(a) resign his or her office by 10 Working Days' notice in writing to the Panel Chair;

(b) be removed from office by the Panel Chair on notice to the Panel if the Elected Member fails to attend (either in person or via his or her Alternate) at least 50% of the Panel meetings held in any period of 12 months; or

(c) be removed from office by the other Panel Members (acting unanimously) if

such other Panel Members consider that the Elected Member is in breach of the confirmation given by that Elected Member pursuant to Section C3.8 (Panel Member Confirmation).

C4.6 An Elected Member shall automatically be removed from office if he or she:

(a) dies;

(b) is admitted to hospital in pursuance of an application under the Mental Health Act 1983 or the Mental Health (Care and Treatment) (Scotland) Act 2003, or an order is made by a court with competent jurisdiction in matters concerning mental disorder for his detention or for the appointment of a receiver, curator bonis or other person with respect to his property or affairs;

(c) becomes bankrupt or makes any arrangement or composition with his creditors;

(d) becomes prohibited by law from being a director of a company under the Companies Act 2006; and/or

(e) is convicted of an indictable criminal offence.

C5 PROCEEDINGS OF THE PANEL

Meetings of the Panel

C5.1 The Panel shall hold meetings with such frequency as it may determine or the Panel Chair may direct, but in any event shall meet when necessary to meet its responsibilities under Section D (Modification Process) and at least once every two months.

C5.2 The location and timing of each meeting shall be determined by the Panel. Panel Members shall endeavour to attend each meeting in person, but attendance by telephone conference or other technological means shall be permitted (provided that each of the Panel Members attending the meeting acknowledges that he or she can communicate with each other).

C5.3 Subject to the other provisions of this Code, the Panel may regulate the conduct of its meetings as it sees fit.

Quorum

C5.4 No business shall be transacted at any meeting of the Panel unless a quorum is present at that meeting. The quorum for each Panel meeting shall be one half of all Panel Members appointed at the relevant time, at least one of whom must be the Panel Chair.

Meeting Notice and Papers

C5.5 Each meeting that the Panel determines, or the Panel Chair directs, is to be held shall be convened by the Secretariat. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Panel may approve). Such notice must be given to:

(a) the Panel Members (and any appointed Alternates);

(b) each of the persons referred to in Section C5.13;

(c) the Parties; and

(d) any other person that the Panel determines, or the Panel Chair directs, should be invited to the meeting.

C5.6 The notice of each Panel meeting shall contain or be accompanied by the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and supporting papers.

C5.7 The accidental omission to give notice of a meeting to, or the non-receipt of notice of a Panel meeting by, a person entitled to receive notice shall not invalidate the proceedings of that meeting.

Panel Chair

C5.8 The Panel Chair shall preside at every meeting of the Panel. If the Panel Chair is unable to attend a Panel meeting, the Panel Chair shall ensure that his or her Alternate attends the meeting as Panel Chair.

C5.9 The Panel Chair shall not be entitled to vote unless there is a deadlock, in which case the Panel Chair shall have the casting vote.

Voting

C5.10 Subject to Section C5.9, each Panel Member shall be entitled to attend, and to speak and vote at, every meeting of the Panel.

C5.11 All decisions of the Panel shall be by resolution. In order for a resolution of the Panel to be passed at a meeting, a simple majority of those Panel Members voting at that meeting must vote in favour of that resolution.

C5.12 A resolution in writing signed by or on behalf of all the Panel Members shall be as valid and effective as if it had been passed at a meeting of the Panel duly convened and held. Such a resolution may be signed in any number of counterparts.

Attendance by other persons

C5.13 One representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Panel:

(a) the Secretary of State;

(b) the Authority; and

(c) any other person that the Panel determines, or the Panel Chair directs, should be invited to attend.

C5.14 Any Party shall be entitled to send a representative to attend a Panel meeting provided that Party gives the Secretariat at least 3 Working Days' notice in advance of such meeting (or such shorter period of notice as the Panel Chair may approve). Such a representative shall be entitled to attend and (at the Panel Chair's invitation) speak at (but in no circumstances vote at) the meeting.

C5.15 The Panel Chair may (at his or her discretion on grounds of confidentiality) exclude from any part of a Panel meeting persons admitted pursuant to Section C5.13(c) or C5.14.

Minutes of Panel Meetings

C5.16 The Secretariat shall, following each Panel meeting (and in any event at or before the next Panel meeting), circulate copies of the minutes of that meeting to each person who was entitled to receive a notice of that meeting. The Panel may determine that certain parts of a meeting are confidential, in which case those matters will not be included in the minutes circulated to persons other than the Panel, the Secretary of State and the Authority.

C5.17 If any Panel Member disagrees with any item of the minutes, he shall notify the Secretariat of those items with which he or she disagrees, and the Secretariat shall incorporate those items upon which there is disagreement into the agenda for the next following meeting of the Panel.

C5.18 The Secretariat shall maintain a record of all resolutions voted on by the Panel,

indicating how each Panel Member voted on each resolution, and shall make such record available on request to any Party.

Alternates

C5.19 Each Panel Member may, from time to time by notice in writing to the Secretariat, appoint another natural person to act as his or her alternate (an **Alternate**). The Panel Chair must appoint a person to act as his or her Alternate.

C5.20 Each such Alternate must, before his or her appointment as such can become valid, have provided the confirmations referred to in Sections C3.8(a) and (c) (Panel Member Confirmation).

C5.21 Where a Panel Member does not attend at a Panel meeting, the Panel Member's Alternate shall be entitled to attend (and count, in his capacity as Alternate, towards the quorum at) that meeting, and to exercise and discharge all the functions, powers and duties of the Panel Member at that meeting.

C5.22 Each Panel Member may, by notice in writing to the Secretariat, remove or replace the person appointed from time to time by that Panel Member as his or her Alternate. An Alternate shall immediately cease to be an Alternate on the occurrence of any of the events set out in Section C4.5 (Removal of Elected Members) in respect of the Alternate. Where an Alternate's appointor ceases to be a Panel Member for any reason, the Alternate's role as such shall also cease.

C5.23 Unless the context otherwise requires, any reference in this Code to a Panel Member shall be construed as including a reference to that Panel Member's Alternate.

Conflicts of interest

C5.24 Given the duty of each Panel Member to act independently, as set out in C3.7 (Duties of the Panel), conflicts of interest should not regularly arise.

C5.25 Notwithstanding Section C5.24, where a decision of the Panel will have particular consequences for a particular Party or class of Parties, each Panel Member shall consider whether that decision presents a conflict of interest (whether because such Party or Parties comprise Related Persons of the Panel Member or otherwise).

C5.26 Where a Panel Member considers that a decision does present a conflict of interest, the Panel Member shall absent him or herself from the Panel meeting for that decision and abstain from the vote regarding that decision. Furthermore, where the Panel Chair considers that a decision does present a conflict of interest for a Panel Member, the Panel Chair may require the Panel Member to absent him or herself from the Panel meeting for that decision and to abstain from the vote regarding that decision.

C6 SUB-COMMITTEES

Sub-Committees

C6.1 The Panel may establish committees (**Sub-Committees**) for the purposes of doing or assisting the Panel in doing anything to be done by the Panel pursuant to this Code. The Panel shall establish those Sub-Committees expressly provided for in this Code.

C6.2 The Panel may establish a Sub-Committee on a standing basis or for a fixed period or a finite purpose.

C6.3 The Panel may decide that any Sub-Committee (other than one whose establishment is expressly provided for in this Code) is to be dissolved. Those Sub-Committees expressly provided for in this Code are to remain established for so long as they are provided for in this Code.

C6.4 Subject to Section C6.5, the Panel may delegate to any Sub-Committee such of the duties, powers and functions of the Panel as the Panel may specify. The Panel shall delegate to any Sub-Committee expressly provided for in this Code all of the duties, powers, and functions of the Panel relating to the functions of that Sub-Committee described in this Code.

Working Groups

C6.5 The Panel may not establish Sub-Committees to undertake the functions expressly reserved to Working Groups under Section D (Modification Process). Working Groups are to be subject to the requirements of Section D6 (Refinement Process), which may impose requirements by reference to this Section C6.

Membership

C6.6 Each Sub-Committee expressly provided for in this Code shall be composed of such persons as are determined in accordance with the provisions of this Code (if any) that prescribe such membership (and otherwise in accordance with Section C6.7).

C6.7 Subject to Section C6.6:

(a) each Sub-Committee shall be composed of such persons of suitable experience

and qualifications as the Panel shall decide and as are willing to serve thereon, and which may include any Panel Member;

(b) before establishing each Sub-Committee, the Panel shall invite (by such means as it considers appropriate) applications from individuals who wish to serve on that Sub-Committee;

(c) once a Sub-Committee has been established, the Panel may admit such additional persons to, or remove any person from, that Sub-Committee as the Panel considers appropriate (including on the application of any Party or any member of the Sub-Committee).

C6.8 Each person serving on a Sub-Committee shall, when acting in that capacity:

(a) act independently, not as a delegate, and without undue regard to the interests, of any Related Person; and

(b) act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

Member Confirmation

C6.9 Unless the Panel otherwise directs, a person who is to serve on a Sub-Committee shall not do so unless he or she has first provided a written confirmation to SECCo (for the benefit of SECCo and each Party) that that person:

(a) agrees to serve on the Sub-Committee in accordance with this Code, including the requirements of Section C6.8; and

(b) will be available as reasonably required throughout his or her term of office, both to attend Sub-Committee meetings and to undertake work outside those meetings as may reasonably be required.

Terms of Reference and Procedural Requirements

C6.10 The Panel shall set out in writing the duties, powers, and functions of the Panel that it has delegated to each Sub-Committee. The Panel shall also specify in the same document the terms of reference and procedural rules that are to be followed by the

Sub-Committee (which may be revised from time to time by the Panel); provided that, in the case of Sub-Committees expressly provided for in this Code, the Panel must specify terms of reference and procedural rules consistent with the requirements (if any) expressly set out in this Code.

C6.11 Save to the extent otherwise specified by the Panel in accordance with Section C6.10, each Sub-Committee shall conduct its business in accordance with the requirements applying to the Panel in accordance with Section C5 (Proceedings of the Panel).

C6.12 No Sub-Committee may further delegate any of its duties, powers and functions unless expressly authorised to do so by the terms of reference and procedural rules specified in accordance with Section C6.10.

Decisions of Sub-Committees

C6.13 Resolutions of Sub-Committees shall only have binding effect as decisions of the Panel if the Panel has formally delegated the decision-making powers to the Sub-Committee.

C6.14 The Panel shall be deemed to have delegated its decision-making powers to each Sub-Committee expressly provided for in this Code, insofar as such decision-making powers relate to the functions of the Sub-Committee. The delegation of decision-making powers to any other Sub-Committee shall require the unanimous agreement of all Panel Members at the meeting at which the decision to delegate such powers is agreed.

C6.15 For the avoidance of doubt, the delegation to a Sub-Committee of any duties, powers and functions of the Panel shall not relieve the Panel of its general responsibility to ensure that such duties, powers and functions are exercised in accordance with this Code.

C7 CODE ADMINISTRATOR, SECRETARIAT AND SECCO

Code Administrator

C7.1 The Panel may, from time to time, appoint and remove, or make arrangements for the appointment and removal of, one or more persons to be known as the **Code Administrator**.

C7.2 The Code Administrator shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Panel may assign to the Code Administrator from time to time. In particular, the Code Administrator shall:

(a) comply with the Code Administration Code of Practice and perform its tasks and functions in a manner consistent with the Code Administration Code of Practice Principles (provided that the requirements of this Code shall apply in the event of any inconsistencies between this Code and the requirements of the Code Administration Code of Practice);

(b) in conjunction with the other persons named as code administrators in the Code Administration Code of Practice, review and where appropriate propose to the Authority that amendments be made to the Code Administration Code of Practice (subject always to the Authority's approval of those amendments);

(c) report to the Panel on any inconsistencies between this Code and the requirements of the Code Administration Code of Practice;

(d) support the process by which Applicants apply to become a Party, as set out in Section B (Accession);

(e) support the process for Modifications, as set out in Section D (Modification Process);

(f) facilitate a process whereby Parties can submit a potential Modification Proposal to the Code Administrator to have that potential variation developed, refined and discussed prior to the Party deciding whether to formally submit a Modification Proposal (whether through the Change Board or another forum);

(g) support the process by which Parties become Users, as set out in Section H1 (User Entry Process);

(h) act as a critical friend in providing assistance and support to Parties (and prospective Parties) in relation to the other tasks and functions to be performed by the Code Administrator, with a view to providing particular assistance and support to small Parties and the Consumer Members;

(i) without prejudice to the generality of Section C7.2(i), provide support and assistance to the Proposer of a Modification Proposal, including assistance in understanding this Code so as to properly frame the Modification Proposal;

(j) advise the Panel (and Sub-Committees and Working Groups) as to, and in respect of, the matters of which it is necessary or appropriate that the Panel (or the Sub-Committee or Working Group) should be aware in order to discharge their functions in accordance with this Code; and

(k) provide or procure such information in connection with the implementation of this Code as the Panel may require.

C7.3 The Panel shall be responsible for ensuring that the Code Administrator undertakes its tasks and functions in respect of this Code. In particular, the Panel shall ensure that the arrangements under which the Code Administrator is appointed oblige the Code Administrator to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

C7.4 Subject to the other requirements of this Section C7, the Code Administrator shall be appointed by the Panel on such terms and conditions and in return for such remuneration as the Panel sees fit.

C7.5 In no event shall the Code Administrator be a Party, an Affiliate of a Party, an employee of a Party, an employee of an Affiliate of a Party, a DCC Service Provider, an Affiliate of a DCC Service Provider, an employee of a DCC Service Provider, or an employee of an Affiliate of a DCC Service Provider.

Secretariat

C7.6 The Panel may, from time to time, appoint and remove, or make arrangements for the appointment and removal of, one or more persons to be known as the **Secretariat**.

C7.7 The Secretariat shall perform those tasks and functions expressly ascribed to it under this Code, and any other tasks and functions as the Panel may assign to the Secretariat from time to time. In particular, the Secretariat shall:

(a) support the election of Elected Members, as set out in Section C4 (Elected Members);

(b) support the proceedings of the Panel (and Sub-Committees and Working Groups), as set out in Section C5 (Proceedings of the Panel);

(c) provide or procure such facilities and services in connection with the operation of the Panel (and Sub-Committees and Working Groups) as the Panel may require;

(d) maintain each Party's Party Details, as set out in Section M6 (Party Details);

(e) procure the creation, hosting and maintenance of the Website; and

(f) make an accurate and up-to-date copy of this Code available on the Website.

C7.8 The Panel shall be responsible for ensuring that the Secretariat undertakes its tasks and functions in respect of this Code. In particular, the Panel shall ensure that the arrangements under which the Secretariat is appointed oblige the Secretariat to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

C7.9 Subject to the other requirements of this Section C7, the Secretariat shall be appointed by the Panel on such terms and conditions and in return for such remuneration as the Panel sees fit.

C7.10 In no event shall the Secretariat be a Party, an Affiliate of a Party, an employee of a Party, an employee of an Affiliate of a Party, a DCC Service Provider, and Affiliate of a DCC Service Provider, an employee of a DCC Service Provider, or an employee of

an Affiliate of a DCC Service Provider.

SECCo

C7.11 SECCo shall be established in accordance with Schedule 4.

C7.12 SECCo shall act as a corporate vehicle in relation to the business of the Panel, including:

(a) ~~-~~entering into any contractual arrangements in order to give effect to any resolution of the Panel which it is necessary or desirable to implement by means of a binding contract; and

~~(a)~~(b) becoming a Subscriber for IKI Certificates as directed by the Panel for the purpose of exercising any function of the Panel under this Code.~~-~~

C8 PANEL COSTS AND BUDGETS

General

C8.1 The costs and expenses incurred by (or on behalf of) the Panel in exercising its powers and performing its duties in respect of this Code shall be incurred by SECCo, and the DCC shall provide SECCo with the funds necessary to meet such costs and expenses.

SEC Costs and Expenses

C8.2 The costs and expenses capable of recovery under this Section C8 (the **Recoverable Costs**) shall be all the reasonable costs and expenses incurred:

(a) subject to Section C8.3, by the Panel Members in their capacity as such (including in their capacity as directors of SECCo);

(b) subject to Section C8.3, by those serving on Sub-Committees (but not, for the avoidance of doubt, Working Groups) in their capacity as such;

(c) by SECCo under or in connection with this Code; or

(d) by SECCo under or in connection with contracts that SECCo has entered into in accordance with this Code, including the contracts for:

(i) the appointment of the Code Administrator and the Secretariat;

(ii) the appointment of the Panel Chair;

(iii) the appointment of any person serving on a Sub-Committee expressly provided for in this Code where that person is expressly stated to be remunerated; and

(iv) the appointment of advisers,

(in each case) provided that such costs or expenses are provided for in, or otherwise consistent with, an Approved Budget.

C8.3 Subject to the terms of those contracts referred to in Sections C8.2(d):

(a) each Panel Member and each person serving on a Sub-Committee shall be entitled to recover all reasonable travel expenses properly incurred by them in their roles as such (and the Panel shall establish a policy that sets out guidelines regarding what constitutes reasonable travel expenses); and

(b) no Panel Member or person serving on a Sub-Committee shall be entitled to a salary in respect of their role as such, or to any payment in respect of time they incur in their role as such.

Reimbursing Panel Members

C8.4 Where a Panel Member or person serving on a Sub-Committee wishes to recover any Recoverable Costs, he or she shall submit evidence of the Recoverable Costs in question to the Panel (or a named person approved by the Panel) for approval. The cost or expense in question shall only be approved to the extent that it is a Recoverable Cost, and only if the evidence is submitted in a timely manner (and in any event on or before the 20th Working Day following the end of the relevant Regulatory Year). Once approved, the evidence of the Recoverable Cost shall be submitted to SECCo for payment.

C8.5 Within 20 Working Days following receipt of evidence of a Recoverable Cost that has been approved in accordance with Section C8.4, SECCo shall pay the relevant amount to the relevant person.

SEC Costs to be Reimbursed by DCC

C8.6 The Recoverable Costs incurred by SECCo shall be reimbursed to SECCo by the DCC.

C8.7 SECCo may periodically invoice the DCC for the Recoverable Costs incurred, or reasonably expected to be incurred, by SECCo; provided that SECCo shall deduct from such Recoverable Costs amounts that SECCo has received by way of Application Fee payments and any amounts that represent previous overpayments by the DCC (due to the inaccuracy of SECCo estimates, or otherwise).

C8.8 The DCC shall pay each invoice submitted by SECCo in accordance with Section

C8.7 within 10 Working Days of receipt of such invoice by the DCC.

C8.9 It is acknowledged that the DCC is entitled to recover amounts paid by it to SECCo in accordance with this Section C8 through the Charges (subject to the requirements of the DCC Licence).

C8.10 In the event that the DCC does not pay SECCo in accordance with Section C8.8, and subject to prior approval from the Authority, SECCo may invoice the Parties who hold Energy Licences for the unpaid amount (and those Parties shall pay the invoiced amounts to SECCo as if they were Charges). Where this Section C8.10 applies, the amount to be paid by each Party shall be determined in accordance with a methodology approved by the Authority, and all amounts paid shall be reimbursed by SECCo to the relevant Party (plus interest at the Non-Default Interest Rate) at such time as the Authority may determine.

Draft Budgets and Work Plans

C8.11 The Panel shall, during January of each year, prepare and circulate to all the Parties a draft budget for the next three Regulatory Years commencing thereafter (a **Draft Budget**).

C8.12 Each Draft Budget shall set out the Panel's good-faith estimate of the Recoverable Costs that it anticipates will be incurred (or committed to) during the relevant Regulatory Years, and shall be accompanied by a detailed work plan showing the activities and projects to which the relevant costs and expenses relate. Each Draft Budget must provide for limits (both individually and in the aggregate) on costs and expenses not expressly provided for in the budget which can be incurred without having to amend the budget.

Approval of Budgets

C8.13 In respect of the Draft Budget circulated in January for the next Regulatory Year commencing thereafter, the Panel shall:

(a) arrange for the circulation to all the Parties of the comments received from the Parties regarding the Draft Budget in the 20 Working Days following its

circulation;

(b) consider and respond to those comments, and circulate its responses to all the Parties;

(c) to the extent that it considers it appropriate to do so, amend the Draft Budget and/or the accompanying work plan in the light of those comments;

(d) approve the Draft Budget (subject to any such amendments) and publish that budget and the accompanying work plan on the Website; and

(e) specify a date in such publication (being not less than 15 Working Days following the date of publication) from which such budget will (subject to Section C8.14) become the **Approved Budget** for the relevant Regulatory Year.

Appeal of Budget

C8.14 Each of the Parties or Citizens Advice or Citizens Advice Scotland may appeal to the Authority the Panel's approval of a budget as the Approved Budget for a Regulatory Year. Any such appeal will only be validly made if notified to the Authority within 10 Working Days following the publication of such Draft Budget pursuant to Section C8.13(e), and if copied to the Panel. In the event an appeal is validly made, the Panel shall arrange for a copy of the appeal to be circulated to all the Parties, and:

(a) the Authority may give notice that it dismisses the appeal where it considers that the appeal is trivial or vexatious or has no reasonable prospect of success, in which case the budget approved by the Panel shall remain the Approved Budget; or

(b) the Authority may give notice that it will further consider the appeal, in which case the budget approved by the Panel shall remain the Approved Budget pending and subject to any interim directions issued by the Authority, and:

(i) where the Authority determines that the budget approved by the Panel is consistent with the General SEC Objectives, then such budget shall remain the Approved Budget; or

(ii) where the Authority determines that the budget approved by the Panel is not consistent with the General SEC Objectives, then either (as directed by the Authority):

(A) such budget shall be amended in such manner as the Authority may direct, and such budget as so amended will be Approved Budget; or

(B) the Panel shall produce a further Draft Budget and re-commence the process set out in Section C8.13.

Amendments to Budgets

C8.15 The Approved Budget relating to each Regulatory Year may be amended by the Panel from time to time (whether before during or after that Regulatory Year, and including in respect of Recoverable Costs already incurred), provided that the Panel has first:

(a) circulated and invited comments on the proposed amendments in accordance with Section C8.13 as if it were a Draft Budget; and

(b) circulated and considered any comments received on the proposed amendments within 20 Working Days of such circulation on the same basis as is referred to in Section C8.13.

Reports

C8.16 The Panel shall, as soon as is reasonably practicable following the end of each Regulatory Year, produce and circulate to Parties a report on the costs and expenses incurred (or committed to) during that Regulatory Year and the activities and projects to which those costs and expenses relate.

Audit

C8.17 The Panel shall arrange for the monies paid by and to SECCo pursuant to this Section C8 during each Regulatory Year to be audited by a firm of chartered accountants on an annual basis in order to verify whether the requirements of this Section C8 have been met.

C8.18 The Panel shall send a copy of such auditor's report to all the Parties within 10 Working Days of its receipt by the Panel.

SECTION D – MODIFICATION PROCESS

D1 RAISING MODIFICATION PROPOSALS

Modifications

D1.1 This Code may only be varied in accordance with the provisions of this Section D.

D1.2 Each variation of this Code must commence with a proposal made in accordance with the provisions of this Section D1 (a **Modification Proposal**).

Persons Entitled to Submit Modification Proposals

D1.3 A Modification Proposal may be submitted by any of the following persons (the **Proposer**):

(a) a Party;

(b) Citizens Advice or Citizens Advice Scotland;

(c) any person or body that may from time to time be designated in writing by the Authority for the purpose of this Section D1.3;

(d) the Authority or the DCC acting at the direction of the Authority, but in each case only in respect of variations to this Code which the Authority reasonably considers are necessary to comply with or implement:

(i) the EU Regulations; and/or

(ii) any relevant legally binding decisions of the European Commission and/or the Agency for the Co-operation of Energy Regulators; and

(e) the Panel (where all Panel Members at the relevant meeting vote unanimously in favour of doing so), but only in respect of variations to this Code which are intended to give effect to:

(i) recommendations contained in a report published by the Panel pursuant to Section C2.3(i) (Panel Duties);

(ii) recommendations contained in a report published by the Code Administrator pursuant to Section C7.2(c) (Code Administrator);

(iii) Fast-Track Modifications (as described in Section D2 (Modification Paths)); and/or

(iv) consequential changes to this Code required as a result of changes proposed or already made to one or more other Energy Codes.

Form of the Proposal

D1.4 The Proposer must submit a Modification Proposal to the Code Administrator.

D1.5 The Code Administrator shall from time to time publish a prescribed form of Modification Proposal on the Website. The prescribed form must require the provision by the Proposer of all of the information set out in Section D1.7, and any other information that the Panel may reasonably approve.

D1.6 Each Proposer must use the prescribed form when submitting a Modification Proposal.

Content of the Proposal

D1.7 A Modification Proposal must contain the following information:

(a) the name of the Proposer;

(b) the name and contact details of an employee or representative of the Proposer who will act as a principal point of contact in relation to the proposal;

(c) the date on which the proposal is submitted;

(d) a description in sufficient detail of the nature of the proposed variation to this Code and of its intended purpose and effect;

(e) a statement of whether, in the opinion of the Proposer, the Modification Proposal should be a Path 1 Modification, a Path 2 Modification or a Path 3 Modification;

(f) a statement of whether the Proposer considers, in the light of any guidance on the topic issued by the Authority from time to time, that the Modification Proposal should be treated as an Urgent Proposal (and, if so, its reasons for so considering);

(g) a statement of whether or not the Modification Proposal is intended to be a Fast-Track Modification (bearing in mind that only the Panel may raise Fast-Track Modifications);

(h) a statement of the reasons why the Proposer believes that this Code would, if the proposed variation were made, better facilitate the achievement of the SEC Objectives than if that variation were not made;

(i) a statement of whether the Proposer believes that there would be a material impact on Greenhouse Gas Emissions as a result of the proposed variation being made;

(j) a statement as to which parts of this Code the Proposer considers would require to be amended in order to give effect to the proposed variation or as a consequence of that variation (including legal drafting if the Proposer so wishes);

(k) a statement as to which Party Categories, in the opinion of the Proposer, are likely to be affected by the proposed variation;

(l) a statement of whether changes are likely to be required to other Energy Codes as a result of the proposed variation being made;

(m) a statement of whether, in the opinion of the Proposer, the Modification Proposal will require changes to DCC Systems, User Systems and/or Smart Metering Systems; and

(n) the timetable in accordance with which the Proposer recommends that the proposed variation should be implemented (including the proposed implementation date).

Modification Register

D1.8 The Secretariat shall establish and maintain a register (the **Modification Register**) of all current and past Modification Proposals from time to time.

D1.9 The Modification Register shall contain, in respect of each Modification Proposal submitted pursuant to this Section D1:

(a) a unique reference number by which the Modification Proposal can be identified;

(b) a brief summary of the Modification Proposal and its purpose and effect;

(c) a copy of (or internet link to) the Modification Proposal;

(d) the stage of the process set out in this Section D that the Modification Proposal has reached;

(e) following the Modification Proposal's initial consideration by the Panel pursuant to Section D3:

(i) whether it is a Path 1 Modification, a Path 2 Modification or a Path 3 Modification;

(ii) whether the proposal is a Fast-Track Proposal; and

(iii) the timetable applying in respect of the Modification Proposal;

(f) whether the Authority has determined the Modification Proposal to be an Urgent Proposal;

(g) where the Modification Proposal has been submitted to the Refinement Process, the agendas and minutes for Working Group meetings;

(h) once it has been produced, the Modification Report for the Modification Proposal;

(i) once it has been made, the decision of the Panel (in the case of Fast-Track Modifications) or of the Change Board (in the case of all other Modification

Proposals); and

(j) such other matters relating to the Modification Proposal as the Panel may reasonably determine from time to time.

D1.10 The Secretariat shall ensure that the Modification Register is updated at regular intervals so that the information it contains in relation to each Modification Proposal is, so far as is reasonably practicable, accurate and up-to-date.

D1.11 The Secretariat shall ensure that the Modification Register is published on the Website, and that a copy of the Modification Register is sent to each Party at least once every month.

Representations from Parties

D1.12 Each Party shall be free to make written representations from time to time regarding each Modification Proposal. Such representations should be made to the Code Administrator in the first instance. The Code Administrator shall:

(a) in the case of Fast-Track Modifications, bring such representations to the attention of the Panel;

(b) in the case of Modifications Proposals (other than Fast-Track Modifications) which are not following the Refinement Process, consider such representations when producing the Modification Report; and

(c) in the case of Modifications Proposals (other than Fast-Track Modifications) which are following the Refinement Process, bring such representations to the attention of the relevant Working Group.

D2 MODIFICATION PATHS

General

D2.1 Each Modification Proposal will follow one of four modification paths (as described in this Section D2). The modification path to be followed in respect of a Modification Proposal will depend upon the nature of the variation proposed in the Modification Proposal.

D2.2 The Panel's determination (whether under Section D3.6 or subsequently) of whether a Modification Proposal is a Path 1 Modification, a Path 2 Modification or a Path 3 Modification shall be conclusive unless and until any contrary determination is made by the Authority in accordance with Section D4 (Authority Determinations).

D2.3 Where the Panel raises a Fast-Track Modification, such Modification Proposal shall be treated as a Fast-Track Modification unless and until any contrary determination is made by the Authority in accordance with Section D4 (Authority Determinations).

Path 1 Modifications: Authority-led

D2.4 A Modification Proposal that proposes variations to this Code that satisfy one or more of the following criteria shall have the status of a **Path 1 Modification**:

(a) the variations arise out of a Significant Code Review and the Authority directs the DCC to submit the Modification Proposal; and/or

(b) the Modification Proposal is submitted by the Authority or the DCC at the direction of the Authority pursuant to Section D1.3(d).

D2.5 The DCC shall submit a Modification Proposal in respect of any variations arising out of a Significant Code Review that the DCC is directed to submit by the Authority.

Path 2 Modifications: Authority Determination

D2.6 Unless it is a Path 1 Modification, a Modification Proposal that proposes variations to this Code that satisfy one or more of the following criteria shall have the status of a **Path 2 Modification**:

(a) the variations are likely to have a material effect on existing or future Energy Consumers;

(b) the variations are likely to have a material effect on competition in the Supply of Energy or Commercial Activities connected with the Supply of Energy;

(c) the variations are likely to have a material effect on the environment, on access to or privacy of Data, on security of the Supply of Energy, and/or on the security of Systems and/or Smart Metering Systems;

(d) the variations are likely to have a material effect on the arrangements set out in Section C (Governance) or this Section D; and/or

(e) the variations are likely to unduly discriminate in their effects between one Party (or class of Parties) and another Party (or class of Parties).

Path 3 Modification: Self-Governance

D2.7 A Modification Proposal that is not a Path 1 Modification, a Path 2 Modification or a Fast Track Modification shall have the status of a **Path 3 Modification**.

Fast-Track Modifications

D2.8 The Panel may itself raise Modification Proposals where it considers it necessary to do so to correct typographical or other minor errors or inconsistencies in this Code (**Fast-Track Modifications**).

D3 INITIAL CONSIDERATION OF MODIFICATION PROPOSALS

Invalid Modification Proposals

D3.1 The Code Administrator shall refuse (and may only refuse) to accept the submission of a Modification Proposal that is not submitted:

(a) by a person entitled to submit Modification Proposals in accordance with Section D1.3 (Persons Entitled to Submit Modification Proposals); and/or

(b) in the form, and containing the content, required by Sections D1.6 (Form of the Proposal) and D1.7 (Content of the Proposal).

D3.2 Where the Code Administrator refuses to accept the submission of a Modification Proposal, it shall notify the Panel and the Proposer of that refusal as soon as is reasonably practicable, setting out the grounds for such refusal.

D3.3 Where the Panel is notified that the Code Administrator has refused to accept the submission of a Modification Proposal, the Panel may instruct the Code Administrator to accept the submission of that proposal (and Section D3.4 shall apply as if the Code Administrator had not refused to accept the Modification Proposal).

Initial Comment by the Code Administrator

D3.4 Unless the Code Administrator has refused to accept the submission of the Modification Proposal, the Code Administrator shall, within the time period reasonably necessary to allow the Panel to comply with the time periods set out in Section D3.5, submit to the Panel:

(a) each Modification Proposal; and

(b) without altering the Modification Proposal in any way and without undertaking any detailed evaluation of the Modification Proposal, the Code Administrator's written views on the matters that the Panel is to consider under Section D3.6.

Initial Consideration by the Panel

D3.5 The Panel shall consider each Modification Proposal and the accompanying documents referred to in section D3.4:

(a) in the case of Modification Proposals expressed by the Proposer to be urgent, within 5 Working Days after the proposal's submission; and

(b) in respect of all other Modification Proposals, at the next Panel meeting occurring more than 6 Working Days after the Modification Proposal's submission (provided that, in the case of Fast-Track Modifications, the Panel shall not consider the Modification Proposal earlier than 15 Working Days after it was raised).

D3.6 In considering each Modification Proposal pursuant to Section D3.6, the Panel shall determine:

(a) whether to refuse the Modification Proposal in accordance with Section D3.8;

(b) whether the Modification Proposal is a Path 1 Modification, a Path 2 Modification or a Path 3 Modification (taking into account the view expressed by the Proposer in the Modification Proposal and as described in Section D2);

(c) whether the Authority should be asked to consider whether the Modification Proposal should be treated as an Urgent Proposal (and, where the Proposer has expressed the Modification Proposal to be urgent, the Panel shall so ask the Authority);

(d) in the case of Fast-Track Modifications, whether the Modification Proposal should be approved or withdrawn (and such approval shall require the unanimous approval of all the Panel Members present at the relevant meeting);

(e) whether, in accordance with Section D3.9, it is necessary for the Modification Proposal to go through the Refinement Process, or whether it can progress straight to the Report Process;

(f) the timetable to apply in respect of the Modification Proposal, in accordance

with the criteria set out in Section D3.10; and

(g) whether the Modification Proposal should be considered together with any other current Modification Proposal(s) (whether because they complement or contradict one another or for any other reason), in which case the Modification Proposals in question shall be considered by the same Working Group.

D3.7 The Secretariat shall, as soon as reasonably practicable following the Panel's determination under Section D3.6 in respect of each Modification Proposal, confirm that determination to the Proposer and update the Modification Register.

Refusal by the Panel

D3.8 The Panel may not refuse a Path 1 Modification. Save in the case of Path 1 Modifications, the Panel may choose to refuse a Modification Proposal if that Modification Proposal has substantively the same effect as another Modification Proposal which was submitted by a Proposer on an earlier date and which:

(a) has not been refused, approved, rejected or withdrawn pursuant to this Section D at the time of the Panel's decision under this Section D3.8; or

(b) was refused or rejected pursuant to this Section D on a date falling within the period of two months immediately preceding the time of the Panel's decision under this Section D3.8.

Determining whether the Refinement Process should be followed

D3.9 The Panel shall determine whether each Modification Proposal must go through the Refinement Process, or whether it can progress straight to the Report Process. The Panel shall ensure that the following Modification Proposals are subject to the Refinement Process:

(a) those submitted by the Panel itself (other than Fast-Track Modifications);

(b) those that the Panel considers are likely to have an impact on the ability of the DCC to discharge its duties and comply with its obligations under the Relevant Instruments;

(c) those that the Panel considers are likely to require changes to DCC Systems, User Systems and/or Smart Metering Systems; or

(d) any other Modification Proposals, unless the Panel considers them to be clearly expressed and concerned solely with:

(i) insubstantial or trivial changes that are unlikely to be controversial (including typographical errors and incorrect cross-references); and/or

(ii) giving effect to variations that are mandated by the Relevant Instruments in circumstances where there is little or no discretion as to how they are to be given effect.

Timetable

D3.10 The Panel shall determine the timetable to be followed in respect of each Modification Proposal. In particular, the Panel shall:

(a) in the case of Path 1 Modifications, determine a timetable consistent with any relevant timetable issued by the Authority;

(b) in the case of Urgent Proposals, determine a timetable that is (or amend the existing timetable so that it becomes) consistent with any relevant timetable issued by the Authority; and

(c) (subject to Sections D3.10(a) and (b)) specify the date by which the Modification Report is to be finalised; being as soon as reasonably practicable after the Panel's decision in respect of such timetable (having regard to the complexity, importance and urgency of the Modification Proposal).

D3.11 The Panel may, whether at its own initiation or on the application of another person, determine amendments to the timetable applying from time to time to each Modification Proposal; provided that any such amendment is consistent with Section D3.10. The Secretariat shall, as soon as reasonably practicable following any Panel determination under this Section D3.11, confirm that determination to the Proposer and the Change Board and update the Modification Register.

D3.12 The Panel, the Code Administrator, the Secretariat, any relevant Working Group, the Change Board and the Parties shall each (insofar as within its reasonable control) complete any and all of the respective tasks assigned to them in respect of a Modification Proposal in accordance with the timetable applying to that Modification Proposal from time to time (including as provided for in Section D4.9).

D4 AUTHORITY DETERMINATIONS

Authority Determination of Modification Path

D4.1 This Section D4.1 applies in respect of each Modification Proposal that the Panel has determined to be a Path 2 Modification or a Path 3 Modification. The Authority may:

(a) at its own initiation, or on the application of a Party or Citizens Advice or Citizens Advice Scotland; and

(b) having consulted with the Panel,

determine that the Modification Proposal should properly (in accordance with Section D2) be considered (in the case of a Path 2 Modification) to be a Path 3 Modification or be considered (in the case of a Path 3 Modification) to be a Path 2 Modification. Any such determination shall be final and binding for the purposes of this Code.

Referral of Disputes to the Authority

D4.2 Where the Panel:

(a) refuses a Modification Proposal pursuant to Section D3 (Initial Consideration of Modification Proposals);

(b) determines that the Modification Proposal is a Path 1 Modification, a Path 2 Modification or a Path 3 Modification where such determination differs from the view of the Proposer expressed in the Modification Proposal; and/or

(c) determines a timetable (or an amendment to the timetable) in respect of the Modification Proposal which the Proposer considers inconsistent with the requirements of Section D3 (Initial Consideration of Modification Proposals),

then the Proposer may refer the matter to the Authority for determination in accordance with Section D4.3.

D4.3 The Proposer may only refer a matter to the Authority pursuant to Section D4.2 where such referral is made within 10 Working Days of the Proposer being notified by the Secretariat of the relevant matter. The Proposer shall send to the Panel a copy of any

referral made pursuant to this Section D4.3.

D4.4 Where the Authority, after having consulted with the Panel, considers that the Panel's decision that is the subject of a matter referred to the Authority by a Proposer in accordance with Section D4.3 was made otherwise than in accordance with Section D3, then the Authority may determine the matter. Any such determination shall be final and binding for the purposes of this Code.

Authority Determination in respect of Urgent Proposals

D4.5 Where a Proposer has expressed a Modification Proposal to be urgent and/or where the Panel considers a Modification Proposal to be urgent, the Panel shall ask the Authority whether the Modification Proposal should be treated as an Urgent Proposal.

D4.6 A Modification Proposal shall only be an **Urgent Proposal** where the Authority directs the Panel to treat the Modification Proposal as an Urgent Proposal (whether following a referral by the Panel pursuant to Section D4.5, or at the Authority's own initiation).

D4.7 An Urgent Proposal shall be progressed:

(a) in accordance with any timetable specified by the Authority from time to time, and the Panel shall not be entitled to vary such timetable without the Authority's approval; and

(b) subject to any deviations from the procedure set out in this Section D as the Authority may direct (having consulted with the Panel).

Authority Determination in respect of Significant Code Reviews

D4.8 During a Significant Code Review Phase:

(a) the Panel shall report to the Authority on whether or not the Panel considers that any Modification Proposal on which the Change Board had not voted prior to the commencement of the Significant Code Review (whether submitted before or after the commencement of the Significant Code Review) falls within the scope of the Significant Code Review;

(b) the Panel may (subject to Section D4.8(d)) suspend the progress of any Modification Proposal that the Panel considers to fall within the scope of that Significant Code Review;

(c) the Authority may (subject to Section D4.8(d)) direct the Panel to suspend the progress of any Modification Proposal that the Authority considers to fall within the scope of that Significant Code Review (and the Panel shall comply with such directions); and

(d) the Authority may direct the Panel to cease the suspension of any Modification Proposal that has been suspended pursuant to this Section D4.8 (and the Panel shall comply with such directions). Any and all suspensions pursuant to this Section D4.8 shall automatically cease at the end of the Significant Code Review Phase.

D4.9 The commencement and cessation of suspensions in respect of a Modification proposal pursuant to Section D4.8 shall have the effect of modifying the timetable applying to that Modification Proposal.

D5 WITHDRAWAL BY PROPOSER

Right to Withdraw

D5.1 Subject to Section D5.2, the Proposer for a Modification Proposal may withdraw the Modification Proposal on notice to the Secretariat at any time prior to the decision of the Change Board in respect of that Modification Proposal.

D5.2 In the case of Path 1 Modifications, the Proposer may only withdraw the Modification Proposal where the Proposer provides evidence that the Authority has given its consent to such withdrawal. The Proposer may not withdraw a Modification Proposal following any direction by the Authority to the Panel pursuant to Section D9.3 (Send-Back Process).

D5.3 As soon as is reasonably practicable after receiving any notice in accordance with Section D5.1, the Secretariat shall notify the Parties that the Proposer has withdrawn its support and shall update the Modification Register accordingly.

Adoption of Withdrawn Proposals

D5.4 Where, within 10 Working Days of the Secretariat sending notice under Section D5.3, the Secretariat receives notice from a Party that it is prepared to adopt the Modification Proposal, such Party shall (for all purposes in respect of this Code) be deemed thereafter to be the Proposer for the Modification Proposal (and, where the Secretariat receives more than one such notice, the first such notice shall have priority over the others).

D5.5 Where Section D5.4 applies, the Modification Proposal shall not be withdrawn, and the Secretariat shall notify the Parties and update the Modification Register.

Withdrawn Proposals

D5.6 Subject to Section D5.5, a Modification Proposal that has been withdrawn in accordance with Section D5.1 shall cease to be subject to the process set out in this Section D.

D6 REFINEMENT PROCESS

Application of this Section

D6.1 This Section D6 sets out the **Refinement Process**. This Section D6 only applies in respect of a Modification Proposal where it is determined that the Modification Proposal is to be subject to the Refinement Process in accordance with Section D3 (Initial Consideration of Modification Proposals). The Refinement Process never applies to Fast-Track Modifications.

Establishment of a Working Group

D6.2 Where this Section D6 applies, the Panel shall establish a group of persons (a **Working Group**) for the purposes set out in Section D6.8.

D6.3 Each Working Group so established must comprise:

(a) at least five individuals who:

(i) each have relevant experience and expertise in relation to the subject matter of the Modification Proposal (provided that there is no need to duplicate the experience and expertise available to the Working Group via the Technical Architecture and Business Architecture Sub-Committee); and

(ii) whose backgrounds are broadly representative of the persons likely to be affected by the Modification Proposal if it is approved,

(and the Panel, with the cooperation of the Parties, shall seek to establish a standing list of persons with potentially relevant experience who may be willing to serve on Working Groups);

(b) where the Proposer nominates such a person, one person nominated by the Proposer; and

(c) a Working Group chair to be (subject to Section D6.4) selected from among the members of the Working Group by such members.

D6.4 The Code Administrator shall attend meetings of the Working Groups established pursuant to this Section D6, and support the activities of such Working Groups. The Code Administrator shall provide feedback to any Party that requests it regarding the progress of the Refinement Process and the outcome of Working Group meetings. Where the Panel or the relevant Working Group so determines, the Code Administrator shall act as chair of a Working Group.

D6.5 A person appointed to serve on a Working Group, when acting in that capacity, shall act in a manner designed to facilitate the performance by the Panel of its duties under this Code.

D6.6 Each person appointed to serve on a Working Group must, before that appointment takes effect, confirm in writing to SECCo (for the benefit of itself and each Party) that that person:

(a) agrees to serve on that Working Group and to do so in accordance with this Code, including the requirements of Section D6.5; and

(b) will be available as reasonably required throughout the Refinement Process for the Modification Proposal, both to attend Working Group meetings and to undertake work outside those meetings as may reasonably be required.

D6.7 Except to the extent inconsistent with this Section D6, the provisions of Section C6 (Sub-Committees) shall apply in respect of each Working Group as if that Working Group was a Sub-Committee.

Purpose of Refinement Process

D6.8 The purpose of the Refinement Process is to:

(a) consider and (to the extent necessary) clarify the likely effects of the Modification Proposal, including to identify the Parties, Party Categories, Energy Consumers and other persons likely to be affected by the Modification Proposal;

(b) evaluate and (to the extent necessary) develop and refine the content of the Modification Proposal;

(c) evaluate and (to the extent necessary) amend the proposed implementation timetable of the Modification Proposal, including (where relevant) so as to ensure consistency with the Panel Release Management Policy (provided that the proposed implementation timetable of a Path 1 Modification cannot be so amended);

(d) consider (to the extent the Working Group considers necessary) the impact which the Modification Proposal would have, if approved, on the matters referred to in Section D6.9;

(e) seek (to the extent the Working Group considers necessary) the Technical Architecture and Business Architecture Sub-Committee's views of the impact which the Modification Proposal would have, if approved, on the DCC Systems and Smart Metering Systems; provided that the Working Group shall always seek such views:

(i) in respect of proposals to modify the Technical Code Specifications; and/or

(ii) where the Technical Architecture and Business Architecture Sub-Committee has notified the Working Group that the Technical Architecture and Business Architecture Sub-Committee wishes to express a view;

(f) seek (to the extent the Working Group considers necessary) the Security Sub-Committee's views on the Modification Proposal; provided that the Working Group shall always seek such views:

(i) in respect of proposals to modify the Security Obligations and Assurance Arrangements; and/or

(ii) where the Security Sub-Committee has notified the Working Group that the Security Sub-Committee wishes to express a view;

(g) seek (to the extent the Working Group considers necessary) the SMKI PMA's views on the Modification Proposal; provided that the Working Group shall

always seek such views:

(i) in respect of proposals to modify the SMKI SEC Documents; and/or

(ii) where the SMKI PMA has notified the Working Group that the SMKI PMA wishes to express a view;

(h) seek (to the extent the Working Group considers necessary) the Alt HAN Forum's views on the Modification Proposal; provided that the Working Group shall always seek such views:

(i) in respect of proposals to modify Section Z (The Alt HAN Arrangements);

(ii) in respect of proposals to modify any SEC Subsidiary Document which relates to Section Z (The Alt HAN Arrangements);

(iii) in respect of proposals to modify Section K (Charging Methodology) which are likely to affect the Alt HAN Charges; and/or

(iv) where the Alt HAN Forum (or a Forum Sub-Group acting on its behalf) has notified the Working Group that it wishes to express a view;

(i) consider whether, if the Modification Proposal is approved, this Code would better facilitate the achievement of the SEC Objectives than if the Modification Proposal was rejected;

(j) consider whether it is likely that there would be a material impact on Greenhouse Gas Emissions as a result of the Modification Proposal being approved, and (if so) assessing such impact (which assessment shall be conducted in accordance with any guidance on the evaluation of Greenhouse Gas Emissions issued by the Authority from time to time); and

(k) consider whether, if the Modification Proposal is approved, changes are likely to be required to other Energy Codes as a result.

Analysis by the DCC

D6.9 At the request of a Working Group established pursuant to this Section D6 in respect of a Modification Proposal, the DCC shall prepare an analysis of how the following matters would be affected if that Modification Proposal were to be approved:

(a) the ability of the DCC to discharge its duties and comply with its obligations under the Relevant Instruments; and/or

(b) the extent to which changes would be required to DCC Systems, User Systems and/or Smart Metering Systems; and (if so) the likely development, capital and operating costs associated with such changes and any consequential impact on the Charges.

D6.10 The DCC shall provide such further explanation of any analysis prepared pursuant to Section D6.9 as the Working Group may reasonably require.

D6.11 In considering whether the approval of a Modification Proposal would better facilitate the achievement of the SEC Objectives than the rejection of the Modification Proposal, the Working Group shall have regard to any analysis provided by the DCC pursuant to Section D6.9.

Working Group Consultation

D6.12 Each Working Group established pursuant to this Section D6 in respect of a Modification Proposal shall consider any representations made to it by Parties from time to time regarding the subject-matter of the Modification Proposal.

D6.13 Each Working Group established pursuant to this Section D6 in respect of a Modification Proposal shall undertake at least one formal consultation in respect of the Modification Proposal seeking views on the matters set out in Section D6.8. The Working Group shall consult with the Parties, Citizens Advice or Citizens Advice Scotland and (where appropriate) any interested third parties (including, where relevant, Energy Consumers and/or those who represent or advise Energy Consumers).

D6.14 Each Working Group established pursuant to this Section D6 in respect of a

Modification Proposal shall publish on the Website, and bring to the Parties' attention, a document (the **Consultation Summary**) containing the following:

(a) the final consultation draft of the Modification Proposal, including in particular the legal text of the proposed variation and the proposed implementation timetable;

(b) all consultation responses received and not marked as confidential; and

(c) a statement of whether the Working Group considers that the approval of the Modification Proposal would better facilitate the achievement of the SEC Objectives than the rejection of the Modification Proposal (and if so why).

Alternative Proposals

D6.15 Alternative Proposals may arise in one of two ways:

(a) where the majority of the Working Group considers that there is more than one variation to this Code that could achieve the purpose of the Modification Proposal (and that each such variation would, if made, better facilitate the achievement of the SEC Objectives than if that variation were not made), then the Working Group may decide to submit more than one proposed variation to this Code (identifying one proposal as its preferred variation, and the others as **Alternative Proposals**); and/or

(b) where the Proposer, or the person appointed to the Working Group pursuant to Section D6.3(b), objects to the proposed variation(s) to this Code preferred by the majority of the Working Group, such person may insist that the variation to this Code that it prefers is included in addition (an **Alternative Proposal**).

D6.16 References in this Section D to a Modification Proposal shall (except where the context otherwise requires) be deemed to include reference to any Alternative Proposal included in accordance with Section D6.15.

D7 REPORT PHASE

Modification Report

D7.1 The Code Administrator shall, in respect of each Modification Proposal, prepare a written report on the proposal (the **Modification Report**); provided that no Modification Report shall be required for Fast-Track Modifications. This stage of the process is referred to as the **Report Phase**.

D7.2 The Code Administrator shall prepare the Modification Report for each Modification Proposal:

(a) where the Refinement Process has been followed, in accordance with the instructions of the relevant Working Group; or

(b) where the Refinement Process has not been followed, on the basis of the Modification Proposal and in consultation with the Proposer.

Content of the Modification Report

D7.3 The Modification Report for each Modification Proposal shall:

(a) be addressed and delivered to the Panel;

(b) set out the legal text of the proposed variation to this Code (and, where applicable, set out the alternative legal text of the Alternative Proposal);

(c) specify the proposed implementation timetable (including the proposed implementation date);

(d) specify the likely effects of the proposed variation if it is implemented;

(e) specify, in the opinion of the Working Group (or, where the Refinement Process was not followed, the Code Administrator), which Party Categories are likely to be affected by the Modification Proposal;

(f) specify whether the implementation of the Modification Proposal will require changes to DCC Systems, User Systems and/or Smart Metering Systems; and (if so) the likely development, capital and operating costs associated with such

changes and any consequential impact on the Charges;

(g) specify whether, if the Modification Proposal is approved, this Code would better facilitate the achievement of the SEC Objectives than if the Modification Proposal was rejected;

(h) specify whether it is likely that there would be a material impact on Greenhouse Gas Emissions as a result of the Modification Proposal being approved, and (if so) assessing such impact (which assessment shall be conducted in accordance with any guidance on the evaluation of Greenhouse Gas Emissions issued by the Authority from time to time);

(i) specify whether, if the Modification Proposal is approved, changes are likely to be necessary to other Energy Codes, and whether changes have been proposed in respect of the affected Energy Codes; and

(j) where the Modification Proposal was subject to the Refinement Process prior to the Report Phase, include:

(i) the Consultation Summary produced by the Working Group in respect of the Modification Proposal;

(ii) a summary of any views provided by the Technical Architecture and Business Architecture Sub-Committee, the Security Sub-Committee, the SMKI PMA or the Alt HAN Forum in respect of the Modification Proposal pursuant to Section D6.8 (Purpose of the Refinement Process); and

(iii) a summary of any analysis provided by the DCC pursuant to Section D6.9 (Analysis by the DCC).

Consideration of the Modification Report

D7.4 Upon completion of the Modification Report, the Code Administrator will place such report on the agenda for the next meeting of the Panel. Where the Refinement Process was followed, a member of the relevant Working Group shall attend that Panel meeting, and may be invited to present the findings of the Working Group to the

Panel and/or answer the questions of Panel Members in respect of the Modification Report.

D7.5 The Panel shall consider each Modification Report and shall determine whether to:

(a) return the Modification Report back to the Working Group (or, where there was no Refinement Process, the Code Administrator) for further clarification or analysis (in which case, the Panel shall determine the timetable and terms of reference of such further analysis); or

(b) allow the Modification Report to proceed to the Modification Report Consultation.

D7.6 The Panel shall not make any statement regarding whether it believes the Modification Proposal should be successful.

D7.7 Where the Panel determines that a Modification Report is to proceed to the Modification Report Consultation, the Panel shall determine:

(a) the timetable for such Modification Report Consultation, including the period for which the consultation is to remain open (which cannot be more than 15 Working Days); and

(b) the Party Categories that the Panel considers are likely to be affected by the Modification Proposal.

Modification Report Consultation

D7.8 Where the Panel determines that a Modification Report is to proceed to the Modification Report Consultation, the Code Administrator shall arrange for a consultation seeking the views of Parties (other than the DCC) on the Modification Report (the **Modification Report Consultation**). The Code Administrator shall:

(a) invite consultation responses in accordance with the timetable determined by the Panel and in the form referred to in Section D7.9;

(b) collate the responses received during the consultation, and add those responses to the Modification Register; and

(c) place the Modification Report on the agenda for the next meeting of the Change Board following the collation of such consultation responses.

D7.9 Each Modification Report Consultation shall allow for each Party (other than the DCC) that wishes to respond to the consultation to respond by way of a form that provides for a response in one of the following manners (where applicable, in respect of the Modification Proposal and the Alternative Proposal separately):

(a) 'no interest' where the Party considers that it and its Party Category are unlikely to be affected by the Modification Proposal;

(b) 'abstain' where the Party wishes to abstain for reasons other than as described in Section D7.9(a);

(c) 'approve' where the Party considers that making the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected; or

(d) 'reject' where the Party considers that not making the variation would better facilitate the achievement of the SEC Objectives than if the variation was approved,

and which prompts the Party to give a reason for its response by reference to the SEC Objectives.

D7.10 Each Party's response to a Modification Report Consultation will only be validly given if made on the forms provided and received on or before the deadline for responses.

D8 CHANGE BOARD AND CHANGE BOARD DECISION

Establishment of the Change Board

D8.1 The Panel shall establish a Sub-Committee for the purposes of this Section D8, to be known as the **Change Board**. Save as expressly set out in this Section D8, the Change Board shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Function of the Change Board

D8.2 The function of the Change Board shall be to:

(a) facilitate the development, refinement and discussion of potential variations to this Code prior to their formal submission as Modification Proposals;

(b) consider each Modification Report and the responses received in response to the Modification Report Consultation; and

(c) decide whether to approve or reject the Modification Proposal in the form set out in the Modification Report (and, where applicable, whether to approve or reject each Alternative Proposal).

Effect of the Change Board Decision

D8.3 The effect of the Change Board decision shall:

(a) in the case of Path 1 Modifications and Path 2 Modifications, be to recommend to the Authority that the variation be approved or rejected; or

(b) in the case of Path 3 Modifications, be to approve or reject the variation.

Membership of the Change Board

D8.4 The following persons shall serve on the Change Board (each being a **Change Board Member**):

(a) one person nominated jointly by Citizens Advice and Citizens Advice Scotland;

(b) one person appointed by each of the Voting Groups within the Party Category representing the Large Supplier Parties;

(c) three persons appointed by the Party Category representing the Small Supplier Parties;

(d) three persons appointed by the Party Categories representing Electricity Network Parties and the Gas Network Parties collectively; and

(e) three persons appointed by the Party Category representing the Other SEC Parties.

D8.5 Each Voting Group, Party Category or Party Categories (as applicable) referred to in each sub-section of Section D8.4 shall nominate its appointee(s) to serve as Change Board Member(s) to the Secretariat. Each Change Board Member shall serve for a term of one year, and shall be capable of being reappointed at the end of that term. The relevant Voting Group, Party Category or Party Categories may (on notice to the Secretariat) establish a rota whereby more than one person shares the office of Change Board Member.

D8.6 It shall be for the Parties within the relevant Party Category or Party Categories (as applicable) referred to in each sub-section of Section D8.4 to determine how they agree between themselves on the identity of each person to be appointed as a Change Board Member on their behalf. In the event that the Parties within such Party Category or Party Categories cannot so agree, the Secretariat shall seek the preference of the Parties within the relevant Party Category or Party Categories (as applicable) and the person preferred by the majority of those Parties that express a preference (on a one-vote-per-Party basis) shall be appointed as a Change Board Member. In the absence of a majority preference the relevant Change Board Member position shall remain unfilled.

D8.7 The Panel shall only be entitled to remove a Change Board Member from office where such Change Board Member is repeatedly absent from meetings to an extent that frustrates the proceedings of the Change Board. The Voting Group by which a Change Board Member was appointed pursuant to Section D8.4(b) shall be entitled to remove that Change Board Member by notice in writing to the Secretariat. The Party

Category or Party Categories (as applicable) referred to in each other sub-section of Section D8.4 shall be entitled to remove the Change Board Member appointed by them from office by notice in writing to the Secretariat; provided that the majority of the Parties within the relevant Party Category or Party Categories (as applicable) must approve such removal.

Duties of Change Board Members

D8.8 The Consumer Member serving on the Change Board will, when acting as a Change Board Member, act in a manner consistent with the statutory functions of Citizens Advice or Citizens Advice Scotland. Each other Change Board Member will act in the interests of the Voting Group, Party Category or Party Categories (as applicable) by which the Change Board Member was appointed.

D8.9 In giving effect to his or her duties under Section D8.8, each Change Board Member (other than the Consumer Member) shall:

(a) be guided (but not bound) by the responses to the Modification Report Consultation given by Parties within the Voting Group, Party Category, or Party Categories (as applicable) by which such Change Board Member was appointed;

(b) seek to clarify with the relevant Party any responses to the Modification Report Consultation that are not clear to the Change Board Member, or which the Change Board Member considers to be based on a misunderstanding of the facts;

(c) seek to act in the best interests of the majority, whilst representing the minority view (and, where a majority is not significant, the Change Board Member should consider whether abstention from the vote best represents the interests of the Change Board Member's constituents); and

(d) be entitled to vote or abstain without regard to the Panel's indication of which Party Categories the Panel considered to be affected by the Modification Proposal.

D8.10 The confirmation to be given by each Change Board Member to SECCo in accordance with Section C6.9 (Member Confirmation) shall refer to Section D8.8 in place of Section C6.8.

Proceedings of the Change Board

D8.11 The Code Administrator shall chair the Change Board meetings. The chair shall have no vote (casting or otherwise).

D8.12 The quorum for Change Board meetings shall be:

(a) at least three persons appointed by the Large Supplier Parties;

(b) at least one person appointed by the Small Supplier Parties;

(c) at least two persons appointed by the Electricity Network Parties and Gas Network Parties collectively; and

(d) at least one person appointed by the Other SEC Parties,

provided that fewer (or no) appointees from a Party Category shall be required where that Party Category has not appointed that many (or any) Change Board Members; and further provided that no appointees from a Party Category shall be required where the Panel indicated pursuant to Section D7.7(b) that that Party Category was not likely to be affected by the Modification Proposal in question.

D8.13 In addition to those persons referred to in Section C5.13, representatives of the DCC shall be entitled to attend and speak (but not vote) at each meeting of the Change Board.

The Change Board Vote

D8.14 In respect of each Modification Report referred to the Change Board, the Change Board shall vote:

(a) whether to recommend to the Panel that the Panel consider returning the Modification Report to the Working Group (or, where there was no Refinement Process, the Code Administrator) for further clarification or

analysis; and if not

(b) whether to approve the variation set out in the Modification Report or any Alternative Modification (on the basis that the Change Board may only approve one of them).

D8.15 A vote referred to in Section D8.14 shall take the form of a vote by:

(a) the Consumer Member serving on the Change Board;

(b) the Change Board Members appointed by the Voting Groups within the Party Category representing the Large Supplier Parties (whose collective vote shall be determined in accordance Section D8.16);

(c) the Change Board Members appointed by the Party Category representing the Small Supplier Parties (whose collective vote shall be determined in accordance with Section D8.16);

(d) the Change Board Members appointed by the Party Categories representing Electricity Network Parties and the Gas Network Parties (collectively) (whose collective vote shall be determined in accordance with Section D8.16); and

(e) the Change Board Members appointed by the Party Category representing the Other SEC Parties (whose collective vote shall be determined in accordance with Section D8.16),

and a vote pursuant to Section D8.14 shall only be successfully passed if the majority of the votes cast in accordance with this Section D8.15 are cast in favour. For the avoidance of doubt: an abstention shall be treated as if no vote was cast; where there are no Change Board Members present from within the categories referred to in each of Sections D8.15(a) to (e) they shall be deemed to have abstained; and a tie amongst the votes cast shall not be a vote in favour.

D8.16 Each of the collective votes by Change Board Members referred to in Section D8.15(b) to (e) shall be determined by a vote among the relevant Change Board Members, such vote to be undertaken on the basis:

(a) of one vote per Change Board Member; and

(b) that the majority of those Change Board Members that are present must vote in favour in order for the collective vote to be considered a vote in favour (and, for the avoidance of doubt, a tie amongst the votes cast shall not be a vote in favour).

D8.17 In casting his or her vote, each Change Board Member must record the reason for his or her vote, and where voting on whether or not to approve a variation must explain whether the making of the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected.

Communicating the Change Board Vote

D8.18 Following the vote of the Change Board in respect of each Modification Report, the Code Administrator shall update the Modification Register to include the outcome of the vote and the reasons given by the Change Board Members pursuant to Section D8.17.

D8.19 Where the outcome of the Change Board vote is to recommend to the Panel that the Panel consider returning the Modification Report for further clarification or analysis (as referred to in Section D8.14(a)), the Panel may either follow such recommendation or return the Modification Report to the Change Board without any further clarification or analysis. Where the Panel returns the Modification Report to the Change Board without any further clarification or analysis, the Change Board shall not vote again on the matters referred to in Section D8.14(a) and must vote on whether to approve the variation (as referred to in Section D8.14(b)).

D8.20 Where the Change Board votes on whether to approve a variation set out in a Modification Report (as referred to in Section D8.14(b)), the Code Administrator shall communicate the outcome of that vote to the Authority and the Panel, and shall send copies of the following to the Authority:

(a) the Modification Report;

(b) the Modification Report Consultation and the responses received in respect of

the same; and

(c) the outcome of the Change Board vote, including the reasons given by the Change Board Members pursuant to Section D8.17.

D9 MODIFICATION PROPOSAL DECISION

General

D9.1 The final decision as to whether or not to approve a Modification Proposal shall depend upon whether the Modification Proposal is:

(a) a Path 1 Modification or a Path 2 Modification;

(b) a Path 3 Modification; or

(c) a Fast-Track Modification.

Path 1 Modifications and Path 2 Modifications

D9.2 A Path 1 Modification or a Path 2 Modification shall only be approved where the Authority determines that the Modification Proposal shall be approved (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code). In making such determination, the Authority will have regard to:

(a) its objectives and statutory duties under the Electricity Act and the Gas Act;

(b) whether or not the approval of the variation would better facilitate the achievement of the SEC Objectives than if the variation was rejected;

(c) the decision of the Change Board in respect of the Modification Proposal, which shall be considered to constitute a recommendation by the Parties as to whether or not to approve the Modification Proposal; and

(d) such other matters as the Authority considers appropriate.

Send-Back Process

D9.3 Where the Authority considers that it is unable to form an opinion in relation to a Modification Proposal submitted to it, then it may issue a direction to the Panel specifying any additional steps that the Authority requires in order to form such an opinion (including drafting or amending the proposed legal text, revising the proposed implementation timetable, and/or revising or providing additional analysis and/or

information). Where the Authority issues a direction to the Panel pursuant to this Section D9.3:

(a) the decision of the Change Board in respect of the Modification Proposal shall be null and void;

(b) the Panel shall send the Modification Proposal back to the relevant Working Group (or shall establish a Working Group) to consider the matters raised by the Authority, and to prepare a revised Modification Report;

(c) the Panel shall revise the timetable applying to the Modification Proposal; and

(d) the Secretariat shall update the Modification Register to record the status of the Modification Proposal.

Path 3 Modifications

D9.4 A Path 3 Modification shall only be approved where the Change Board votes to approve the Modification Proposal, subject to the following:

(a) any Party that disagrees with the decision of the Change Board, may (within 10 Working Days following the publication of that decision) refer the matter to the Panel, and the Panel shall determine whether it wishes to reverse the decision of the Change Board;

(b) any Party that disagrees with the decision of the Panel pursuant to Section D9.4(a), may (within 10 Working Days following the publication of that decision) refer the matter to the Authority, and the Authority shall determine whether the Modification Proposal should be rejected or approved in accordance with Section D9.2 (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code); and

(c) accordingly, where the consequence of the Panel's or the Authority's determination is that the Modification Proposal is to be rejected (where it has previously been approved) the Modification Proposal shall be cancelled and not implemented (or, if already implemented, shall be reversed).

Fast-Track Modifications

D9.5 In the case of a Fast-Track Modification, any decision of the Panel under Section D3.6 to approve the Modification Proposal shall be final, subject to the following:

(a) where the Panel has raised a Fast-Track Modification, any Party may notify the Panel that the Party believes that the procedure for Fast-Track Modifications is inappropriate given the nature of the variation in question (and the Party should give reasons to substantiate this belief);

(b) when the Panel considers the status of the Fast-Track Modification in accordance with Section D3.6 (Initial Consideration of Modification Proposals), it shall consider any notifications received pursuant to Section D9.5(a);

(c) where the Panel nevertheless determines under Section D3.6 (Initial Consideration of Modification Proposals) that the Modification Proposal should be approved, the Panel shall notify the Party that raised the issue under Section D9.5(a);

(d) such Party may, within 10 Working Days thereafter, refer the matter to the Authority for final determination; and

(e) following a referral to the Authority in accordance with Section D9.5(d), where the Authority determines that the Panel's decision to follow the Fast-Track Procedure was inappropriate given the nature of the variation in question, the Modification Proposal shall be cancelled and not implemented (or, if already implemented, shall be reversed).

D10 IMPLEMENTATION

General

D10.1 Once a Modification Proposal has been approved in accordance with Section D9 (Modification Proposal Decision), the Panel shall ensure that this Code is varied in accordance with that Modification Proposal, as set out in this Section D10.

Implementation

D10.2 The Panel shall, at the next Panel meeting after a Modification Proposal has been approved:

(a) determine what actions are required in order to ensure that the approved variation to this Code is made in accordance with the approved implementation timetable; and

(b) set a timetable for the completion of each of those actions.

D10.3 It shall be the duty of the Panel to ensure that the actions which are required to secure that an approved variation to this Code is made in accordance with the approved implementation timetable are taken.

D10.4 Each Party shall co-operate with the Panel to the extent required to ensure that such variation is made with effect from such date.

Subsequent Amendment to Implementation Timetable

D10.5 Where, having regard to representations received from the Code Administrator or from any Party, the Panel considers that it is not reasonably practicable to make the approved variation to this Code in accordance with the approved implementation timetable:

(a) the Panel may request the Authority to direct that a new implementation timetable be substituted for the first such timetable; and

(b) where the Authority makes such a direction following a request by the Panel, the implementation timetable directed by the Authority shall have effect in

substitution for the first such timetable, and the requirements of this Section D10 shall be defined by relation to that later date.

D10.6 Without prejudice to the generality of Section D10.5, the Panel shall make a request to the Authority under that Section where:

(a) the decision of the Authority to approve the relevant Modification Proposal is subject to an appeal pursuant to section 173 of the Energy Act 2004 or is challenged by judicial review; and

(b) the Panel considers that it is appropriate in the circumstances for the timetable to be delayed given such appeal or challenge.

Release Management

D10.7 To the extent that implementation of an approved Modification Proposal will involve Release Management (or require the DCC or Users to undertake Release Management as a consequence of the Modification Proposal), the Panel shall ensure that such implementation is undertaken in accordance with a policy for Release Management (the "**Panel Release Management Policy**").

D10.8 The Panel shall ensure that the Panel Release Management Policy:

(a) defines the scope of the matters that are to be subject to the policy in a manner consistent with the Service Management Standards;

(b) includes a mechanism for setting priorities for different types of such matters;

(c) defines periods of change-freeze where no such matters may be implemented; and

(d) defines periods of notice to be given to the Users prior to the implementation of such matters.

D10.9 The Panel shall make the Panel Release Management Policy available to the DCC and Users on the SEC Website. The Panel shall consult with the DCC and Users before it first establishes the Panel Release Management Policy, and before it makes any changes to the Panel Release Management Policy.

SECTION E: REGISTRATION DATA

E1 RELIANCE ON REGISTRATION DATA

DCC

E1.1 The DCC shall, from time to time, use and rely upon the Data provided to it pursuant to Section E2 as most recently updated pursuant to Section E2 (the **Registration Data**); provided that the DCC shall be allowed up to three hours from receipt to upload such Data to the DCC Systems.

E1.2 Without prejudice to the generality of Section E1.1, the DCC shall use and rely upon the Registration Data when:

(a) assessing a User's eligibility to receive certain Services (as described in Section H4 (Processing Service Requests); and

(b) calculating the Charges payable by a Party.

E1.3 The DCC shall have no liability to any Party where it provides (or does not provide) a Service in circumstances where it should not (or should) have done so, to the extent that the same arises due to inaccuracies in the Registration Data that are not caused by the DCC.

Panel

E1.4 The Panel shall periodically request from the DCC any Registration Data reasonably required by the Panel in relation to the proper exercise of its duties, powers and functions, including the Registration Data required by the Panel to establish into which Party Category a Party falls. Where aggregated or anonymised data (or similar) is sufficient for the Panel's needs, the Panel shall request, and the DCC shall provide, the data in such format.

E1.5 The DCC shall provide to the Panel any Registration Data requested by the Panel in accordance with Section E1.4.

E1.6 The Panel (and the Secretariat) shall, from time to time, use and rely upon the

Registration Data most recently provided to the Panel pursuant to Section E1.5.

E2 PROVISION OF DATA

Responsibility for Providing Electricity Registration Data

E2.1 The Electricity Network Party in respect of each MPAN relating to its network shall provide (or procure that its Registration Data Provider provides) the following information to the DCC in respect of that MPAN (insofar as such information is recorded in the relevant registration systems). The information in question is the following:

(a) the identity of the Electricity Network Party~~Registration Data Provider~~ for the MPAN;

(b) whether or not the MPAN has a status that indicates that it is 'traded' (as identified in the MRA), and the effective date of that status;

(c) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become Registered in respect of the MPAN, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Registered in respect of the MPAN;

(d) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become the Meter Operator in respect of the MPAN, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Meter Operator in respect of the MPAN;

(e) the address, postcode and UPRN for the Metering Point to which the MPAN relates;

(f) the direction of energy flow to or from the Metering Point to which the MPAN relates (and the date from which that direction of flow has been effective);

(g) the profile class (as defined in the MRA) assigned to the MPAN, and each and every other (if any) profile class assigned to the MPAN at any time within the 24 months preceding the date on which the Registration Data is provided

(including the date from and to which such profile class was effective); and

(h) details of whether an objection has been received regarding a change to the person who is to be Registered in respect of the MPAN, and whether that objection has been removed or upheld, or has resulted in the change to the person who is to be Registered being withdrawn (as at the date on which the Registration Data is provided).

Responsibility for Providing Gas Registration Data

E2.2 The Gas Network Party in respect of each Supply Meter Point on its network shall provide (or procure that its Registration Data Provider provides) the following information to the DCC in respect of that Supply Meter Point (insofar as such information is recorded in the relevant registration systems). The information in question is the following:

(a) the identity of the Registration Data Provider for the Supply Meter Point;

(b) the identity of the Gas Network Party for the network to which the Supply Meter Point relates, and the identity of the Gas Network Party for any network to which the Supply Meter Point related at any time within the 24 months preceding the date on which the Registration Data is provided (and the date from and to which that was the case);

(c) the MPRN for the Supply Meter Point;

(d) whether or not the Supply Meter Point has a status that indicates that gas is offtaken at that point (as identified in the UNC), and, where~~the effective date of~~ that status has changed since the Registration Data was last provided, notification to that effect;

(e) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become Registered in respect of the Supply Meter Point, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Registered in respect of the Supply Meter

Point;

(f) the identity of each person which has been (at any time within the 24 months preceding the date on which the Registration Data is provided), is, or is due to become the Meter Asset Manager in respect of the Supply Meter Point, including (to the extent applicable) the date on which each such person became or ceased to be (or is to become or ceased to be) Meter Asset Manager in respect of the Supply Meter Point;

(g) the address, postcode and UPRN for the Supply Meter Point; and

(h) whether the Supply Meter Point serves a Domestic Premises or Non-Domestic Premises.

Obligation on DCC to Provide Data

E2.3 The DCC shall provide the information set out in Section E2.4 to the Registration Data Provider nominated by each Electricity Network Party and each Gas Network Party (as such information is further described in the Registration Data Interface Documents).

E2.4 The information to be provided by the DCC:

(a) to each Electricity Network Party's Registration Data Provider is:

(i) whether there is (or used to be) an Enrolled Smart Metering System associated with each of the MPANs relating to the Electricity Network Party's network (and the date of its Enrolment or Withdrawal); and

(ii) the identity of the person which the DCC believes to be Registered in respect of each of the MPANs relating to the Electricity Network Party's network; and

(b) to each Gas Network Party's Registration Data Provider is whether there is (or used to be) an Enrolled Smart Metering System associated with each of the Supply Meter Points on the Gas Network Party's network (and the date of its Enrolment or Withdrawal).

Frequency of Data Exchanges

E2.5 A full set of the Data to be exchanged under this Section E2 shall be provided on or before the date on which this Section E2.5 comes into full force and effect. Thereafter, the Data to be exchanged under this Section E2 shall (subject to Section E2.8) be provided by way of incremental updates to Data previously provided (so that only Data that has changed is updated).

E2.6 The incremental updates to Data to be provided in accordance with this Section E2 shall be updated at the frequency and/or time required in accordance with the Registration Data Interface Documents.

E2.7 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider shall:

(a) where a full set of the Registration Data Provider's Registration Data has been requested, take all reasonable steps~~use all reasonable endeavours~~ (including working outside of normal business hours where reasonably necessary) to provide the DCC with such data as soon as reasonably practicable following such request (and in any event within the shorter of three Working Days or four days); or

(b) where a subset of the Registration Data Provider's Registration Data has been requested, provide the DCC with the requested Data in accordance with the Registration Data Interface Documents.

Registration Data Interface

E2.8 The DCC shall maintain the Registration Data Interface in accordance with the Registration Data Interface Specification, and make the interface available to the Registration Data Providers to send and receive Data via the DCC Gateway Connections in accordance with the Registration Data Interface Code of Connection.

E2.9 The DCC shall ensure that the Registration Data Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

E2.10 Each Electricity Network Party and each Gas Network Party shall ensure that its

Registration Data Provider shall (when acting in such capacity) comply with the applicable obligations set out in the Registration Data Interface Documents and the Incident Management Policy.

E2.11 For the avoidance of doubt, the DCC shall comply with the applicable obligations set out in the Registration Data Interface Documents and the Incident Management Policy (as it is obliged to do in respect of all applicable provisions of this Code).

Registration Data Refreshes

E2.12 The Registration Data Interface Documents shall provide for the means, processes and timetables for requesting and providing full and partial refreshes of the Registration Data Provider's Registration Data as required by Section E2.7.

E2.13 Where the DCC identifies any omissions or manifest errors in the Registration Data, the DCC shall seek to resolve any such omissions or manifest errors in accordance with the Incident Management Policy. In such circumstances, the DCC may continue (notwithstanding Section E1.1) to rely upon and use any or all of the Registration Data that existed prior to its receipt of the incremental update that included any such omission or manifest error, unless the Incident Management Policy provides for an alternative course of action.

Security Obligations and RDP IDs

E2.14 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall (when acting in its capacity as the Network Party's Registration Data Provider) comply with the obligations expressed to be placed on Users and identified in Section E2.15 as if, in the case of each such obligation:

(a) references to User were references to such Registration Data Provider; and

(b) references to User Systems were references to the RDP Systems of that Registration Data Provider.

E2.15 The obligations identified in this Section E2.15 are those obligations set out at:

(a) Sections G3.2 to G3.3 (Unauthorised Activities: Duties to Detect and Respond);

(b) Sections G3.8 to G3.9 (Management of Vulnerabilities);

(c) Sections G5.14 to G5.18 (Information Security: Obligations on Users), save that for this purpose the reference:

(i) in Section G5.18(b)(i) to "Sections G3 and G4" shall be read as if it were to "Sections G3.2 to G3.3 and G3.8 to G3.9"; and

(ii) in Section G5.18(b)(iii) to "Sections G5.19 to G5.24" shall be read as if it were to "Section G5.19(d)".

E2.16 Each Electricity Network Party and each Gas Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall (when acting in its capacity as the Network Party's Registration Data Provider):

(a) Digitally Sign any communication containing Registration Data which is sent to the DCC using a Private Key associated with an Organisation Certificate for which that RDP is the Subscriber, in accordance with the requirements of the Registration Data Interface Specification;

(b) for that purpose, propose to the DCC one or more EUI-64 Compliant identification numbers, issued to it by the Panel, to be used by that RDP when acting in its capacity as such (save that it may use the same identification number when acting as an RDP for more than one Network Party).

E2.17 The DCC shall accept each identification number proposed by each Registration Data Provider for the purposes set out in Section E2.16 (and record such numbers as identifying, and use such numbers to identify, such RDP when acting as such); provided that the DCC shall only accept the proposed number if it has been issued by the Panel.

Disputes

E2.18 Any Dispute regarding compliance with this Section E2 may be referred to the Panel for its determination, which shall be final and binding for the purposes of this Code; save that Disputes regarding compliance with Section E2.14 shall be subject to the means of Dispute resolution applying to the provisions of Section G (Security) referred to in Section E2.15 (as set out in Section G).

E3 DCC GATEWAY CONNECTIONS FOR REGISTRATION DATA PROVIDERS

Provision of a DCC Gateway Connection for RDPs

E3.1 Registration Data Providers may request DCC Gateway Connections, and the DCC shall offer to provide such connections, in accordance with Sections H15.4 and H15.6 to H15.12 (as if Registration Data Providers were Parties), save that a Registration Data Provider shall not specify which DCC Gateway Bandwidth Option it requires, and shall instead specify which (if any) other Registration Data Providers it intends to share the connection with pursuant to Section E3.4.

E3.2 The DCC shall provide DCC Gateway Connections to the premises of Registration Data Providers in accordance with Sections H15.13 to H15.15 (as if Registration Data Providers were Parties), save that no Charges shall apply.

E3.3 The DCC shall ensure that the DCC Gateway Connection it provides to the premises of Registration Data Providers pursuant to this Section E3 is of a sufficient bandwidth to meet the purposes for which such connection will be used by the Registration Data Provider, and any other Registration Data Providers notified to the DCC in accordance with Section E3.1 or E3.4 (provided, in the case of those notified in accordance with Section E3.4, that the DCC may object to the transfer or sharing where it reasonably believes that the connection will not be of sufficient bandwidth to meet the needs of all of the Registration Data Providers in question).

E3.4 Each Registration Data Provider may transfer or share its rights in respect of the DCC Gateway Connection provided to its premises pursuant to this Section E3 in accordance with Sections H15.16 and H15.17 (as if Registration Data Providers were Parties), save that such rights may only be transferred to or shared with other Registration Data Providers for the purposes of accessing the Registration Data Interface.

E3.5 Once a DCC Gateway Connection has been established:

(a) the Registration Data Provider that requested it (or to whom it has been transferred in accordance with Section E3.4) and the DCC shall each comply

with the provisions of the DCC Gateway Connection Code of Connection applicable to the DCC Gateway Bandwidth Option utilised at the connection; and

(b) the DCC shall make the connection available to such Registration Data Provider until: (i) the DCC is notified by such Registration Data Provider that it wishes to cancel the connection; or (ii) such Registration Data Provider ceases to be a Registration Data Provider for one or more Network Parties.

DCC Gateway Equipment at RDP Premises

E3.6 The DCC and each Registration Data Provider shall comply with the provisions of Sections H15.20 to H15.28 in respect of the DCC Gateway Equipment installed (or to be installed) at a Registration Data Provider's premises (as if Registration Data Providers were Parties), save that Section H15.28 shall be construed by reference to Section E3.5(b).

Interpretation

E3.7 Given the application of certain provisions of Section H15 to Registration Data Providers in accordance with this Section E3, defined terms used in Section H15 and/or the DCC Gateway Connection Code of Connection shall be construed accordingly (including DCC Gateway Party by reference to the Registration Data Provider which requested the connection, or to whom the right to use the connection has been transferred pursuant to Sections E3.4 and H15.16). Given that Registration Data Providers do not specify the DCC Gateway Bandwidth Option that they require (and that the DCC instead determines the most appropriate bandwidth), references in Section H15 to the bandwidth requested by a Party shall be construed accordingly.

Liability of and to the Network Parties

E3.8 Each Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall comply with the obligations expressed to be placed on Registration Data Providers under or pursuant to this Section E3.

E3.9 Where more than one Network Party nominates the same Registration Data Provider, each of those Network Parties shall be jointly and severally liable for any failure by that Registration Data Provider to comply with the obligations expressed to be placed on Registration Data Providers under or pursuant to this Section E3.

E3.10 The DCC acknowledges that it is foreseeable that Network Parties will have made arrangements with their Registration Data Providers such that breach by the DCC of this Section E3 will cause the Network Parties to suffer loss for which the DCC may be liable (subject to Section M2 (Limitations of Liability)).

Disputes

E3.11 Where a Registration Data Provider wishes to raise a dispute in relation to its request for a DCC Gateway Connection, then the dispute may be referred to the Panel for determination. Where that Registration Data Provider or the DCC disagrees with any such determination, then it may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

SECTION F – SMART METERING SYSTEM REQUIREMENTS

F1 TECHNICAL ARCHITECTURE AND BUSINESS ARCHITECTURE SUB-COMMITTEE

Establishment of the Technical Architecture and Business Architecture Sub-Committee

F1.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section F1, to be known as the "**Technical Architecture and Business Architecture Sub-Committee**".

F1.2 Save as expressly set out in this Section F1, the Technical Architecture and Business Architecture Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

F1.3 Membership of the Technical Architecture and Business Architecture Sub-Committee shall be determined by the Panel:

(a) having regard to the need to provide an appropriate level of technical and business architecture expertise in the matters that are the subject of the Technical Architecture and Business Architecture Sub-Committee's duties; and

(b) otherwise in accordance with Section C6.7 (Membership).

Duties of the Technical Architecture and Business Architecture Sub-Committee

F1.4 The Technical Architecture and Business Architecture Sub-Committee shall undertake the following duties on behalf of the Panel:

(a) to provide the Panel, the Change Board and Working Groups with technical and business architecture support and advice in respect of Modification Proposals that provide for variations to the Technical Code Specifications (or variations to other parts of this Code that affect the End-to-End Technical Architecture and/or the Business Architecture);

(b) to provide the Panel, the Change Board and Working Groups with technical

and business architecture support and advice in respect of Modification Proposals that are identified as likely (if approved) to require changes to the End-to-End Technical Architecture and/or to the Business Architecture;

(c) to provide the Authority (on request) with such information as the Authority may request regarding the technical aspects of any Notification (or potential Notification);

(d) to provide the Panel with technical and business architecture support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Technical Code Specifications (or other parts of this Code that affect the End-to-End Technical Architecture and/or the Business Architecture);

(e) to review (where directed to do so by the Panel) the effectiveness of the End-to-End Technical Architecture (including so as to evaluate whether the Technical Code Specifications continue to meet the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the Technical Architecture and Business Architecture Sub-Committee considers appropriate);

(f) to review (where directed to do so by the Panel) the effectiveness of the Business Architecture (including their assessment against the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the Technical Architecture and Business Architecture Sub-Committee considers appropriate);

(g) to review (where directed to do so by the Panel) the effectiveness of the HAN Requirements (including their assessment against the SEC Objectives), in consultation with Parties and Competent Authorities (but without engaging directly with Energy Consumers), and report to the Authority and the Panel on the outcome of such review;

(h) to support the Panel in the technical and business architecture aspects of the annual report which the Panel is required to prepare and publish under Section C2.3(h) (Panel Duties);

(i) to develop and thereafter maintain the Technical Architecture Document and the Business Architecture Document, and arrange for their publication on the Website;

(j) to provide the Panel with support and advice in respect of any other matter (not expressly referred to in this Section F1.4) which is concerned with the End-to-End Technical Architecture and/or the Business Architecture; and

(k) perform any other duties expressly ascribed to the Technical Architecture and Business Architecture Sub-Committee elsewhere in this Code.

F1.5 The Technical Architecture and Business Architecture Sub-Committee shall establish a process whereby the Code Administrator monitors Modification Proposals with a view to identifying (and bringing to the Technical Architecture and Business Architecture Sub-Committee's attention) those proposals that are likely to affect the End-to-End Technical Architecture and/or the Business Architecture. The Code Administrator shall comply with such process.

F1.6 The Panel shall make each report produced pursuant to Section F1.4 available to the Parties, subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

DCC Obligations

F1.7 The DCC shall provide all reasonable assistance and information to the Technical Architecture and Business Architecture Sub-Committee in relation to the performance of its duties as it may reasonably request, including by providing the Technical Architecture and Business Architecture Sub-Committee with any requested Solution Architecture Information.

Provision of Information in respect of HAN Requirement Reviews

F1.8 Each Party shall provide to the Technical Architecture and Business Architecture Sub-Committee all such information as it may reasonably request in relation to its reviews of the HAN Requirements.

F2 CERTIFIED PRODUCTS LIST

Certified Products List

F2.1 The Panel shall establish and maintain a list of the Device Models for which the Panel has received all the Assurance Certificates required for the Physical Device Type relevant to that Device Model (the "**Certified Products List**").

F2.2 The Panel shall ensure that the Certified Products List identifies the Data required in accordance with the CPL Requirements Document, and that the Certified Products List is updated to add and remove Device Models in accordance with the CPL Requirements Document.

Background to Assurance Certificates

F2.3 The Technical Specification relevant to the Physical Device Type sets out which Physical Device Types require Assurance Certificates from one or more of the following persons (each being an "**Assurance Certification Body**"):

(a) the ZigBee Alliance;

(b) the DLMS User Association; and

(c) CESG.

F2.4 The following Assurance Certification Bodies issue the following certificates in respect of Device Models of the relevant Physical Device Types (each being, as further described in the applicable Technical Specification, an "**Assurance Certificate**"):

(a) the ZigBee Alliance issues certificates which contain the ZigBee certified logo and interoperability icons;

(b) the DLMS User Association issues certificates which include the conformance tested service mark ("**DLMS Certificates**"); and

(c) CESG issues commercial product assurance scheme certificates ("**CPA**

Certificates").

F2.5 An Assurance Certificate will not be valid unless it expressly identifies the Device Model(s) and the relevant Physical Device Type to which it applies. An Assurance Certificate will not be valid if it specifies an expiry date that falls more than 6 years after its issue.

Expiry of CPA Certificates

F2.6 As CPA Certificates will contain an expiry date, the following Parties shall ensure that a replacement CPA Certificate is issued in respect of Device Models for the following Physical Device Types before the expiry of such CPA Certificate (to the extent Device Models of the relevant Physical Device Type require CPA Certificates in accordance with the applicable Technical Specification):

(a) the DCC for Communications Hubs; and

(b) the Import Supplier and/or Gas Supplier (as applicable) for Device Models of all other Physical Device Types.

F2.7 The Panel shall notify the Parties on or around the dates occurring 12 and 6 months prior to the date on which the CPA Certificate for any Device Model is due to expire.

Publication and Use by the DCC

F2.8 Subject to the requirements of the CPL Requirements Document, the Panel shall (within one Working Day after being required to add or remove Device Models to or from the Certified Products List in accordance with the CPL Requirements Document):

(a) provide the updated Certified Products List to the DCC (by way of an extract containing such subset of the information contained within the Certified Products List as the DCC reasonably requires from time to time);

(b) publish a copy of the updated Certified Products List on the Website; and

(c) notify the Parties that the Certified Products List has been updated.

F2.9 Subject to the requirements of the CPL Requirements Document, the DCC shall, from time to time, use and rely upon the Certified Products List most recently received by the DCC from the Panel at that time, provided that the DCC shall be allowed up to 24 hours from receipt to make any modifications to the Smart Metering Inventory that are necessary to reflect the updated Certified Products List. Deployed Products List.

F2.10 The DCC shall create, keep reasonably up-to-date and provide to the Panel (and the Panel shall publish on the Website) a list of all the combinations of different Device Models that comprise a Smart Metering System (together with associated Type 2 Devices) that exist from time to time (to the extent recorded by the Smart Metering Inventory).

Technical Specification Compatibility

F2.11 The Panel shall create, keep reasonably up-to-date and publish on the Website a matrix detailing which versions of each Specification are compatible with which versions of each other Specification (where 'compatible' in this context means, in respect of versions of two or more Specifications, that Devices which comply with one such version are designed to interoperate with other Devices that comply with another such version or versions). The Panel shall, as soon as reasonably practicable after it makes a change to such matrix, notify all the Parties that a change has been made.

F3 PANEL DISPUTE RESOLUTION ROLE

F3.1 Where a Party considers that a device which is required under the Energy Licences to meet the requirements of the Technical Specifications does not meet the applicable requirements of the Technical Specifications, then that Party may refer the matter to the Panel for its determination. For the purposes of this Section F3, the relevant licence requirements are Condition 39 of the Electricity Supply Licences, Condition 33 of the Gas Supply Licences, and Condition 17, Part E of the DCC Licence.

F3.2 The devices to which this Section F3 applies need not form part of Enrolled Smart Metering Systems.

F3.3 The DCC shall retain evidence to demonstrate that the Communications Hubs (as defined in the DCC Licence) meet the DCC's obligations under the DCC Licence to ensure compliance with the CHTS. The DCC shall make that evidence available to the Panel or the Authority on request.

F3.4 Save to the extent the DCC is responsible under Section F3.3, each Supplier Party shall retain evidence to demonstrate that the Devices for which it is responsible under the Energy Licences for ensuring Technical Specification compliance do so comply. Each Supplier Party shall make that evidence available to the Panel or the Authority on request.

F3.5 Where the Panel determines that any device or devices that were intended to meet the requirements of a Technical Specification do not meet the applicable requirements of the Technical Specification, the Panel may (to the extent and at such time as the Panel sees fit, having regard to all the circumstances and any representations made by any Competent Authority or any Party) require the relevant Supplier Party or the DCC (as applicable under Section F3.3 or F3.4) to give effect to a reasonable remedial plan designed to remedy and/or mitigate the effect of such non-compliance within a reasonable timescale.

F3.6 Where a Party disagrees with any decision of the Panel made pursuant to Section F3.5, that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

F3.7 Subject to any determination by the Authority pursuant to Section F3.6, where the Panel requires a Supplier Party to give effect to a remedial plan in accordance with Section F3.5 and where that Supplier Party fails in a material respect to give effect to that remedial plan, then such failure shall constitute an Event of Default for the purposes of Section M8 (Suspension, Expulsion and Withdrawal).

F3.8 For the avoidance of doubt, no decision of the Panel pursuant to this Section F3 is intended to fetter the discretion of the Authority to enforce any breach of any Energy Licence.

F4 OPERATIONAL FUNCTIONALITY, INTEROPERABILITY AND ACCESS FOR THE DCC

Operational Functionality

F4.1 The Import Supplier, Export Supplier and/or Gas Supplier (as applicable) for each Enrolled Smart Metering System shall ensure that the Smart Metering System (excluding the Communications Hub Function) is not configured in a way that restricts the minimum functions that the Smart Metering System is required to be capable of providing in order that the DCC can provide the Services in accordance with this Code.

Interoperability with DCC Systems

F4.2 Pursuant to the DCC Licence, the DCC has certain obligations to ensure that Communications Hubs are interoperable with the DCC Systems.

F4.3 Save to the extent the DCC is responsible as described in Section F4.2, the Responsible Supplier for each Enrolled Smart Metering System shall ensure that all the Devices forming part of that Smart Metering System are interoperable with the DCC Total System to the extent necessary to enable those Devices to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification.

F4.4 The DCC and each Supplier Party shall:

(a) ensure that testing has been undertaken to demonstrate its compliance with the obligations set out in or referred to in Section F4.2 or F4.3 (as applicable); and

(b) retain evidence of such testing, and make such evidence available to the Panel and the Authority on request.

Remote Access by DCC

F4.5 The Responsible Supplier for each Enrolled Smart Metering System shall ensure that the DCC is allowed such remote access to the Smart Metering System as is reasonably necessary to allow the DCC to provide the Services and any other services permitted

by the DCC Licence in respect of that Smart Metering System (including the right to send communications to, to interrogate, and to receive communications and obtain Data from that Smart Metering System).

Physical Access to Devices by Parties

F4.6 Where a Party is expressly required or permitted by this Code to interfere with a Communications Hub, then the DCC hereby consents to the Party interfering with that Communications Hub in that way (and shall ensure that all persons with a legal interest in the Communications Hub have also so consented).

F4.7 Where a User is expressly required by this Code to interfere with a Device forming part of a Smart Metering System (other than the Devices comprising a Communications Hub), then the Party which owns that Device (or has made arrangements with its owner for its provision) hereby consents to the User interfering with that Device in that way (and shall ensure that all persons with a legal interest in that Device have also so consented).

Communications with Communications Hubs by DCC over the SM WAN

F4.8 Except where expressly permitted or obliged by this Code, the DCC shall ensure that the only Devices with which it communicates over the SM WAN are those listed in the Smart Metering Inventory. Where a Communications Hub Function or Gas Proxy Function has an SMI Status of 'suspended', the DCC shall only initiate a communication with that Device (where it is the target device) if following the successful execution of such communication the DCC can reasonably expect that the associated Communication Hub's Device Model will become one that is listed on the Certified Product List.

F4.9 [Not Used]

Communications Hub Procurement

F4.10 The DCC shall publish on the DCC Website the physical dimensions of the Communications Hub Device Models that are made available from time to time pursuant to the Communications Hub Services.

F4.11 Within the relevant period established in accordance with this Section F4.11, the DCC shall consult the other Parties regarding the physical dimensions of the Communications Hub Device Models first made available pursuant to the Communications Hub Services (and shall give due consideration to any consultation responses received when considering the Communications Hubs to be made available in the future). For the purposes of this Section F4.11, the relevant period is the period of 18 months (or such shorter period as the Panel may determine) after the date from which Smart Meters are capable of being Commissioned pursuant to Section H5 (Smart Metering Inventory and Enrolment Services).

F4.12 Prior to committing to the procurement of any Communications Hubs comprising:

(a) HAN Variants and/or WAN Variants that have not previously been made available pursuant to the Communications Hub Services; and/or

(b) Communications Hubs with physical dimensions that differ from the physical dimensions of any Communications Hubs that are (at the time of such proposed procurement) made available pursuant to the Communications Hub Services,

the DCC shall consult the other Parties regarding the physical dimensions of the Communications Hubs to be procured (and shall give due consideration to any consultation responses received).

F4.13 Prior to committing to any arrangements (or any changes to arrangements) for the financing of any Communications Hub procurement, the DCC shall, to the extent such arrangements (or changes) might reasonably be expected to have a material effect on one or more of the other Parties, consult with the other Parties regarding the same. Such consultation shall include the DCC's explanation of how the arrangements (or changes) are consistent with the requirements of the DCC Licence and this Code.

F5 COMMUNICATIONS HUB FORECASTS & ORDERS

Availability of CH Variants

F5.1 The DCC shall ensure that Communications Hub Device Models are made available to be ordered by Parties under this Section F5 such that the Parties can order Communications Hubs that provide for each and every combination of HAN Variant and WAN Variant; save that this Section F5 does not apply to Special Installation Mesh Communications Hubs. All references in this Section F5 to Communications Hubs shall be deemed to exclude Special Installation Mesh Communications Hubs.

Communications Hub Forecasts

F5.2 For the purposes of this Section F5, a "**Communications Hub Forecast**" means an estimate of the future requirements of a Party for the delivery to it of Communications Hubs by the DCC, which:

(a) is submitted by that Party to the DCC;

(b) covers the period identified in Section F5.3; and

(c) complies with the requirements of Section F5.4.

F5.3 Each Communications Hub Forecast shall cover the period of 24 months commencing with the sixth month after the end of the month in which the forecast is submitted to the DCC.

F5.4 Each Communications Hub Forecast shall:

(a) comprise a forecast of the number of Communications Hubs that the Party requires to be delivered to it in each month of the period to which it relates;

(b) set out that forecast for each such month by reference to:

(i) the aggregate number of Communications Hubs to be delivered;

(ii) the number of Communications Hubs to be delivered in respect of each Region; and

(iii) (for the first 10 months of the period to which the forecast relates) the number of Communications Hubs of each HAN Variant to be delivered in respect of each Region; and

(c) include such further information and be provided in such form as may be set out in the CH Handover Support Materials at the time of its submission.

Parties: Duty to Submit Communications Hub Forecasts

F5.5 Each Supplier Party, and each other Party that intends to order Communications Hubs in the future, shall:

(a) submit a Communications Hub Forecast to the DCC by no later than the 5th Working Day prior to the last Working Day of each month;

(b) submit each Communications Hub Forecast via the CH Ordering System;

(c) ~~use its reasonable endeavours~~take reasonable steps to ensure that the information contained in each Communications Hub Forecast is accurate and up to date; and

(d) ensure that it submits a forecast that will enable it to submit a Communications Hub Order that meets the requirements of Section F5.12.

F5.6 A Party that has not submitted a Communications Hub Forecast for a Region during a month in accordance with this Section F5 shall be deemed to have submitted a forecast which specified:

(a) for the first 23 months of the period covered by the forecast, the same number of Communications Hubs as the Party forecast for the corresponding month in its previous forecast;

(b) for the first 9 months of the period covered by the forecast, the same number of each HAN Variant as the Party forecast for the corresponding month in its previous forecast;

(c) for the 10th month of the period covered by the forecast, the number of each HAN Variant that results from applying the same proportions of each HAN

Variant as applies to the 9th month of the period pursuant to paragraph (b) above; and

(d) for the 24th month of the period covered by the forecast, zero Communications Hubs.

Communications Hub Orders

F5.7 For the purposes of this Section F5, a "**Communications Hub Order**" means an order by a Party for the delivery to it of Communications Hubs and/or Communications Hub Auxiliary Equipment by the DCC, which:

(a) is submitted by that Party to the DCC; and

(b) satisfies the requirements of Section F5.8.

F5.8 Each Communications Hub Order shall (subject to any further requirements set out in the CH Handover Support Materials):

(a) relate to a single Region, and identify the Region to which it relates;

(b) relate to the delivery of Communications Hubs and/or Communications Hub Auxiliary Equipment in the 5th month after the end of the month in which that Communications Hub Order is submitted to the DCC (the "**Delivery Month**");

(c) specify the addresses of the location or locations (each a "**Delivery Location**") at which the delivery of the Communications Hubs and/or Communications Hub Auxiliary Equipment is required, each of which locations must be in Great Britain but need not be in the Region to which the relevant Communications Hub Order relates;

(d) specify, in accordance with Section F5.12, the number (if any) of Communications Hubs of each Device Model to be delivered to each Delivery Location (in each case, a "**Delivery Quantity**");

(e) specify the preferred date within the Delivery Month on which the delivery to each Delivery Location is required (provided that the actual delivery date within the Delivery Month for each Delivery Location (in each case, a

"**Delivery Date**") shall be determined in accordance with the CH Handover Support Materials);

(f) specify the number and type of the Communications Hub Auxiliary Equipment (if any) to be delivered to each Delivery Location; and

(g) include such further information and be provided in such form as may be set out in the CH Handover Support Materials at the time of its submission.

F5.9 In respect of each Communications Hub Order submitted in respect of a Region, the Communications Hubs and/or Communications Hub Auxiliary Equipment to be delivered to each Delivery Location on each Delivery Date shall be a "**Consignment**".

F5.10 In order for a Communications Hub Order to be a compliant order, the order must comply with the requirements of this Section F5.10. A Party is not obliged to submit a compliant order, but a non-compliant order may be amended by the DCC in accordance with Section F5.17. The requirements of this Section F5.10 are, for each Communications Hub Order submitted by a Party in respect of a Region, that the aggregate (for all Consignments) of the Delivery Quantities of each HAN Variant for the Delivery Month must be:

(a) greater than or equal to the higher of:

(i) 50% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 10th month prior to the start of the Delivery Month; and

(ii) 80% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by the Party in the 7th month prior to the start of the Delivery Month; and

(b) less than or equal to the lower of:

(i) 120% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications

Hub Forecast submitted by that Party in the 7th month prior to the start of the Delivery Month; and

(ii) 150% of the number of Communications Hubs of that HAN Variant forecast for that Delivery Month and Region in the Communications Hub Forecast submitted by that Party in the 10th month prior to the start of the Delivery Month.

F5.11 For the purposes of Section F5.10, in calculating, by reference to earlier forecast numbers:

(a) the minimum aggregate of the Delivery Quantities, any fractions of a number shall be rounded down; and

(b) the maximum aggregate of the Delivery Quantities, any fractions of a number shall be rounded up.

F5.12 For each Party's Communications Hub Order relating to a Region, the aggregate of the Delivery Quantities (for all Device Models taken together) that may be specified for each Consignment may not (unless such number is zero) be less than the minimum delivery quantity set out in the CH Handover Support Materials at the time at which the relevant Communications Hub Order is submitted.

Parties: Rights and Duties in relation to Communications Hub Orders

F5.13 Each Party other than the DCC:

(a) may submit one Communications Hub Order in relation to each Region in any month;

(b) shall submit a Communications Hub Order in relation to a Region in a month if the aggregate of the Delivery Quantities for one or more Device Models required for a compliant order in accordance with Section F5.10 is greater than zero; and

(c) where it fails to submit an order where it is required to do so in accordance with Section F5.13(b), shall be deemed to have submitted a Communications

Hub Order for a Delivery Quantity of Communications Hubs of each Device Model equal to the minimum aggregate Delivery Quantity required in respect of that Device Model for a compliant order in accordance with Section F5.10 (and the remaining details of such deemed order shall be determined by the DCC in accordance with the CH Handover Support Materials).

F5.14 Each Party shall ensure that any Communications Hub Order which it elects or is required to submit in any month is submitted by no later than the 5th Working Day prior to the last Working Day of that month.

F5.15 Each Party shall submit its Communications Hub Orders via the CH Ordering System.

DCC: Duties in relation to Communications Hub Orders

F5.16 Where the DCC receives a Communications Hub Order from a Party via the CH Ordering System, the DCC shall:

(a) promptly acknowledge receipt of that order; and

(b) within five Working Days of its receipt of the order, notify the Party either that:

(i) the order satisfies the requirements of Section F5.8, is a compliant order in accordance with Section F5.10 and was submitted in accordance with Section F5.14 (and is therefore accepted); or

(ii) the order does not satisfy some or all of the conditions in (i) above (and is therefore subject to Section F5.17).

F5.17 Where this Section F5.17 applies in respect of a Party's Communications Hub Order, the DCC shall (having regard to the nature, extent and effect of the Party's breach of this Section F5 and/or of the order's non-compliance under Section F5.10, and having regard to the requirements of the DCC Licence) take all reasonable steps to accommodate the order (in whole or part, or subject to amendments). The DCC shall, by the end of the month in which such order is received by the DCC, notify the Party (in each case giving reasons for its decision) that:

(a) the order is accepted in its entirety;

(b) the order is accepted in part or subject to amendment; or

(c) the order is rejected.

DCC Policy

F5.18 The DCC shall develop and make available via the DCC Website a policy describing the circumstances in which it will accept (in whole or part, or subject to amendments) or reject Communications Hub Orders as described in Section F5.17.

Non-Standard Cancellation of Consignments

F5.19 Each Party that has had a Communications Hub Order accepted by the DCC may cancel one or more of the Consignments arising from that Communications Hub Order; provided that the Party must notify the DCC of such cancellation at least 48 hours in advance of the Delivery Date for the Consignment. A Party which cancels one or more Consignments in accordance with this Section F5.19 shall be liable to reimburse the DCC for all reasonable costs and expenses incurred by the DCC as a result of such cancellation. The DCC shall notify the Party of such costs and expenses as soon as reasonably practicable after notice of the cancellation is given. Such compensation shall be included in the next Invoice to be produced by the DCC following its calculation. The DCC shall, where requested not less than 10 Working Days in advance of the Delivery Date, provide a non-binding estimate of the costs and expenses it is likely to incur in the event that a Party opts to cancel a Consignment (such estimate to be provided not less than 5 Working Days in advance of the Delivery Date). The DCC shall take all reasonable steps to ensure the estimate is accurate.

CH Ordering System

F5.20 Subject to Section F5.23, the DCC shall make one or more systems (the **CH Ordering System**) available to other Parties, which Parties can access remotely (via such means, and subject to any security requirements, as are set out in the CH Support Materials).

F5.21 The DCC shall ensure that the CH Ordering System is available in advance of the time from which other Parties are obliged to submit Data via the CH Ordering System, and at all times thereafter (subject to Planned Maintenance undertaken in accordance with Section H8.3).

F5.22 The DCC shall ensure that the CH Ordering System allows each Party to:

(a) submit details of its forecasts, orders and returns of Communications Hubs and/or Communications Hub Auxiliary Equipment, as required in accordance with this Section F5, Sections F6 (Delivery and Acceptance of Communications Hubs) and F8 (Removal and Return of Communications Hub), and the CH Support Materials;

(b) view Data regarding the status of such submissions (but only its own submissions), and (where relevant) receive responses from the DCC regarding such submissions; and

(c) view the SM WAN Coverage Database.

CH Order Management System Accounts

F5.23 The DCC may, as further described in the CH Support Materials:

(a) limit the number of accounts via which each Party is able to access the CH Order Management System without paying any additional Charges; and

(b) allow each Party additional accounts via which it is able to access the CH Order Management System, subject to such Party agreeing to pay the applicable Charges.

F6 DELIVERY AND ACCEPTANCE OF COMMUNICATIONS HUBS

Delivery

F6.1 The DCC shall ensure that the applicable numbers of Communications Hub Products are delivered in accordance with Valid Communications Hubs Orders to the relevant Delivery Location on the relevant Delivery Date during the relevant Delivery Window.

F6.2 The DCC shall ensure that the Communications Hub Products are delivered in accordance with the delivery requirements set out in the CH Handover Support Materials.

F6.3 The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the Communications Hub Products are unloaded from the delivery vehicle at the Delivery Location in accordance with Good Industry Practice and the CH Handover Support Materials.

F6.4 Delivery of Communications Hub Products pursuant to this Code shall occur on removal of the Communications Hub Products from the delivery vehicle at the Delivery Location (subject to any additional requirements in the CH Handover Support Materials).

F6.5 Risk of loss or destruction of or damage to the Communications Hub Products shall transfer to the Party which submitted the Communications Hub Order on commencement of their unloading at the Delivery Location (where not unloaded by the DCC) or on completion of their unloading at the Delivery Location (where unloaded by the DCC).

F6.6 Notwithstanding delivery, legal and beneficial ownership of the Communications Hub Products shall at all times (for the purposes of this Code) remain vested in the DCC, subject only to Section F7.10 (Ownership of and Responsibility for Communications Hub Auxiliary Equipment).

Confirmation of Delivery

F6.7 The Party which submitted the Valid Communications Hub Order shall confirm

whether or not a delivery of Communications Hub Products has been made in compliance with the order within five days after the applicable Delivery Date (such confirmation to be submitted in accordance with and contain the information specified in the CH Handover Support Materials and via the CH Ordering System).

F6.8 Where a Party fails to submit a confirmation in accordance with Section F6.7, the Party shall be deemed to have confirmed that a delivery of Communications Hub Products has been made in compliance with the relevant order.

F6.9 The only grounds for non-compliance under Section F6.7 are that:

(a) no delivery was made to the relevant Delivery Location on the relevant Delivery Date, or the delivery was made but contained fewer Communications Hub Products of the applicable Device Model or type than the DCC was obliged to deliver;

(b) the delivery contained more Communications Hub Products of the applicable Device Model or type than the DCC was obliged to deliver to the relevant Delivery Location on the relevant Delivery Date;

(c) the delivered Communications Hub Products are (or reasonably appear on a visual inspection to be) damaged or have been (or reasonably appear on a visual inspection to have been) tampered with (and such damage or tampering occurred prior to their delivery to the Party as described in Section F6.4); and/or

(d) the Party is otherwise entitled to reject the Communications Hub Products in accordance with the CH Handover Support Materials.

Rejected Communications Hub Products

F6.10 Where a Party notifies the DCC under Section F6.7 that a delivery is non-compliant in accordance with Sections F6.9(b), (c) and/or (d), the Party thereby rejects the Communications Hub Products in question.

F6.11 Where Section F6.10 applies, the Party to which the rejected Communications Hub Products were delivered shall make those Communications Hub Products available

for collection by the DCC in accordance with the CH Handover Support Materials.

F6.12 The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the rejected Communications Hub Products are loaded on to the DCC's vehicle in accordance with Good Industry Practice and the CH Handover Support Materials. Risk of loss or destruction of or damage to such Communications Hub Products shall transfer to the DCC on commencement of such loading (where loaded by the DCC) or on completion of such loading (where not loaded by the DCC).

Replacement Communications Hub Products

F6.13 Where a Party notifies the DCC under Section F6.7 that a delivery is non-compliant in accordance with Sections F6.9(a), (c) and/or (d), the DCC shall ensure that replacement Communications Hub Products of the applicable Device Model or type and in the number necessary to make up the shortfall are delivered to the relevant Delivery Location as soon as reasonably practicable thereafter.

F6.14 Where Section F6.13 applies, the DCC shall (via the CH Ordering System) notify the Party of the dates on which the DCC is able to deliver such replacement Communications Hub Products, and this Section F6 shall apply as if:

(a) the replacement Communications Hub Products to be delivered pursuant to this Section F6.14 were the subject of a Valid Communications Hub Order; and

(b) the date selected by the Party, out of the dates so notified by the DCC, was the Delivery Date for that order.

Access to Delivery Location

F6.15 The Party which submitted the Communications Hub Order shall ensure that each of the DCC and its sub-contractors and its and their agents is allowed access to the Delivery Location for the purposes of exercising the DCC's rights and performing the DCC's obligations under this Section F6.

F6.16 The DCC shall ensure that each person that accesses a Delivery Location pursuant to Section F6.15 shall do so in compliance with Good Industry Practice and the site rules

and reasonable instructions of the relevant Party (or its representatives).

Non-Standard Delivery Options

F6.17 Each Party which submits a Communications Hub Order may specify non-standard delivery instructions where and to the extent provided for in the CH Handover Support Materials. Subject to such Party agreeing to pay any applicable Charges, the DCC shall comply with such delivery instructions.

Failure to Accept Delivery

F6.18 Where the Party which submitted a Valid Communications Hub Order breaches its obligations under this Section F6 and/or the CH Handover Support Materials and as a result the DCC is not able to deliver the Communications Hub Products in accordance with this Code, that Party shall be liable to reimburse the DCC for all reasonable costs and expenses incurred by the DCC as a result. The DCC shall notify the Party of such costs and expenses as soon as reasonably practicable after the event. Such compensation shall be included in the next Invoice to be produced by the DCC following its calculation.

Special Installation Mesh Communications Hubs

F6.19 Special Installation Mesh Communications Hubs are not ordered under Section F5 (Communications Hub Forecasts & Orders). Consequently, Special Installation Mesh Communications Hubs are not delivered under this Section F6. All references in this Section F6 to Communications Hubs shall be deemed to exclude Special Installation Mesh Communications Hubs.

F7 INSTALLATION AND MAINTENANCE OF COMMUNICATIONS HUBS

Installation

F7.1 Each Supplier Party that installs a Communications Hub shall ensure that such Communications Hub is installed in accordance with the CH Installation and Maintenance Support Materials.

F7.2 Where:

(a) a Supplier Party is installing a Communications Hub for a premises; and

(b) the Supplier Party knows (or should reasonably know) that the premises will also require a Communications Hub Function to form part of a Smart Metering System with a Smart Meter for which the Supplier Party is not a Responsible Supplier,

then that Supplier Party shall, to the extent that it is reasonably able to do so, install a Communications Hub such that the Communications Hub Function will be capable of forming part of a Smart Metering System with both the Smart Meter for which it is a Responsible Supplier and the Smart Meter for which it is not a Responsible Supplier.

F7.3 On completion of the installation of a Communications Hub in accordance with Section F7.1, risk of loss or destruction of or damage to the Communications Hub shall cease to vest in the Party which ordered the Communications Hub (or, in the case of Special Installation Mesh Communications Hubs, shall cease to vest in the Supplier Party which took delivery of the Communications Hub).

Risk in the Communications Hubs following Installation

F7.4 Following completion of installation of a Communications Hub, risk of loss or destruction of or damage to the Communications Hub shall vest in the same or a different Party as follows:

(a) where the Communications Hub is removed from a premises by a Supplier Party, then the risk of loss or destruction of or damage to that Communications Hub shall vest in that Supplier Party such that that Supplier Party is

responsible for all such risk since installation of the Communication Hub until such risk transfers to the DCC under Section F8.11 (Acceptance of a Returned Communications Hub); or

(b) where a Communications Hub is lost or destroyed following completion of its installation at a premises and before commencement of its removal from a premises by a Supplier Party, then the Supplier Party that is obliged to notify the DCC of a Communications Hub's loss or destruction under Section F8.17(b) (Loss or Destruction of Communications Hubs) shall be deemed to bear the risk of such loss or destruction.

Special Installation Mesh Communications Hubs

F7.4A Where it is determined in accordance with the CH Installation and Maintenance Support Materials that a Supplier Party is required to install a Special Installation Mesh Communications Hub in respect of a premises, then the following provisions shall apply:

(a) the DCC shall (subject to Section F7.5) deliver a Special Installation Mesh Communications Hub to the Supplier Party at the premises;

(b) the DCC shall ensure that the Special Installation Mesh Communications Hub that is delivered is of the HAN Variant that the Supplier Party requests;

(c) delivery, risk and ownership of the Special Installation Mesh Communications Hub shall be subject to Sections F6.5 and F6.6 (Delivery) by reference to the Supplier Party to which the Communications Hub is handed by the DCC and completion of such hand over;

(d) following delivery of a Special Installation Mesh Communications Hub as referred to in this Section F7.4A, the Special Installation Mesh Communications Hub shall be subject to the provisions of this Section F7 and of Sections F8 (Removal and Return of Communications Hubs) and F9 (Categories of Communications Hub Responsibility), save as otherwise expressly provided;

(e) in addition to the application of Section F8 (Removal and Return of Communications Hubs), a Supplier Party may return a Special Installation Mesh Communications Hub to the DCC while the Supplier Party and the DCC are still at the premises to which the Communications Hub was delivered, by handing the Communications Hub to the DCC (and the DCC shall accept handover of the Communications Hub, at which point risk of loss or destruction of or damage to the Communications Hub shall transfer to the DCC);

(f) without prejudice to the other obligations of the DCC and the Responsible Suppliers under this Code in respect of Communications Hubs installed at premises, where a Responsible Supplier reasonably determines that an Incident is likely to require replacement or repair of the Communications Hub Auxiliary Equipment installed by the DCC in respect of a Special Installation Mesh Communications Hub, then the DCC shall (subject to Section F7.5) attend the premises and (where necessary) undertake such replacement or repair; and

(g) notwithstanding Section F7.9, no Party other than the DCC may replace or repair the Communications Hub Auxiliary Equipment installed by the DCC in respect of a Special Installation Mesh Communications Hub.

Special Installations & Modifications

F7.5 Where the CH Installation and Maintenance Support Materials requires the DCC to undertake works on behalf of a Supplier Party, and where such works require the consent or agreement of any person other than the Supplier Party or the DCC (including where the consent or agreement of the Energy Consumer and/or any landlord or other owner of premises is required), then that Supplier Party shall ensure that such consent or agreement is obtained in advance.

F7.6 A Supplier Party responsible under Section F7.5 for obtaining a consent or agreement in relation to works shall ~~use its reasonable endeavours~~take reasonable steps to obtain such consent or agreement in a form that permits the installation, operation, repair, modification, replacement and removal of the equipment.

F7.7 Where the DCC attends any premises and/or undertakes any works in reliance on a consent or agreement obtained (or required to be obtained) by a Supplier Party under Section F7.5, the DCC shall do so:

(a) as the contractor of that Supplier Party;

(b) in accordance with Good Industry Practice, the applicable consent or agreement obtained pursuant to Section F7.5 (and notified to the DCC), and the site rules and reasonable instructions of the owner and/or occupier of the relevant premises;

(c) in compliance with all Laws and/or Directives applicable to the Supplier Party or its representatives (and notified to the DCC), including the requirements of the Supplier Party's Energy Licence concerning Supplier Party representatives who attend premises; and

(d) in compliance with all reasonable requests of the Supplier Party.

Preventing Unauthorised Access to Data

F7.8 The DCC and each other Party that is responsible from time to time for the risk of loss or destruction of or damage to a Communications Hub shall ~~use reasonable endeavours~~ take reasonable steps to ensure that Personal Data held on that Communications Hub is protected from unauthorised access during such period of responsibility.

Ownership of and Responsibility for Communications Hub Auxiliary Equipment

F7.9 In respect of those types of Communications Hub Auxiliary Equipment that are designed to be installed at premises, such Communications Hub Auxiliary Equipment shall be deemed to form part of the Communications Hub, and the provisions of this Section F7 and of Sections F8 (Removal and Return of Communications Hubs) and F9 (Categories of Communications Hub Responsibility) shall be construed accordingly.

F7.10 In respect of those types of Communications Hub Auxiliary Equipment to which Section F7.9 does not apply:

(a) legal and beneficial ownership of such Communications Hub Auxiliary Equipment shall vest in the Party that ordered it on risk in such equipment transferring to that Party under Section F6.5 (Delivery); and

(b) legal and beneficial ownership of such Communications Hub Auxiliary Equipment shall (where applicable) revert to the DCC on risk in such equipment transferring to the DCC under Section F6.12 (Rejected Communications Hub Products).

CH Support Materials Compliance and Access to Premises

F7.11 The DCC shall reply to any reasonable request from a Party for information pertaining to compliance by the DCC with the CH Support Materials.

F7.12 Each Party shall reply to any reasonable request from the DCC for information pertaining to compliance by that Party with the CH Support Materials.

F7.13 Where the DCC wishes to attend a premises at which a Communications Hub is installed in order to assess a Party's compliance with the CH Support Materials in respect of that Communications Hub, the DCC may request access from the Responsible Supplier for the Smart Metering System(s) of which the Communications Hub forms part (or, where there is more than one such Responsible Supplier, from either or both of them as further described in the CH Support Materials).

F7.14 Where a Responsible Supplier consents to a request under Section F7.13, the Responsible Supplier shall take all reasonable steps to obtain the consent of the Energy Consumer to the DCC attending the premises.

F7.15 Where a Responsible Supplier does not consent to a request under Section F7.13, the DCC may refer the matter to the Panel. The Panel shall determine whether it is reasonably necessary for the DCC to attend the premises in order to assess (in general) a Party's compliance with the CH Support Materials. Where the Panel determines that it is, the Responsible Supplier shall take all reasonable steps to obtain the consent of the Energy Consumer to the DCC attending the premises.

F7.16 Where the Energy Consumer's consent is obtained pursuant to Section F7.14 or F7.15,

the Responsible Supplier and the DCC shall follow the relevant procedure for attending the premises set out in the CH Support Materials.

F7.17 Where the DCC attends any premises in reliance on a consent obtained by a Supplier Party pursuant to Section F7.14 or F7.15, the DCC shall do so:

(a) as the contractor of that Supplier Party;

(b) in accordance with Good Industry Practice, the applicable consent (as notified to the DCC), and the site rules and reasonable instructions of the owner and/or occupier of the relevant premises;

(c) in compliance with all Laws and/or Directives applicable to the Supplier Party or its representatives (and notified to the DCC), including the requirements of the Supplier Party's Energy Licence concerning Supplier Party representatives who attend premises; and

(d) in compliance with all reasonable requests of the Supplier Party.

Resolution of SM WAN Coverage Incidents

F7.18 Where a Communications Hub is installed at a premises in accordance with this Code but does not connect to the SM WAN, and the SM WAN Coverage Database indicated (at any time during the 30 days prior to the date of installation) that the SM WAN is (or would be) available in the area in which the premises is located on the installation date, then the DCC shall (within 90 days after having been notified in accordance with the CH Installation and Maintenance Support Materials):

(a) provide a response to the installing Supplier Party that either (i) confirms that the SM WAN is now available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN; or (ii) provides reasons why the SM WAN is not so available; and

(b) (subject to Section F7.20) ensure that, in the case of at least 99% of all Communications Hubs for which the DCC is required to give such a response in each calendar quarter, the SM WAN is made available in the relevant area

such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN (but excluding for this purpose those locations where SM WAN connectivity is affected by problems with access pursuant to Section F7.5 which arise otherwise than as a result of the DCC's breach of this Code).

F7.19 Where a Communications Hub is installed at a premises in accordance with this Code but does not connect to the SM WAN (in circumstances where Section F7.18 does not apply), and the SM WAN Coverage Database is updated after installation to indicate that the premises is within an area in which the SM WAN is available, then (provided the DCC has been notified of the installation in accordance with the CH Installation and Maintenance Support Materials) the DCC shall (within 90 days after such update occurs):

(a) provide a response to the Supplier Party which installed the Communications Hub that either (i) confirms that the SM WAN is now available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN; or (ii) provides reasons why the SM WAN is not so available; and

(b) (subject to Section F7.20) ensure that, in the case of at least 99% of all Communications Hubs for which the DCC is required to give such a response in each calendar quarter, the SM WAN is available in the relevant area such that Communications Hubs installed at premises in that area can be expected to be able to connect to the SM WAN (but excluding for this purpose those locations where SM WAN connectivity is affected by problems with access pursuant to Section F7.5 which arise otherwise than as a result of the DCC's breach of this Code).

F7.20 Until 1 January 2021, Sections F7.18(b) and F7.19(b) do not apply to Communications Hubs installed at premises within a geographic area that is subject to a Network Enhancement Plan. Such Communications Hubs shall, until 1 January 2021, be excluded from the calculations under Sections F7.18(b) and F7.19(b).

F7.21 Within a reasonable period of time following each calendar quarter that ends prior to 1

January 2021, the DCC shall produce a report which identifies:

(a) any new Network Enhancement Plans that have been created during that quarter, any Network Enhancement Plans that were completed during that quarter, and any ongoing Network Enhancement Plans; and

(b) for each such Network Enhancement Plan:

(i) an overview of the geographic area that is subject to the plan;

(ii) the premises (by postcode) that fall within that area; and

(iii) the scheduled date for completion of the planned works (or, where applicable, the actual date of completion).

F7.22 A copy of the report produced under Section H7.21 shall be provided by the DCC to the Parties, the Panel, the Authority and (on request) the Secretary of State.

F8 REMOVAL AND RETURN OF COMMUNICATIONS HUBS

Product Recall / Technology Refresh

F8.1 The DCC's rights under this Section F8.1 are in addition to (and separate from) the rights of the DCC (and the obligations of the other Parties) to remove and/or return Communications Hubs under other provisions of this Code (including pursuant to the Incident Management Policy and the CH Support Materials). The DCC has the right to request (in reliance on this Section F8.1) that Parties return to the DCC one or more Communications Hubs. Following receipt of such a request:

(a) in respect of Communications Hubs that have been delivered but have not yet been installed at premises, the Party which ordered those Communications Hubs shall return them to the DCC;

(b) in respect of Communications Hubs that have been installed at premises and not yet removed from that premises, the Lead Supplier for those Communications Hubs shall remove them from the premises and return them to the DCC (and this obligation shall apply whether or not such Lead Supplier is a User); and

(c) in respect of Communications Hubs that have been removed from a premises and not yet returned to the DCC, the Supplier Party that removed the Communications Hub from the premises shall return them to the DCC.

F8.2 Where Section F8.1 applies, the DCC shall provide to Supplier Parties all such information as they or their Energy Consumers reasonably require in respect of the situation. Those Supplier Parties to whom Section F8.1(b) applies shall issue to affected Energy Consumers such information as is provided by the DCC concerning the situation.

Removal of Communications Hubs

F8.3 Each Supplier Party that:

(a) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, is entitled to remove that Communications Hub

from the premises at which it is installed (but must install a replacement Communications Hub unless the Communications Hub Function is Withdrawn);

(b) Decommissions a Communications Hub Function, shall remove the Communications Hub of which the Communications Hub Function forms part from the premises at which it is installed; and

(c) is a Responsible Supplier for the Communications Hub Function forming part of a Communications Hub, may also be obliged under another provision of this Code to remove a Communications Hub, including where it is obliged to do so in accordance with the Incident Management Policy or the CH Support Materials.

F8.4 Where a Supplier Party removes a Communications Hub from a premises, it shall do so in accordance with the CH Installation and Maintenance Support Materials.

F8.5 Where a Communications Hub is removed by a Supplier Party from a premises at which it was previously installed, then the risk of loss or destruction of or damage to that Communications Hub shall vest in that Supplier Party as set out in Section F7.4(a) (Risk in the Communications Hubs following Installation).

Return of Communications Hubs

F8.6 Where a Communications Hub is removed by a Supplier Party from a premises at which it was previously installed, the Supplier Party shall return the Communications Hub to the DCC within 90 days after the date of its removal. This obligation to return a Communications Hub only applies where the Communications Hub Function which forms part of that Communications Hub has at any time had an SMI Status of 'installed not commissioned' or 'commissioned'.

F8.7 A Party that wishes to return a Communications Hub to the DCC shall be entitled to do so at any time. A Party that ceases to be a Party shall return to the DCC all the Communications Hubs that have been delivered to that Party and not yet installed at premises or reported as lost or destroyed.

F8.8 The DCC shall publish on the CH Ordering System the following information:

(a) the addresses of no more than two locations in respect of each Region to which Communications Hubs can be returned (which locations must be in Great Britain), making clear which Device Models may be returned to which locations;

(b) the operating hours of each such location during which returns can be made (which operating hours must be reasonable); and

(c) any changes to the information required to be published under (a) and (b) above, for which at least four months' advance notice must be given (unless the Panel approves a shorter period).

F8.9 A Party required or opting to return one or more Communications Hubs to the DCC shall:

(a) notify the DCC of the number of Communications Hubs to be returned, of the location to which they are to be returned (being one of the locations published for the relevant Region in accordance with Section F8.8), of the date on which they are to be returned, and of any further information required in accordance with the CH Installation and Maintenance Support Materials;

(b) return those Communications Hubs to the location and on the date notified in accordance with (a) above during the applicable operating hours for that location published in accordance with Section F8.8;

(c) otherwise comply with the return requirements set out in the CH Installation and Maintenance Support Materials; and

(d) be liable to pay the applicable Charges in the event that it returns one or more Communications Hubs to the wrong returns location.

Acceptance of Returned Communications Hubs

F8.10 The Party assigned responsibility for doing so under the CH Handover Support Materials shall ensure that the returned Communications Hubs are unloaded from the

vehicle in which they have been returned, and that they are unloaded in accordance with Good Industry Practice and the CH Installation and Maintenance Support Materials.

F8.11 Risk of loss or destruction of or damage to returned Communications Hubs shall transfer to the DCC on commencement of such unloading (where unloaded by the DCC) or on completion of such unloading (where not unloaded by the DCC).

Access to Returns Locations

F8.12 The DCC shall ensure that each Party (and its sub-contractors and its and their agents) is allowed access to the locations published pursuant to Section F8.8 for the purposes of exercising the Party's rights and performing the Party's obligations under this Section F8.

F8.13 The relevant Party shall ensure that any person that accesses a location pursuant to Section F8.14 shall do so in compliance with Good Industry Practice and the site rules and reasonable instructions of the DCC (or its representatives).

Reconditioning or Disposal of Communications Hubs by the DCC

F8.14 The DCC shall take all reasonable steps to recondition and redeploy each Communications Hub that is returned to the DCC (having regard to the requirements of the DCC Licence).

F8.15 Before a Communications Hub that has been returned to the DCC is delivered to a Party pursuant to Section F6 (Delivery and Acceptance of Communications Hubs), the DCC shall ensure that all Data relating to one or more Energy Consumers is permanently erased from that Communications Hub in accordance with the standard referred to in Section G2.18 (Management of Data).

F8.16 Unless the Communications Hub is reconditioned and redeployed in accordance with Sections F8.14 and F8.15, the DCC shall ensure that each Communications Hubs that has been returned to the DCC is disposed of in accordance with Good Industry Practice and the standard referred to in Section G2.18 (Management of Data).

Loss or Destruction of Communications Hubs

F8.17 Where a Communications Hub has been lost or destroyed (save where such loss or destruction occurs while the risk of loss or destruction was the responsibility of the DCC), the following Party shall notify the DCC of such loss or destruction (via the CH Ordering System):

(a) where such loss or destruction occurs prior to completion of the Communications Hub's installation at a premises by a Supplier Party, the Party that ordered that Communications Hub (or, in the case of Special Installation Mesh Communications Hubs, the Supplier Party which took delivery of the Communications Hub);

(b) where such loss or destruction occurs after completion of such installation and before commencement of the Communications Hub's removal from a premises by a Supplier Party, the Supplier Party responsible under the Incident Management Policy for resolving the relevant Incident; or

(c) where such loss or destruction occurs after commencement of the Communications Hub's removal from a premises by a Supplier Party, the Supplier Party which undertook such removal.

F8.18 Where a Communications Hub is lost or destroyed following completion of its installation at a premises by a Supplier Party and before commencement of its removal from a premises by a Supplier Party, then the Supplier Party that is obliged to notify the DCC of such loss or destruction under Section F8.17(b) shall be deemed to bear the risk of such loss or destruction as described in Section F7.4(b) (Risk in the Communications Hubs following Installation Installation).

F9 CATEGORIES OF COMMUNICATIONS HUB RESPONSIBILITY

Overview

F9.1 The reason for the return of each returned Communications Hub, or for its loss or destruction, shall be determined in accordance with this Section F9.

F9.2 The Party which returns a Communications Hub to the DCC shall specify the reason for the Communications Hub's return. The Party which notifies the DCC of a Communications Hub's loss or destruction shall specify the reason it was lost or destroyed. In any such case, such Party shall specify the reason in accordance with the CH Support Materials.

F9.3 The reason specified by the relevant Party pursuant to Section F9.2 shall be subject to any contrary determination in accordance with this Section F9.

F9.4 The reason for the return of a Communications Hub, as finally determined in accordance with this Section F9, shall be used to determine the applicable category of responsibility (as described in Section F9.4), which is then used for the purposes of calculating the Charges (or adjustments to the Charges in accordance with this Section F9).

Reasons

F9.5 The reasons that apply for the purposes of this Section F9 are as follows:

(a) that the Communications Hub Function which forms part of the Communications Hub has been Withdrawn from a Non-Domestic Premises;

(b) return of a Communications Hub to the DCC due to a Special Second-Fuel Installation;

(c) return of a Communications Hub to the DCC due to a Special WAN-Variant Installation;

(d) loss or destruction of or damage to a Communications Hub, which occurred while the relevant Party was responsible for such risk and which was caused otherwise than by a breach of this Code by the DCC or a CH Defect;

(e) return of a Communications Hub to the DCC, other than where another reason under this Section F9.5 applies;

(f) that the Communications Hub has a CH Defect;

(g) loss or destruction of or damage to a Communications Hub caused by a breach of this Code by the DCC;

(h) rejection of a Communications Hub in accordance with Section F6.10 (Rejected Communications Hub Products); and

(i) return of a Communications Hub to the DCC where requested by the DCC under Section F8.1 (Product Recall / Technology Refresh).

Categories of Responsibility

F9.6 For the purposes of this Section F9 and the Charging Methodology:

(a) each of the reasons described in Sections F9.5(d) and (e) constitute a "**CH User Responsibility**", and where the Party required to do so under Section F9.2 fails to specify a reason in accordance with that Section the reason shall be deemed to be a CH User Responsibility;

(b) each of the reasons described in Sections F9.5(f) and (g) (where they apply prior to completion of the installation of the Communications Hub at a premises in accordance with the CH Installation and Maintenance Support Materials) and Section F9.5(h) constitute a "**CH Pre-Installation DCC Responsibility**";

(c) each of the reasons described in Sections F9.5(f) and (g) (where they apply following completion of the installation of the Communications Hub at a premises in accordance with the CH Installation and Maintenance Support Materials) constitute a "**CH Post-Installation DCC Responsibility**";

(d) the reason described in Sections F9.5(i) constitute a "**Product Recall or Technology Refresh**"; and

(e) the reasons described in Sections F9.5(a), (b) and (c) do not need to be

categorised, as they do not directly give rise to a Charge or an adjustment to the Charges under this Section F9.

CH Fault Diagnosis

F9.7 The DCC has the right to examine and test returned Communications Hubs and to investigate the cause of any damage to or loss or destruction of Communications Hubs to verify whether the reason given by a Party pursuant to Section F9.2 is correct (being "**CH Fault Diagnosis**").

F9.8 The DCC shall undertake CH Fault Diagnosis in accordance with the process for the same described in the CH Installation and Maintenance Support Materials (which may include sampling and extrapolation of results based on sampling).

F9.9 The DCC shall, within 10 days after the return of Communications Hubs or notification of their loss or destruction by a Party, notify that Party (via the CH Ordering System) if the DCC intends to undertake any CH Fault Diagnosis in respect of those Communications Hub.

F9.10 In the absence of a notification in accordance with Section F9.9, the reason given by a Party in accordance with Section F9.2 in respect of the Communications Hubs in question shall be deemed to be correct.

F9.11 Provided the DCC has first given notice in accordance with Section F9.9, where the DCC disputes the reason given by a Party pursuant to Section F9.2 in respect of any Communications Hubs, the DCC shall provide to the Party a report setting out the DCC's analysis of why the reason given by the Party is not correct.

F9.12 Where the DCC does not provide a report to the Party in accordance with Section F9.11 within 35 days after the DCC's notice to a Party under Section F9.9, the reason given by the Party in accordance with Section F9.2 in respect of the Communications Hubs in question shall be deemed to be correct.

F9.13 Unless the Party notifies the DCC of the Party's objection to the DCC's analysis within 35 days after receipt of a report in accordance with Section F9.11, the analysis set out in the report shall be deemed to be correct.

F9.14 Where the Party notifies the DCC of an objection within the time period required by Section F9.13, then either of them may refer the matter to the Panel for determination (which determination shall be final and binding for the purposes of this Code). Where the Panel is unable to determine the reason for a Communications Hub's return, then the reason given by the relevant Party under Section F9.2 shall be deemed to be correct.

Reporting on DCC Faults

F9.15 The DCC shall report to the Panel and the other Parties on the number of Communications Hubs for which the reason for return, loss or destruction is determined in accordance with this Section F9 to have been a CH Pre-Installation DCC Responsibility or a CH Post-Installation DCC Responsibility. The DCC shall report in respect of successive periods of three months (starting with the month in which Communications Hubs are first delivered pursuant to this Section F). Such report shall include a supporting explanation of the circumstances that gave rise to such instances of CH Pre-Installation DCC Responsibility or CH Post-Installation DCC Responsibility. Where the DCC is disputing (under CH Fault Diagnosis) whether an instance of CH Pre-Installation DCC Responsibility or CH Post-Installation DCC Responsibility has arisen, the DCC shall not include those instances until the matter is finally resolved (under CH Fault Diagnosis).

Compensation for CH Type Faults

F9.16 Where the reason for a Communications Hub's return, loss or destruction is determined in accordance with this Section F9 to have been a CH Post-Installation DCC Responsibility, then a "**CH Type Fault**" shall be said to have occurred in respect of that Communications Hub (at the time of such return or notification, and in respect of the Party making such return or notification).

F9.17 Section F9.18 shall apply in respect of a Region and a calendar year, where the number of CH Type Faults relating to that Region and occurring during that calendar year exceeds 0.5% of the total number of Communications Hubs that are installed at premises within that Region as at the end of that calendar year.

F9.18 Where this Section F9.18 applies in respect of a Region and a calendar year, the DCC shall be liable to pay to Parties collectively an amount of liquidated damages equal to the positive amount (if any) calculated as follows:

(a) £50.00; multiplied by

(b) the Consumer Prices Index for April of that calendar year, divided by the Consumer Prices Index for September 2013; multiplied by

(c) (i) the number of CH Type Faults relating to that Region and occurring during that calendar year; less (ii) 0.5% of the total number of Communications Hubs that are installed at premises within that Region as at the end of that calendar year; less (iii) the number of CH Type Faults relating to that Region and occurring during that calendar year for which the DCC is liable to pay a CH Batch Fault Payment.

F9.19 The aggregate amount (if any) payable by the DCC under Section F9.18 in respect of a Region and a calendar year shall be payable by the DCC to each Party (the amount payable to each Party being a "**CH Type Fault Payment**") pro-rated in proportion to:

(a) the number of CH Type Faults (across all Regions) which occurred in respect of that Party during that calendar year, less the number of CH Type Faults (across all Regions) which occurred in respect of that Party during that calendar year for which the DCC is liable to pay a CH Batch Fault Payment; as compared to

(b) the total number of CH Type Faults (across all Regions) which occurred in respect of all Parties during that calendar year, less the number of CH Type Faults (across all Regions) which occurred in respect of all Parties during that calendar year for which the DCC is liable to pay a CH Batch Fault Payment.

Compensation for Batch Faults

F9.20 A "**CH Batch Fault**" shall occur in respect of a Delivery Batch where:

(a) the number of CH Type Faults which occur in respect of a Communications Hub forming part of that Delivery Batch, and which occur within 12 months

following completion of the installation of that Communications Hub; exceeds

(b) 10% of the number of Communications Hubs comprising that Delivery Batch.

F9.21 Where a CH Batch Fault occurs in respect of a Delivery Batch, the DCC shall be liable to pay to each Party an amount of liquidated damages (being a "**CH Batch Fault Payment**") equal to:

(a) £50.00; multiplied by

(b) the Consumer Prices Index for April of that calendar year, divided by the Consumer Prices Index for September 2013; multiplied by

(c) the number of CH Type Faults which occurred in respect of that Party and a Communications Hub which formed part of that Delivery Batch, and which occur within 12 months following completion of the installation of that Communications Hub.

Payment of Type Fault and Batch Fault Compensation

F9.22 The DCC shall include each CH Type Fault Payment and each CH Batch Fault Payment payable to a Party as a credit in favour of that Party under the DCC's Invoices (so as to reduce the Charges payable by that Party).

Compensation for Product Recall or Technology Refresh

F9.23 Where the reason for a Communications Hub's return is determined in accordance with this Section F9 to have been a Product Recall or Technology Refresh, then the DCC shall (notwithstanding Section M2.8 (Exclusion of Other Liabilities)) be liable to each other Party for the reasonable costs and expenses incurred by that Party in:

(a) any corrective action taken by that Party in accordance with this Code or other Laws and/or Directives (including any withdrawal or recall activities); and/or

(b) notifying or warning Energy Consumers of any corrective action taken by the DCC and/or any other Party (and providing Energy Consumers with relevant information regarding such corrective action).

Damage Caused by Defective Communications Hubs

F9.24 Where a CH Defect causes loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data), such loss or damage shall be deemed to have been caused by a breach of this Code by the DCC, including for the purposes of M2.5 (Damage to Physical Property).

Exclusive Remedies for Site Visits

F9.25 Notwithstanding Sections F9.24 and M2.6(a) (Recovery of Loss which is Expressly Permitted), no Party shall be entitled to recover from the DCC any costs or expenses incurred in attending a premises for the purposes of repairing or replacing any Devices damaged or destroyed as a result of a CH Defect. This Section F9.25 is without prejudice to the CH Type Fault Payments, CH Batch Fault Payments, and compensation under Section F9.23 in respect of Product Recall or Technology Refresh.

Exclusive Remedy for Damaged or Lost Communications Hubs

F9.26 No Party shall have any liability to the DCC for damage to, or loss or destruction of, Communications Hubs. This Section F9.26 is without prejudice to the Charges payable in respect of the Communications Hub Services.

F10 TEST COMMUNICATIONS HUBS

Overview

F10.1 Unless expressly stated otherwise, the references in this Code to Communications Hubs do not include Test Communications Hubs.

F10.2 Without limiting the generality of Section F10.1, because Test Communications Hubs are not to be treated as Communications Hubs, Test Communications Hubs shall:

(a) not be included in Communications Hub Forecasts or Communications Hub Orders;

(b) not be subject to Sections F5 (Communications Hub Forecasts & Orders) to F9 (Categories of Communications Hub Responsibility);

(c) not be (or be capable of being) Commissioned; and

(d) only be populated with Test Certificates (and not actual Organisation Certificates or Device Certificates).

Prototype Communications Hubs

F10.3 Where the DCC provides a Prototype Communications Hub as a Test Communications Hub (in accordance with the definition of Test Communications Hub), the DCC shall provide details of the manner in which the Prototype Communications Hub does not comply with CHTS. For the purposes of this Section F10.3 and the definition of Prototype Communications Hub, until such time as the CHTS forms part of this Code, the references to the CHTS shall be construed by reference to the draft of the CHTS that the Secretary of State directs from time to time for the purposes of this Section F10.3.

Provision of Test Communications Hubs

F10.4 The DCC shall, from the relevant date set out in the End-to-End Testing Approach Document, provide Test Communications Hubs to other Parties and to any other person that requests them (in each case in accordance with the other provisions of this Section F10). The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to

provide Test Communications Hubs from an earlier date. Where the DCC is able to make Test Communications Hubs available from an earlier date, the DCC shall publish a notice to that effect on the DCC Website.

F10.5 Where a person that is not a Party wishes to order Test Communications Hubs, the DCC shall offer terms upon which Test Communications Hubs may be ordered. Such offer shall be provided as soon as reasonably practicable after receipt of the request, and shall be based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances). A person that is bound by an agreement entered into with the DCC pursuant to this Section F10.5 shall be a "**TCH Participant**". The DCC shall not provide Test Communications Hubs to a person that is not a Party or a TCH Participant.

F10.6 The DCC shall allow Parties and TCH Participants to order and return Test Communications Hubs via a reasonable means.

F10.7 The DCC shall publish on the DCC Website a guide describing the process by which Parties and other persons may obtain and return Test Communications Hubs.

Ordering, Delivery, Rejection and Returns

F10.8 Where a Party or a TCH Participant has ordered one or more Test Communications Hubs via the means described in Section F10.6:

(a) the person that ordered the Test Communications Hubs shall be liable to pay the applicable Charge;

(b) the DCC shall deliver the Test Communications Hubs to the location in Great Britain requested by the person that ordered the Test Communications Hubs, on the date requested by that person (provided that the DCC shall have no obligation to deliver Test Communications Hubs earlier than the date 18 weeks after the date on which the Test Communications Hubs were ordered);

(c) delivery of the Test Communications Hubs shall occur on their removal from the delivery vehicle at the delivery location;

(d) legal and beneficial ownership of (and responsibility for loss or destruction of

or damage to) the Test Communications Hubs shall vest in the person that ordered them on commencement of their unloading at the delivery location (where not unloaded by the DCC) or on completion of their unloading at the delivery location (where unloaded by the DCC);

(e) the person that ordered the Test Communications Hubs shall be entitled to reject a delivery and arrange for the return of the rejected Test Communications Hubs to the DCC on the following basis (and only where notified to the DCC within five days of the delivery date):

(i) to the extent the delivery contained more Test Communications Hubs than were ordered; and/or

(ii) to the extent the Test Communications Hub Products are (or reasonably appear on a visual inspection to be) damaged or have been (or reasonably appear on a visual inspection to have been) tampered with (and such damage or tampering occurred prior to their delivery);

(f) the person that ordered the Test Communications Hubs shall be entitled to return them to the DCC where a CH Defect arises within 6 months following their delivery, but not thereafter (for which purpose, the definition of CH Defect shall be construed by reference to the requirements for Test Communications Hubs rather than those for Communications Hubs);

(g) a person wishing to return a Test Communications Hub to the DCC pursuant to (e) or (f) above shall return it to the DCC in accordance with the relevant rules applicable to Communications Hubs under Section F8 (Removal and Return of Communications Hubs); and

(h) legal and beneficial ownership of (and responsibility for loss or destruction of or damage to) the Test Communications Hubs rejected or returned pursuant to this Section F10.8 shall revert to the DCC on completion of their unloading at the returns location (where not unloaded by the DCC) or on commencement of their unloading at the returns location (where unloaded by the DCC).

F10.9 The rejection and/or return of Test Communications Hubs by a Party or TCH

Participant pursuant to Section F10.8 is relevant in determining the Charges payable by that Party or TCH Participant. Where the DCC wishes to do so, it may undertake physical and electronic analysis in respect of Test Communications Hubs rejected or returned, in which case the process for CH Fault Diagnosis shall apply, but:

(a) by reference to the reason for rejection and/or return given pursuant to Section F10.6 (rather than by reference to the reason given pursuant to Section F9 (Categories of Communications Hub Responsibility)); and

(b) without the DCC's ability to apply sampling and extrapolation to the extent that such an ability is set out in the CH Installation and Maintenance Support Materials.

Use of Test Communications Hubs

F10.10 The Party or TCH Participant that ordered a Test Communications Hub shall (unless or until it is returned pursuant to Section F10.8) ensure that the Test Communications Hub shall:

(a) only be used by Parties or TCH Participant for the purposes of tests undertaken under this Code, or for the purposes of testing Devices or Systems to be used in relation to this Code; and

(b) be used and maintained in accordance with Good Industry Practice, and the requirements of this Code applicable to Test Communications Hubs.

F10.11 Where a CH Defect in a Test Communications Hub (for which purpose, the definition of CH Defect shall be construed by reference to the requirements for Test Communications Hubs rather than those for Communications Hubs) causes loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data), such loss or damage shall be deemed to have been caused by a breach of this Code by the DCC, including for the purposes of M2.5 (Damage to Physical Property).

SECTION G - SECURITY

G1 SECURITY: GENERAL PROVISIONS

Interpretation

G1.1 Sections G2 to G9 shall be interpreted in accordance with the following provisions of this Section G1.

Transitional Period for Updated or Replacement Standards

G1.2 Section G1.3 applies where:

(a) the DCC or any User is required, in accordance with any provision of Sections G2 to G9, to ensure that it, or that any of its policies, procedures, systems or processes, complies with:

(i) any standard, procedure or guideline issued by a third party; and

(ii) any equivalent to that standard, procedure or guideline which updates or replaces it from time to time; and

(b) the relevant third party issues an equivalent to that standard, procedure or guideline which updates or replaces it.

G1.3 Where this Section G1.3 applies, the obligation on the DCC or User (as the case may be):

(a) shall be read as an obligation to comply with the updated or replaced standard, procedure or guideline from such date as is determined by the Panel (having considered the advice of the Security Sub-Committee) in respect of that document; and

(b) prior to that date shall be read as an obligation to comply (at its discretion) with either:

(i) the previous version of the standard, procedure or guideline; or

(ii) the updated or replaced standard, procedure or guideline.

G1.4 Any date determined by the Panel in accordance with Section G1.3 may be the subject of an appeal by the DCC or any User to the Authority (whose decision shall be final and binding for the purposes of this Code).

Obligations on Users

G1.5 Obligations which are expressed to be placed on a User shall, where that User performs more than one User Role, be read as applying to it separately in respect of each of its User Roles.

G1.6 For the purposes of Section G1.5, where any Network Party is deemed to have nominated itself as a Registration Data Provider (in accordance with the definition of Registration Data Provider), its role as a Registration Data Provider shall be treated as if it were an additional category of User Role.

Exclusion for Export Suppliers and Registered Supplier Agents

G1.7 Where a User acts in the User Role of 'Export Supplier' or 'Registered Supplier Agent', it is not to be subject to any of the obligations expressed to be placed on Users except for those obligations set out at:

(a) Sections G3.2 to G3.3 (Unauthorised Activities: Duties to Detect and Respond);

(b) Sections G3.8 to G3.9 (Management of Vulnerabilities);

(c) Sections G5.14 to G5.18 (Information Security: Obligations on Users), save that for this purpose the reference:

(i) in Section G5.18(b)(i) to "Sections G3 and G4" shall be read as if it were to "Sections G3.2 to G3.3 and G3.8 to G3.9"; and

(ii) in Section G5.18(b)(iii) to "Sections G5.19 to G5.24" shall be read as if it were to "Section G5.19(d)"; and

(d) G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users).

Disputes

G1.8 Where, in ~~A~~any dispute between a Party and a User, a question arises as to whether that ~~regarding the compliance of a~~ User has complied with any of its obligations under Sections G3 to G6:

(a) that question may be referred by either of them to the Panel for its determination; and

(b) ~~. W~~where ~~a Party~~either of them disagrees with any such determination of the Panel, then ~~that Party~~it may refer the matter to the Authority in accordance with Section M7 (Dispute Resolution).

G1.9 Section G1.8:

(a) shall be without prejudice to the provisions of Section M8.2 (Notification of an Event of Default); and

~~(c)~~(b) shall not apply in respect of any other question in dispute between a Party and a User relating to or arising from the question of whether the User has complied with any of its obligations under Sections G3 to G6.

G2 SYSTEM SECURITY: OBLIGATIONS ON THE DCC

Unauthorised Activities: Duties to Detect and Respond

G2.1 The DCC shall take reasonable steps~~use its reasonable endeavours~~:

(a) to ensure that the DCC Systems are capable of detecting any unauthorised connection that has been made to them, and any unauthorised attempt to connect to them, by any other System; and

(b) if the DCC Systems detect such a connection or attempted connection, to ensure that the connection is terminated or the attempted connection prevented (as the case may be).

G2.2 The DCC shall take reasonable steps~~use its reasonable endeavours~~:

(a) to ensure that the DCC Total System is capable of detecting any unauthorised software that has been installed or executed on it and any unauthorised attempt to install or execute software on it;

(b) if the DCC Total System detects any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

G2.3 The DCC shall:

(a) take reasonable steps~~use its reasonable endeavours~~ to ensure that:

(i) the DCC Total System is capable of identifying any deviation from its expected configuration; and

(ii) any such identified deviation is rectified; and

(b) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of the DCC Total System.

G2.4 The DCC shall ~~use its reasonable endeavours~~take reasonable steps to ensure that the DCC Total System:

(a) is capable of identifying any unauthorised or unnecessary network port, protocol, communication, application or network service;

(b) causes or permits to be open at any time only those network ports, and allows only those protocols, which are required at that time for the effective operation of that System, and blocks all network ports and protocols which are not so required; and

(c) causes or permits at any time only the making of such communications and the provision of such applications and network services as are required at that time for the effective operation of that System.

G2.5 The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that each component of the DCC Total System is, at each point in time, enabled only with the functionality that is necessary for it effectively to fulfil its intended role within the DCC Total System at that time.

G2.6 The DCC shall:

(a) ensure that the DCC Total System records all system activity (including all attempts to access resources, or Data held, on it) in audit logs;

(b) ensure that the DCC Total System detects any attempt by any person to access resources, or Data held, on it without possessing the authorisation required to do so; and

(c) take reasonable steps ~~use its reasonable endeavours~~ to ensure that the DCC Total System prevents any such attempt at unauthorised access.

G2.7 The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that the DCC Total System is capable of detecting any instance of Data leaving it by any means (including in particular by network transfers and the use of removable media) without authorisation.

Adverse Events: Duties to Detect and Prevent

G2.8 The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that:

(a) the DCC Total System detects any Denial of Service Event; and

(b) any unused or disabled component or functionality of the DCC Total System is incapable of being a means by which that System is Compromised.

G2.9 The DCC shall use its best endeavours to:

(a) ensure that the DCC Total System is not Compromised;

(b) where the DCC Total System is Compromised, minimise the extent to which it is Compromised and any adverse effect arising from it having been Compromised; and

(c) ensure that the DCC Total System detects any instance in which it has been Compromised.

Security Incident Management

G2.10 The DCC shall ensure that, where the DCC Total System detects any:

(a) unauthorised event or deviation of a type referred to in Sections G2.1 to G2.7; or

(b) event which results, or was capable of resulting, in the DCC Total System being Compromised,

the DCC takes all of the steps required by the DCC Information Security Management System.

G2.11 The DCC shall, on the occurrence of a Major Security Incident in relation to the DCC Total System, promptly notify the Panel and the Security Sub-Committee.

System Design and Operation

G2.12 The DCC shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate the DCC Total System so as to protect it from being Compromised.

Management of Vulnerabilities

G2.13 The DCC shall ensure that an organisation which is a CESG CHECK service provider carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

(a) in respect of each DCC System, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to the DCC Systems.

G2.14 The DCC shall ensure that it carries out assessments that are designed to identify any vulnerability of the DCC Systems to Compromise:

(a) in respect of each DCC System, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of the DCC Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to the DCC Systems.

G2.15 Where, following any assessment of the DCC Systems in accordance with Section G2.13 or G2.14, any such vulnerability has been detected, the DCC shall:

(a) take reasonable steps ~~use its reasonable endeavours~~ to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable; and

(b) in the case of a material vulnerability, promptly notify the Security Sub-Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed.

Management of Data

G2.16 Where the DCC carries out a Back-Up of any Data held on the DCC Total System, it shall ensure that the Data which are Backed-Up are:

(a) protected in accordance with the Information Classification Scheme, including when being transmitted for the purposes of Back-Up; and

(b) stored on media that are located in physically secure facilities, at least one of which facilities must be in a different location to that part of the DCC Total System on which the Data being Backed-Up is ordinarily held.

G2.17 The DCC shall develop and maintain, and hold all Data in accordance with, a DCC Data Retention Policy.

G2.18 The DCC shall ensure that where, in accordance with the DCC Data Retention Policy, any Data are no longer required for the purposes of the Authorised Business, they are securely deleted in compliance with:

(a) HMG Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(b) any equivalent to that HMG Information Assurance Standard which updates or replaces it from time to time.

DCC Total System: Duty to Separate

G2.19 The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that any software or firmware installed on the DCC Total System for the purposes of security is Separated from any software or firmware that is installed on that System for any other purpose.

G2.20 The DCC shall ensure that:

(a) all DCC Systems which form part of the DCC Total System are Separated from any other Systems;

(b) the DCC IT Testing and Training Systems and DCC IT Supporting Systems are Separated from the DCC Live Systems; and

(c) subject to the provisions of Section G2.21, each individual System within the DCC Live Systems is Separated from each other such System.

G2.21 The individual System referred to at paragraph (c) of the definition of DCC Live Systems in Section A1 (Definitions) need not be Separated from the individual System referred to at paragraph (a) of that definition to the extent that it uses that individual System referred to at paragraph (a) solely for the purposes of confirming the relationship between:

(a) an MPAN or MPRN and any Party Details;

(b) an MPAN or MPRN and any Device; or

(c) any Party Details and any User ID.

DCC Live Systems: Independence of User Systems

G2.22 The DCC shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems,

unless that individual satisfies the requirements of Section G2.23.

G2.23 An individual satisfies the requirements of this Section only if, at any time at which that individual is engaged in any activity described in Section G2.22, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any User Systems; or

(ii) the development, design, build, testing, configuration, implementation,

operation, maintenance, modification or decommissioning of any User Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the DCC reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with the DCC Information Security Management System.

G2.24 The DCC shall ensure that no resources which form part of the DCC Live Systems also form part of any User Systems.

Monitoring and Audit

G2.25 The DCC shall ensure that all system activity audit logs are reviewed regularly in accordance with the DCC Information Security Management System.

G2.26 The DCC shall ensure that all such system activity recorded in audit logs is recorded in a standard format which is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information), or any equivalent to that British Standard which updates or replaces it from time to time; and

(b) in the case of activity on the DCC Systems only, CESG Good Practice Guide 18:2012 (Forensic Readiness), or any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

G2.27 The DCC shall monitor the DCC Systems in compliance with:

(a) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(b) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

G2.28 The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that the DCC Systems are capable of detecting Anomalous Events, in particular by reference to the:

(a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Commands, Service Responses and Alerts;

(b) audit logs of each component of the DCC Total System;

(c) error messages generated by each device which forms part of the DCC Total System;

(d) Incident Management Log compiled in accordance with Section H9; and

(e) patterns of traffic over the SM WAN.

G2.29 The DCC shall:

(a) take reasonable steps ~~use its reasonable endeavours~~ to ensure that the DCC Systems detect all Anomalous Events; and

(b) ensure that, on the detection of any Anomalous Event, it takes all of the steps required by the DCC Information Security Management System.

Manufacturers: Duty to Notify and Be Notified

G2.30 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which forms part of the DCC Total System, it shall:

(a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware or the developer of the software or firmware (as the case may be);

(b) take reasonable steps ~~use its reasonable endeavours~~ to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable; and

(c) promptly notify the Security Sub-Committee of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which those steps are intended to be completed.

G2.31 The DCC shall not be required to notify a manufacturer or developer in accordance with

Section G2.30(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified.

G2.32 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of the DCC Total System arrangements designed to ensure that the DCC will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software or firmware.

G2.33 Any arrangements established in accordance with Section G2.32 may provide that the manufacturer or developer (as the case may be) need not be required to notify the DCC where that manufacturer or developer has reason to be satisfied that the DCC is already aware of the matter that would otherwise be notified under the arrangements.

Parse and Correlate Software: Duty to Notify

G2.34 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any version of the Parse and Correlate Software, it shall notify the Users and (wherever it is reasonably practicable to do so) the developer of the software.

G2.35 The DCC shall not be required to notify a developer or User in accordance with Section G2.34 where it has reason to be satisfied that the developer or User is already aware of the matter that would otherwise be notified.

Cryptographic ~~Processing~~Credential Tokens

G2.36 Before supplying any Cryptographic Credential Token to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of the software which forms part of that Cryptographic Credential Token:

(a) operates so as to generate Public Keys each of which is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated;

(b) has been adequately tested for the purpose of ensuring that it fulfils its intended purpose; and

(c) has been subject to a software code review, by an individual or organisation with the professional competence to carry out such a review, for the purpose of identifying any vulnerabilities in the code that were not intended as a feature of its design.

G2.37 The DCC shall, wherever it is reasonably practicable to do so, establish with the manufacturers of the hardware and developers of the software and firmware which form part of any Cryptographic Credential Tokens to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software or firmware.

G2.38 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any hardware, software or firmware which form part of any Cryptographic Credential Token which has been supplied by it in accordance with the provisions of this Code, it shall notify the Subscribers for Certificates associated with the use of Cryptographic Credential Tokens and (wherever it is reasonably practicable to do so) the manufacturer of the hardware or (as the case may be) developer of the software or firmware.

Cryptographic Processing

~~G2.36~~G2.39 The DCC shall ensure that it carries out all Cryptographic Processing which:

(a) is for the purposes of complying with its obligations as CoS Party; or

(b) results in the application of a Message Authentication Code to any message in order to create a Command,

within Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

~~G2.37~~G2.40 The DCC shall ensure that it carries out all other Cryptographic Processing only within Cryptographic Modules established in accordance with its Information Classification Scheme.

Network Time

~~G2.38~~G2.41 For the purposes of Section G2.~~39~~42:

(a) the "**Network Time**" means one or more time sources maintained by the DCC from which all Commissioned Communications Hub Functions synchronise time; and

(b) the "**Independent Time Source**" means a time source that is:

(i) accurate;

(ii) not maintained by the DCC; and

(iii) determined in a manner that is independent of any part of the DCC Total System.

~~G2.39~~G2.42 The DCC shall ensure that:

(a) the DCC Total System is capable of detecting any instance in which the Network Time materially differs from the Independent Time Source; and

(b) if the DCC Total System detects such a material difference, the DCC takes all of the steps required by the DCC Information Security Management System to rectify the inaccuracy of its Network Time.

Integrity of Communication over the SM WAN

~~G2.40~~G2.43 The DCC shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that all communications which are transmitted over the SM WAN are protected so that the Data contained in them remains confidential, and their integrity is preserved, at all times during transmission to and from Communications Hubs.

~~G2.41~~G2.44 The DCC shall not process any communication received over the SM WAN, or send to any Party any communication over the SM WAN, where it is aware that the

Data contained in that communication has been Compromised.

G3 SYSTEM SECURITY: OBLIGATIONS ON USERS

Unauthorised Activities: Duties to Detect and Respond

G3.1 Each User shall:

(a) take reasonable steps ~~use its reasonable endeavours~~ to ensure that:

(i) its User Systems are capable of identifying any deviation from their expected configuration; and

(ii) any such identified deviation is rectified; and

(b) for these purposes maintain at all times an up-to-date list of all hardware, and of all software and firmware versions and patches, which form part of the configuration of those User Systems.

G3.2 Each User shall take reasonable steps~~use its reasonable endeavours~~:

(a) to ensure that its User Systems are capable of detecting any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;

(b) if those User Systems detect any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

G3.3 Each User shall:

(a) ensure that its User Systems record all attempts to access resources, or Data held, on them;

(b) ensure that its User Systems detect any attempt by any person to access resources, or Data held, on them without possessing the authorisation required to do so; and

(c) take reasonable steps ~~use its reasonable endeavours~~ to ensure that its User Systems prevent any such attempt at unauthorised access.

Security Incident Management

G3.4 Each User shall ensure that, on the detection of any unauthorised event of the type referred to at Sections G3.1 to G3.3, it takes all of the steps required by its User Information Security Management System.

G3.5 Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, promptly notify the Panel and the Security Sub-Committee.

System Design and Operation

G3.6 Each User shall, at each stage of the System Development Lifecycle, have regard to the need to design and operate its User Systems so as to protect them from being Compromised.

Management of Vulnerabilities

G3.7 Each Supplier Party shall ensure that either a tester who has achieved CREST certification or an organisation which is a CESG CHECK service provider carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of its User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G3.8 Each User shall ensure that it carries out assessments that are designed to identify any vulnerability of its User Systems to Compromise:

(a) in respect of each of its User Systems, on at least an annual basis;

(b) in respect of each new or materially changed component or functionality of its

User Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G3.9 Where, following any assessment of its User Systems in accordance with Section G3.7 or G3.8, any material vulnerability has been detected, a User shall ensure that it:

(a) takes reasonable steps ~~uses its reasonable endeavours~~ to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable; and

(b) promptly notifies the Security Sub-Committee of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) and the time within which they are intended to be completed.

Management of Data

G3.10 Each User shall:

(a) develop and maintain, and hold all Data in accordance with, a User Data Retention Policy; and

(b) when any Data held by it cease to be retained in accordance with the User Data Retention Policy, ensure that they are securely deleted in accordance with its Information Classification Scheme.

User Systems: Duty to Separate

G3.11 Each User shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that any software or firmware that is installed on its User Systems for the purposes of security is Separated from any software or firmware that is installed on those Systems for any other purpose.

User Systems: Independence of DCC Live Systems

G3.12 Each User shall ensure that no individual is engaged in:

(a) the development of bespoke software or firmware, or the customisation of any

software or firmware, for the purpose of its installation on any part of its User Systems; or

(b) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of its User Systems,

unless that individual satisfies the requirements of Section G3.13.

G3.13 An individual satisfies the requirements of this Section only if, at any time at which that individual is engaged in any activity described in Section G3.12, he or she:

(a) is not at the same time also engaged in:

(i) the development of bespoke software or firmware, or the customisation of any software or firmware, for the purpose of its installation on any part of the DCC Live Systems; or

(ii) the development, design, build, testing, configuration, implementation, operation, maintenance, modification or decommissioning of any part of the DCC Live Systems; and

(b) has not been engaged in any activity described in paragraph (a) for a period of time which the User reasonably considers to be appropriate, having regard to the need to ensure the management of risk in accordance with its User Information Security Management System.

G3.14 Each User shall ensure that no resources which form part of its User Systems also form part of the DCC Live Systems.

Monitoring

G3.15 Each Supplier Party shall take reasonable steps ~~use its reasonable endeavours~~ to ensure that its User Systems are capable of detecting Anomalous Events, in particular by reference to the:

(a) sending or receipt (as the case may be) of Service Requests, Pre-Commands, Signed Pre-Commands, Commands, Service Responses and Alerts;

(b) audit logs of each Device for which it is the Responsible Supplier; and

(c) error messages generated by each Device for which it is the Responsible Supplier.

G3.16 Each Supplier Party shall:

(a) take reasonable steps~~use its reasonable endeavours~~ to ensure that its User Systems detect all Anomalous Events; and

(b) ensure that, on the detection by its User Systems of any Anomalous Event, it takes all of the steps required by its User Information Security Management System.

Manufacturers: Duty to Notify and Be Notified

G3.17 Where a User becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of:

(a) any hardware, software or firmware which forms part of its User Systems; or

(b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function) for which it is the Responsible Supplier,

it shall comply with the requirements of Section G3.18.

G3.18 The requirements of this Section are that the User shall:

(a) wherever it is reasonably practicable to do so notify the manufacturer of the hardware or Device or the developer of the software or firmware (as the case may be);

(b) take reasonable steps ~~use its reasonable endeavours~~ to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable; and

(c) promptly notify the Security Sub-Committee of the steps being taken to rectify the cause of the vulnerability or likely cause of the material adverse effect, or to mitigate its potential impact (as the case may be), and the time within which

those steps are intended to be completed.

G3.19 A User shall not be required to notify a manufacturer or developer in accordance with Section G3.18(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified

G3.20 Each User shall, wherever it is practicable to do so, establish with:

(a) the manufacturers of the hardware and developers of the software and firmware which form part of its User Systems; and

(b) (where applicable) any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function) for which it is the Responsible Supplier,

arrangements designed to ensure that the User will be notified where any such manufacturer or developer (as the case may be) becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such hardware, software, firmware or Device.

G3.21 Any arrangements established in accordance with Section G3.20 may provide that the manufacturer or developer (as the case may be) need not be required to notify the User where that manufacturer or developer has reason to be satisfied that the User is already aware of the matter that would otherwise be notified under the arrangements.

Cryptographic Processing

G3.22 Each User shall ensure that it carries out Cryptographic Processing only within Cryptographic Modules established in accordance with its Information Classification Scheme.

User Systems: Physical Location

G3.23 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

(a) any Cryptographic Module which constitutes a component of its User Systems and in which:

(i) any Private Key that is used to Digitally Sign Pre-Commands is held; and

(ii) Pre-Commands are Digitally Signed; and

(b) any functionality of its User Systems which is used to apply Supply Sensitive Checks,

is located, operated, configured, tested and maintained in the United Kingdom by User Personnel who are located in the United Kingdom.

G3.24 Each User to which Section G3.23 applies shall ensure that the components and the functionality of its User Systems to which that Section refers are operated from a sufficiently secure environment in accordance with the provisions of Section G5.17.

Supply Sensitive Check

G3.25 Each User which is an Eligible User in relation to any Supply Sensitive Service Request shall ensure that:

(a) it applies a Supply Sensitive Check prior to Digitally Signing a Pre-Command in respect of any Supply Sensitive Service Request;

(b) it both applies that Supply Sensitive Check and Digitally Signs the relevant Pre-Command in the United Kingdom; and

(c) the Pre-Command has been processed only in the United Kingdom between the application of the Supply Sensitive Check and the Digital Signature.

G4 ORGANISATIONAL SECURITY: OBLIGATIONS ON USERS AND THE DCC

Obligations on Users

G4.1 Each User shall:

(a) ensure that each member of its User Personnel who is authorised to access Data held on its User Systems holds a security clearance which is appropriate to the role performed by that individual and to the Data which he or she is authorised to access; and

(b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data which he or she is authorised to access.

G4.2 Each User shall comply with Section G4.3 in respect of any of its User Personnel who are authorised to carry out activities which:

(a) involve access to resources, or Data held, on its User Systems; and

(b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device in a manner that could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises.

G4.3 Each User shall ensure that any of its User Personnel who are authorised to carry out the activities identified in Section G4.2:

(a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or

(ii) any equivalent to that British Standard which updates or replaces it from time to time; and

(b) where they are not located in the United Kingdom are subject to security

screening in a manner that is compliant with:

(i) the British Standard referred to in Section G4.3(a); or

(ii) any comparable national standard applying in the jurisdiction in which they are located.

Obligations on the DCC

G4.4 The DCC shall:

(a) ensure that each member of DCC Personnel who is authorised to access Data held on the DCC Total System holds a security clearance which is appropriate to the role performed by that individual and to the Data to which he or she is authorised to access; and

(b) annually review the security clearance held by each such individual and ensure that it continues to be appropriate to the role performed by that individual and to the Data to which he or she is authorised to access.

G4.5 The DCC shall comply with Section G4.6 in respect of any of the DCC Personnel who are authorised to carry out activities which:

(a) involve access to resources, or Data held, on the DCC Total System; and

(b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device.

G4.6 The DCC shall ensure that any of the DCC Personnel who are authorised to carry out the activities identified in Section G4.5:

(a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or

(ii) any equivalent to that British Standard which updates or replaces it from time to time; and

(b) where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) the British Standard referred to in Section G4.6(a); or

(ii) any comparable national standard applying in the jurisdiction in which they are located.

G4.7 The DCC shall ensure that each member of DCC Personnel who is a Privileged Person has passed a Security Check before being given any access to Data held on the DCC Total System.

G4.8 Where the DCC is required to ensure that any two Systems forming part of the DCC Total System are Separated, it shall either:

(a) ensure that no person is a Privileged Person in relation to both of those Systems; or

(b) to the extent that any person is a Privileged Person in relation to both Systems, it establishes additional controls sufficient to ensure that the activities of that person cannot become a means by which any part of the DCC Live Systems is Compromised to a material extent.

G5 INFORMATION SECURITY: OBLIGATIONS ON THE DCC AND USERS

Information Security: Obligations on the DCC

G5.1 The DCC shall establish, maintain and implement processes for the identification and management of the risk of Compromise to the DCC Total System, and such processes shall comply with:

(a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Management Systems); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time

G5.2 The DCC shall carry out an assessment of such processes for the identification and management of risk:

(a) on at least an annual basis;

(b) on any occasion on which it implements a material change to the DCC Total System; and

(c) on the occurrence of any Major Security Incident in relation to the DCC Total System.

G5.3 Where the DCC is required in accordance with the DCC Licence to obtain and hold ISO 27001 certification, it shall:

(a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as the DCC Information Security Management System;

(b) ensure that the DCC Information Security Management System:

(i) is so designed as to ensure that the DCC complies with its obligations under Sections G2 and G4;

(ii) meets the requirements of Sections G5.4 to G5.13; and

(iii) provides for security controls which are proportionate to the potential impact of each part of the DCC Total System being Compromised, as determined by means of processes for the management of information risk; and

(c) review the DCC Information Security Management System on at least an annual basis, and make any changes to it following such a review in order to ensure that it remains fit for purpose.

The DCC Information Security Management System

G5.4 The DCC Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:

(a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the DCC Total System, including measures relating to Data handling, retention and protection; and

(b) the establishment and maintenance of an Information Classification Scheme in relation to the DCC Total System.

G5.5 The DCC Information Security Management System shall specify the approach of the DCC to:

(a) information security, including its arrangements to review that approach at planned intervals;

(b) human resources security;

(c) physical and environmental security; and

(d) ensuring that the DCC Service Providers establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the DCC.

G5.6 The DCC Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the DCC to establish and maintain a register of the physical and information assets on which it relies for the

purposes of the Authorised Business (including a record of the member of DCC Personnel who has responsibility for each such asset).

G5.7 The DCC Information Security Management System shall incorporate procedures that comply with:

(a) HMG Security Procedures – Telecommunications Systems and Services, Issue Number 2.2 (April 2012), in respect of the security of telecommunications systems and services; or

(b) any equivalent to those HMG Security Procedures which update or replace them from time to time.

G5.8 The DCC Information Security Management System shall incorporate procedures that comply with:

(a) the appropriate standards of the International Organisation for Standards with respect to network security, comprising ISO/IEC 27033-1:2009, ISO/IEC 27033-2:2012 and ISO/IEC 27033-3:2010 (Information Technology – Security Techniques – Network Security); or

(b) any equivalents to those standards of the International Organisation for Standards which update or replace them from time to time.

G5.9 The DCC Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:

(a) measures to restrict access to Data that is stored on or communicated by means of the DCC Total System to those who require such Data and are authorised to obtain it;

(b) the designation of appropriate levels of identity assurance in respect of those who are authorised to access such Data;

(c) the specification of appropriate levels of security clearance in respect of those who are authorised to access such Data;

(d) procedures for granting, amending and removing authorisations in respect of

access to such Data;

(e) procedures for granting and reviewing security clearances for DCC Personnel; and

(f) measures to ensure that the activities of one individual may not become a means by which the DCC Total System is Compromised to a material extent.

G5.10 The DCC Information Security Management System shall incorporate procedures on the management of information security incidents which comply with:

(a) the standard of the International Organisation for Standards in respect of security incident management known as ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.11 The DCC Information Security Management System shall incorporate procedures on the management of information security incidents which in particular make provision for:

(a) the allocation of clearly defined roles and responsibilities to DCC Personnel;

(b) the manner in which such incidents will be monitored, classified, reported and managed;

(c) a communications plan in relation to all communications with respect to such incidents; and

(d) the use of recovery systems in the case of serious incidents.

G5.12 The DCC Information Security Management System shall incorporate procedures on the management of business continuity that comply with:

(a) the following standards of the International Organisation for Standards in respect of business continuity:

(i) ISO/IEC 22301:2012 (Societal Security – Business Continuity Management Systems – Requirements); and

(ii) ISO/IEC 27031:2011 (Information Technology – Security Techniques – Guidelines for Information and Communications Technology Readiness for Business Continuity); and

(b) the Business Continuity Institute Good Practice Guidelines 2013; or

(c) in each case, any equivalents to those standards or guidelines which update or replace them from time to time.

G5.13 The DCC Information Security Management System shall incorporate procedures in relation to the secure management of all Secret Key Material of the DCC, which shall in particular make provision for:

(a) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to its destruction;

(b) the manner in which that Secret Key Material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and

(c) the verifiable destruction of that Secret Key Material.

Information Security: Obligations on Users

G5.14 Each User shall establish, maintain and implement processes for the identification and management of the risk of Compromise to:

(a) its User Systems;

(b) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;

(c) any other Data, Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface;

(d) any Smart Metering Systems for which it is the Responsible Supplier; and

(e) any communications links established between any of its Systems and the DCC Total System, and any security functionality used in respect of those communications links or the communications made over them.

G5.15 Each User shall ensure that such processes for the identification and management of risk comply with:

(a) the standard of the International Organisation for Standards in respect of information security risk management known as ISO/IEC 27005:2011 (Information Technology – Security Techniques – Information Security Management Systems); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.16 Each User shall carry out an assessment of such processes for the identification and management of risk:

(a) on at least an annual basis;

(b) on any occasion on which it implements a material change to:

(i) its User Systems;

(ii) any security functionality used for the purposes of complying with the requirements of this Section G in relation to its User Systems;

(iii) any other Systems or processes on which it relies for the generation, initiation or processing of Service Requests, Service Responses, Alerts or Data communicated over the Self-Service Interface; or

(iv) any Smart Metering Systems for which it is the Responsible Supplier; and

(c) on the occurrence of any Major Security Incident in relation to its User Systems.

G5.17 Each User shall comply with the following standard of the International Organisation for Standards in respect of the security, reliability and resilience of its information

assets and processes and its User Systems:

(a) ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems); or

(b) any equivalent to that standard which updates or replaces it from time to time.

G5.18 Each User shall:

(a) establish, give effect to, maintain, and comply with a set of policies and procedures to be known as its User Information Security Management System;

(b) ensure that its User Information Security Management System:

(i) is so designed as to ensure that it complies with its obligations under Sections G3 and G4;

(ii) is compliant with the standard referred to at Section G5.17;

(iii) meets the requirements of Sections G5.19 to G5.24; and

(iv) provides for security controls which are proportionate to the potential impact of each part of its User Systems being Compromised, as determined by means of processes for the management of information risk; and

(c) review its User Information Security Management System on at least an annual basis, and make any changes to it following such a review in order to ensure that it remains fit for purpose.

The User Information Security Management System

G5.19 Each User Information Security Management System shall incorporate an information security policy which makes appropriate provision in respect of:

(a) measures to identify and mitigate risks to the security of Data stored on or communicated by means of the User Systems, including measures relating to Data handling, retention and protection;

(b) the establishment and maintenance of an Information Classification Scheme in relation to the User Systems;

(c) the management of business continuity; and

(d) the education, training and awareness of User Personnel in relation to information security.

G5.20 Each User Information Security Management System shall specify the approach of the User to:

(a) information security, including its arrangements to review that approach at planned intervals;

(b) human resources security;

(c) physical and environmental security; and

(d) ensuring that any person who provides services to the User for the purpose of ensuring that the User is able to comply with its obligations under this Code must establish and maintain information, human resources, and physical and environmental security measures which are equivalent to those of the User.

G5.21 Each User Information Security Management System shall incorporate a set of asset management procedures which shall make provision for the User to establish and maintain a register of the physical and information assets on which it relies for the purposes of complying with its obligations under this Code.

G5.22 Each User Information Security Management System shall incorporate a policy on access control, which includes provision in respect of:

(a) measures to restrict access to Data that is stored on or communicated by means of the User Systems to those who require such Data and are authorised to obtain it;

(b) procedures for granting, amending and removing authorisations in respect of access to such Data; and

(c) measures to ensure that the activities of one individual may not become a means by which the User Systems are Compromised to a material extent.

G5.23 Each User Information Security Management System shall incorporate procedures on the management of information security incidents which comply with:

(a) the standard of the International Organisation for Standards in respect of security incident management known as ISO/IEC 27035:2011 (Information Technology – Security Techniques – Information Security Incident Management); or

(b) any equivalent to that standard of the International Organisation for Standards which updates or replaces it from time to time.

G5.24 Each User Information Security Management System shall incorporate procedures in relation to the secure management of all Secret Key Material of the User, which shall in particular make provision for:

(a) the security of that Secret Key Material throughout the whole of its lifecycle from its generation to its destruction;

(b) the manner in which that Secret Key Material will be registered, ordered, generated, labelled, distributed, installed, superseded and renewed; and

(c) the verifiable destruction of that Secret Key Material.

Shared Resources

G5.25 Sections G5.26 to G5.28 apply in relation to a User where:

(a) any resources which form part of its User Systems also form part of the User Systems of another User ("**Shared Resources**"); and

(b) by virtue of those Shared Resources:

(i) its User Systems are capable of being a means by which the User Systems of that other User are Compromised (or vice versa); or

(ii) the potential extent to which the User Systems of either User may be

Compromised, or the potential adverse effect of any Compromise to the User Systems of either User, is greater than it would have been had those User Systems not employed Shared Resources.

G5.26 Where this Section applies, the requirement at Section G5.18(b)(iv) shall be read as a requirement to ensure that the User's Information Security Management System provides for security controls which are proportionate to the potential impact of a Compromise to each part of all User Systems of each User which employ the Shared Resources.

G5.27 Where this Section applies, a User which begins to employ Shared Resources as part of its User Systems:

(a) shall notify the Security Sub-Committee as soon as reasonably practicable after first doing so; and

(b) where those Shared Resources are provided by a third party, shall include in that notification:

(i) the name and contact details of that third party; and

(ii) a description of the services provided by the third party to the User in relation to its User Systems.

G5.28 Where this Section applies, and where a User is entitled to send Critical Service Requests to the DCC, the User shall notify the Security Sub-Committee of the total number of Smart Metering Systems comprising Devices in respect of which such Critical Service Requests are capable of being sent from its User Systems:

(a) as soon as reasonably practicable after it first begins to employ Shared Resources as part of its User Systems; and

(b) at intervals of six months thereafter.

G6 ANOMALY DETECTION THRESHOLDS: OBLIGATIONS ON THE DCC AND USERS

Threshold Anomaly Detection Procedures

G6.1 The "**Threshold Anomaly Detection Procedures**" shall be a SEC Subsidiary Document of that name which:

(a) shall describe the means by which:

(i) each User shall be able securely to notify the DCC of the Anomaly Detection Thresholds set by that User, and of any exceptions that are applicable to each such Anomaly Detection Threshold;

(ii) the DCC shall be able securely to notify each User when a communication relating to that User is quarantined by the DCC; and

(iii) each such User shall be able securely to notify the DCC whether it considers that a communication which has been quarantined should be deleted from the DCC Systems or processed by the DCC;

(b) shall determine the standard of security at which Users and the DCC must be able to notify each other in order for such notifications to be considered, for the purposes of paragraph (a), to have been given 'securely';

(c) may make provision relating to the setting by Users and the DCC of Anomaly Detection Thresholds, including the issue of guidance by the DCC in relation to the appropriate level at which Anomaly Detection Thresholds should be set by Users; and

(d) may make provision relating to the actions to be taken by Users and the DCC in cases in which an Anomaly Detection Threshold has been exceeded, including for communications to be quarantined and remedial action to be taken.

Anomaly Detection Thresholds: Obligations on Users

G6.2 Each User shall comply with any requirements of the Threshold Anomaly Detection Procedures which are applicable to it.

G6.3 Each User which is an Eligible User in relation to any one or more individual Services listed in the DCC User Interface Services Schedule:

(a) shall set Anomaly Detection Thresholds in respect of:

(i) the total number of Critical Commands relating to each such Service; and

(ii) the total number of Service Requests relating to each such Service in respect of which there are Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification; and

(iii) may, at its discretion, set other Anomaly Detection Thresholds.

G6.4 Where a User sets any Anomaly Detection Threshold in accordance with Section G6.3, it shall:

(a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of its User Systems;

(b) before doing so:

(i) take into account any guidance issued by the DCC as to the appropriate level of the Anomaly Detection Threshold; and

(ii) have regard in particular to the forecast number of Service Requests provided by the User to the DCC in accordance with Section H3.22 (Managing Demand for User Interface Services); and

(c) after doing so, notify the DCC of that Anomaly Detection Threshold.

Anomaly Detection Thresholds: Obligations on the DCC

G6.5 The DCC shall comply with any requirements of the Threshold Anomaly Detection Procedures which are applicable to it.

G6.6 The DCC:

(a) shall, for each individual Service listed in the DCC User Interface Services Schedule, set an Anomaly Detection Threshold in respect of :

(i) the total number of Critical Commands relating to that Service; and

(ii) the total number of Service Requests relating to that Service in respect of which there are Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification;

(b) shall set an Anomaly Detection Threshold in respect of a data value that has been agreed with the Security Sub-Committee within each type of Signed Pre-Command; and

(c) may, at its discretion, set other Anomaly Detection Thresholds.

G6.7 Where the DCC sets any Anomaly Detection Threshold in accordance with Section G6.6, it shall:

(a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems; and

(b) before doing so consult, and take into account the opinion of, the Security Sub-Committee as to the appropriate level of the Anomaly Detection Threshold.

G6.8 The DCC shall notify the Security Sub-Committee of:

(a) each Anomaly Detection Threshold that it sets; and

(b) each Anomaly Detection Threshold that is set by a User and notified to the DCC in accordance with Section G6.4(c).

G6.9 Where the DCC is consulted by a User in relation to an Anomaly Detection Threshold which that User proposes to set, the DCC shall:

(a) provide to the User its opinion as to the appropriate level of that Anomaly Detection Threshold; and

(b) in doing so, have regard to the need to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the User Systems of that User.

Anomaly Detection Thresholds: Obligations on the DCC and Users

G6.10 The DCC and each User shall, in relation to each Anomaly Detection Threshold that it sets:

(a) keep the Anomaly Detection Threshold under review, having regard to the need to ensure that it continues to function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System and/or User Systems (as the case may be);

(b) for this purpose have regard to any opinion provided to it by the Security Sub-Committee from time to time as to the appropriate level of the Anomaly Detection Threshold; and

(c) where the level of that Anomaly Detection Threshold is no longer appropriate, set a new Anomaly Detection Threshold in accordance with the relevant provisions of this Section G6.

G7 SECURITY SUB-COMMITTEE

Establishment of the Security Sub-Committee

G7.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section G7, to be known as the "**Security Sub-Committee**".

G7.2 Save as expressly set out in this Section G7, the Security Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Membership of the Security Sub-Committee

G7.3 The Security Sub-Committee shall be composed of the following persons (each a "**Security Sub-Committee Member**"):

(a) the Security Sub-Committee Chair (as further described in Section G7.5);

(b) eight Security Sub-Committee (Supplier) Members (as further described in Section G7.6);

(c) two Security Sub-Committee (Network) Members (as further described in Section G7.8);

(d) one Security Sub-Committee (Other User) Member (as further described in Section G7.10);

(e) one representative of the DCC (as further described in Section G7.12).

G7.4 Each Security Sub-Committee Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as a Security Sub-Committee Member at the same time.

G7.5 The "**Security Sub-Committee Chair**" shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the Security Sub-Committee Chair is appointed for a [three-year] term (following which he or she can apply to be re-appointed);

(c) the Security Sub-Committee Chair is remunerated at a reasonable rate;

(d) the Security Sub-Committee Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members); and

(e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

G7.6 Each of the eight "**Security Sub-Committee (Supplier) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire [two] years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Supplier) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.7 Each of the eight Security Sub-Committee (Supplier) Members shall be appointed in accordance with a process:

(a) by which six Security Sub-Committee (Supplier) Members will be elected by Large Supplier Parties, and two Security Sub-Committee (Supplier) Members will be elected by Small Supplier Parties; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.8 Each of the two "**Security Sub-Committee (Network) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire [two] years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Network) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.9 Each of the two Security Sub-Committee (Network) Members shall be appointed in accordance with a process:

(a) by which one Security Sub-Committee (Network) Member will be elected by the Electricity Network Parties and one Security Sub-Committee (Network) Member will be elected by the Gas Network Parties;

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the

corresponding provisions set out in or applied pursuant to this Section G7).

G7.10 The "**Security Sub-Committee (Other User) Member**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section G7 into this Code):

(a) be appointed in accordance with Section G7.11, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire two years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "Security Sub-Committee (Other User) Member", references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

G7.11 The Security Sub-Committee (Other User) Member shall be appointed in accordance with a process:

(a) by which he or she is elected by those Other SEC Parties which are Other Users; and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", references to "Panel Members" were to "Security Sub-Committee Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section G7).

G7.12 The DCC may nominate one person to be a Security Sub-Committee Member by notice to the Secretariat from time to time. The DCC may replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject

to compliance by the relevant person with Section C6.9 (Member Confirmation).

Proceedings of the Security-Sub Committee

G7.13 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section G7.14:

(a) a representative of the Secretary of State shall be:

(i) invited to attend each and every Security Sub-Committee meeting;

(ii) entitled to speak at such Security Sub-Committee meetings without the permission of the Security Sub-Committee Chair; and

(iii) provided with copies of all the agenda and supporting papers available to Security Sub-Committee Members in respect of such meetings;

(b) the Security Sub-Committee Chair shall invite to attend Security Sub-Committee meetings any persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters.

G7.14 Subject to Section G7.13, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the Security Sub-Committee, for which purpose that Section shall be read as if references to "Panel" were to "Security Sub-Committee", references to "Panel Chair" were to "Security Sub-Committee Chair", and references to "Panel Members" were to "Security Sub-Committee Members".

Duties and Powers of the Security Sub-Committee

G7.15 The Security Sub-Committee:

(a) shall perform the duties and may exercise the powers set out in Sections G7.16 to G7.20; and

(b) shall perform such other duties and may exercise such other powers as may be expressly ascribed to the Security Sub-Committee elsewhere in this Code.

Document Development and Maintenance

G7.16 The Security Sub-Committee shall:

(a) develop and maintain a document, to be known as the "**Security Controls Framework**", which shall:

(i) set out the appropriate User Security Assessment Methodology to be applied to different categories of security assurance assessment carried out in accordance with Section G8 (User Security Assurance); and

(ii) be designed to ensure that such security assurance assessments are proportionate, consistent in their treatment of equivalent Users and equivalent User Roles, and achieve appropriate levels of security assurance in respect of different Users and different User Roles;

(b) carry out reviews of the Security Risk Assessment:

(i) at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System; and

(ii) in any event promptly if the Security Sub-Committee considers there to be any material change in the level of security risk;

(c) maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;

(d) maintain the End-to-End Security Architecture to ensure that it is up to date; and

(e) develop and maintain a document to be known as the "**Risk Treatment Plan**", which shall identify the residual security risks which in the opinion of the Security Sub-Committee remain unmitigated taking into account the security controls that are in place.

Security Assurance

G7.17 The Security Sub-Committee shall:

(a) periodically, and in any event at least once each year, review the Security Obligations and Assurance Arrangements in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;

(b) exercise such functions as are allocated to it under, and comply with the applicable requirements of Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance);

(c) provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of the Security Obligations and Assurance Arrangements;

(d) keep under review the CESG CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;

(e) to the extent to which it considers it appropriate, in relation to any User (or, during the first User Entry Process, Party) which has produced a User Security Assessment Response that sets out any steps that the User proposes to take in accordance with Section G8.24(b):

(i) liaise with that User (or Party) as to the nature and timetable of such steps;

(ii) either accept the proposal to take those steps within that timetable or seek to agree with that User (or Party) such alternative steps or timetable as the Security Sub-Committee may consider appropriate; and

(iii) take advice from the User Independent Security Assurance Service Provider; and

(iv) where the Security Sub-Committee considers it appropriate, request the User Independent Security Assurance Service Provider to carry out a Follow-up Security Assessment;

(f) provide advice to the Panel on the scope and output of the independent security assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;

(g) provide advice to the Panel on the scope and output of the SOC2 assessment of the DCC Total System; and

(h) provide advice to the Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance.

Monitoring and Advice

G7.18 The Security Sub-Committee shall:

(a) provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of security incidents and the management of vulnerabilities on their Systems;

(b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;

(c) provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Security Obligations and Assurance Arrangements;

(d) provide the Panel, the Change Board and any relevant Working Group with support and advice in relation to any Modification Proposal which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(e) advise the Authority of any modifications to the conditions of Energy Licences which it considers may be appropriate having regard to the residual security

risks identified from time to time in the Risk Treatment Plan;

(f) respond to any consultations on matters which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

(g) act in cooperation with, and send a representative to, the SMKI PMA, the Technical Architecture and Business Architecture Sub-Committee and any other Sub-Committee or Working Group which requests the support or attendance of the Security Sub-Committee; and

(h) provide such further support and advice to the Panel as it may request.

Modifications

G7.19 The Security Sub-Committee shall establish a process under which the Code Administrator monitors Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:

(a) are likely to affect the Security Obligations and Assurance Arrangements; or

(b) are likely to relate to other parts of the Code but may have a material effect on the security of the End-to-End Smart Metering System,

and the Code Administrator shall comply with such process.

G7.20 Notwithstanding Section D1.3 (Persons Entitled to Submit Modification Proposals):

(a) the Security Sub-Committee shall be entitled to submit Modification Proposals in respect of the Security Obligations and Assurance Arrangements where the Security Sub-Committee considers it appropriate to do so; and

(b) any Security Sub-Committee Member shall be entitled to submit Modification Proposals in respect of the Security Obligations and Assurance Arrangements where he or she considers it appropriate to do so (where the Security Sub-Committee has voted not to do so).

G7.21 Notwithstanding Section D6.3 (Establishment of a Working Group), and subject to the

provisions of Sections D6.5 and D6.6, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group.

G7.22 For the purposes of Section D7.1 (Modification Report):

(a) written representations in relation to the purpose and effect of a Modification Proposal may be made by:

(i) the Security Sub-Committee; and/or

(ii) any Security Sub-Committee Member (either alone or in addition to any representations made by other Security Sub-Committee Members and/or the Security Sub-Committee collectively); and

(b) notwithstanding Section D7.3 (Content of the Modification Report), the Code Administrator shall ensure that all such representations, and a summary of any evidence provided in support of them, are set out in the Modification Report prepared in respect of the relevant Modification Proposal.

G8 USER SECURITY ASSURANCE

Procurement of the User Independent Security Assurance Service Provider

G8.1 The Panel shall procure the provision of security assurance services:

(a) of the scope specified in Section G8.3;

(b) from a person who:

(i) is suitably qualified in accordance with Section G8.4;

(ii) is suitably independent in accordance with Section G8.7; and

(iii) satisfies the capacity requirement specified in Section G8.11,

and that person is referred to in this Section G8 as the "**User Independent Security Assurance Service Provider**".

G8.2 Except where the contrary is required by the provisions of Section X (Transition), the Panel may appoint more than one person to carry out the functions of the User Independent Security Assurance Service Provider.

Scope of Security Assurance Services

G8.3 The security assurance services specified in this Section G8.3 are services in accordance with which the User Independent Security Assurance Service Provider shall:

(a) carry out User Security Assessments at such times and in such manner as is provided for in this Section G8;

(b) produce User Security Assessment Reports in relation to Users that have been the subject of a User Security Assessment;

(c) receive and consider User Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;

(d) otherwise, at the request of, and to an extent determined by, the Security Sub-Committee, carry out an assessment of the compliance of any User with its

obligations under Sections G3 to G6 where:

(i) following either a User Security Self-Assessment or Verification User Security Assessment, any material increase in the security risk relating to that User has been identified; or

(ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;

(e) review the outcome of User Security Self-Assessments;

(f) at the request of the Security Sub-Committee, provide to it advice in relation to:

(i) the compliance of any User with its obligations under Sections G3 to G6; and

(ii) changes in security risks relating to the Systems, Data, functionality and processes of any User which fall within Section G5.14 (Information Security: Obligations on Users);

(g) at the request of the Panel, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(h) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and

(i) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section G8.

Suitably Qualified Service Provider

G8.4 The User Independent Security Assurance Service Provider shall be treated as suitably qualified in accordance with this Section G8.4 only if it satisfies:

(a) one or more of the requirements specified in Section G8.5; and

(b) the requirement specified in Section G8.6.

G8.5 The requirements specified in this Section G8.5 are that the User Independent Security Assurance Service Provider:

(a) is a CESG Tailored Assurance Service (CTAS) provider;

(b) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or

(c) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Panel substantially equivalent in status and effect to one or more of the arrangements described in paragraphs (a) and (b).

G8.6 The requirement specified in this Section G8.6 is that the User Independent Security Assurance Service Provider:

(a) employs consultants who are members of the CESG Listed Adviser Scheme (CLAS) at the 'Lead' or 'Senior Practitioner' level in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and

(b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Independence Requirement

G8.7 The User Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G8.7 only if it satisfies:

(a) the requirements specified in Section G8.9; and

(b) the requirement specified in Section G8.10.

G8.8 For the purposes of Sections G8.9 and G8.10:

(a) a "**Relevant Party**" means any Party in respect of which the User Independent Security Assurance Service Provider carries out functions under this Section G8; and

(b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as a User under Sections G3 to G6.

G8.9 The requirements specified in this Section G8.9 are that:

(a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the User Independent Security Assurance Service Provider;

(b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the User Independent Security Assurance Service Provider; and

(c) the User Independent Security Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the User Independent Security Assurance Service Provider where it acts in that capacity).

G8.10 The requirement specified in this Section G8.10 is that the User Independent Security Assurance Service Provider is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the User Independent Security Assurance Service Provider itself being a Relevant Service Provider to any Relevant Party).

Capacity Requirement

G8.11 The capacity requirement specified in this Section G8.11 is that the User Independent Security Assurance Service Provider must be capable of meeting the Panel's estimate of the demand for its security assurance services throughout the period in relation to which those services are being procured.

Compliance of the User Independent Security Assurance Service Provider

G8.12 The Panel shall be responsible for ensuring that the User Independent Security Assurance Service Provider carries out its functions in accordance with the provisions of this Section G8.

Users: Duty to Cooperate in Assessment

G8.13 Each User shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the User Independent Security Assurance Service Provider), for the purposes of facilitating an assessment of that User's compliance with its obligations under Sections G3 to G6.

G8.14 For the purposes of Section G8.13, a User shall provide the Security Sub-Committee (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of that User as are used for, and such persons engaged by that User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G3 to G6; and

(ii) such cooperation as may reasonably be requested by the Independent Security Assessment Services Provider for the purposes of carrying out

any security assurance assessment in accordance with this Section G8.

Categories of Security Assurance Assessment

G8.15 For the purposes of this Section G8, there shall be the following four categories of security assurance assessment:

(a) a Full User Security Assessment (as further described in Section G8.16);

(b) a Verification User Security Assessment (as further described in Section G8.17);

(c) a User Security Self-Assessment (as further described in Section G8.18); and

(d) a Follow-up Security Assessment (as further described in Section G8.19).

G8.16 A "**Full User Security Assessment**" shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify the extent to which that User is compliant with each of its obligations under Sections G3 to G6 in each of its User Roles.

G8.17 A "**Verification User Security Assessment**" shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User.

G8.18 A "**User Security Self-Assessment**" shall be an assessment carried out by a User, the outcome of which is reviewed by the User Independent Security Assurance Service Provider, to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a User Security Assessment was carried out in respect of that User.

G8.19 A "**Follow-up Security Assessment**" shall be an assessment carried out by the User Independent Security Assurance Service Provider, following a User Security

Assessment, in accordance with the provisions of Section G8.28.

G8.20 For the purposes of Sections G8.17 and G8.18, a Verification Security Assessment and User Security Self-Assessment shall each be assessments carried out in respect of a User having regard in particular to:

(a) any changes made to any System, Data, functionality or process falling within the scope of Section G5.14 (Information Security: Obligations on Users);

(b) where the User is a Supplier Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Responsible Supplier; and

(c) where the User is a Network Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Electricity Distributor or the Gas Transporter.

User Security Assessments: General Procedure

User Security Assessment Methodology

G8.21 Each User Security Assessment carried out by the User Independent Security Assurance Service Provider shall be carried out in accordance with the User Security Assessment Methodology applicable to the relevant category of assessment.

The User Security Assessment Report

G8.22 Following the completion of a User Security Assessment, the User Independent Security Assurance Service Provider shall, in discussion with the User to which the assessment relates, produce a written report (a "**User Security Assessment Report**") which shall:

(a) set out the findings of the User Independent Security Assurance Service Provider on all the matters within the scope of the User Security Assessment;

(b) in the case of a Full User Security Assessment:

(i) specify any instances of actual or potential non-compliance of the User with its obligations under Sections G3 to G6 which have been identified

by the User Independent Security Assurance Service Provider; and

(ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified; and

(c) in the case of a Verification User Security Assessment:

(i) specify any material increase in the security risk relating to that User which the User Independent Security Assurance Service Provider has identified since the last occasion on which a Full User Security Assessment was carried out in respect of that User; and

(ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes the increase in security risk which it has identified.

G8.23 The User Independent Security Assurance Service Provider shall submit a copy of each User Security Assessment Report to the Security Sub-Committee and to the User to which that report relates.

The User Security Assessment Response

G8.24 Following the receipt by any User of a User Security Assessment Report which relates to it, the User shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

(a) produce a written response to that report (a "**User Security Assessment Response**") which addresses the findings set out in the report; and

(b) submit a copy of that response to the Security Sub-Committee and the User Independent Security Assurance Service Provider.

G8.25 Where a User Security Assessment Report:

(a) following a Full User Security Assessment, specifies any instance of actual or potential non-compliance of a User with its obligations under Sections G3 to

G6; or

(b) following a Verification User Security Assessment, specifies any material increase in the security risk relating to a User since the last occasion on which a Full User Security Assessment was carried out in respect of that User,

the User shall ensure that its User Security Assessment Response includes the matters referred to in Section G8.26.

G8.26 The matters referred to in this Section are that the User Security Assessment Response:

(a) indicates whether the User accepts the relevant findings of the User Independent Security Assurance Service Provider and, where it does not, explains why this is the case;

(b) sets out any steps that the User has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the User Security Assessment Report; and

(c) identifies a timetable within which the User proposes to take any such steps that have not already been taken.

G8.27 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), the Security Sub-Committee (having considered the advice of the User Independent Security Assurance Service Provider) shall review that response and either:

(a) notify the User that it accepts that the steps that the User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the User Security Assessment Report; or

(b) seek to agree with the User such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G8.28 Where a User Security Assessment Response sets out any steps that the User proposes

to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User shall:

(a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) report to the Security Sub-Committee on:

(i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;

(ii) the completion of those steps in accordance with the timetable; and

(iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G8.29 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User Independent Security Assurance Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the relevant User to:

(a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and

(b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

User Security Assessments: Further Provisions

G8.30 The User Independent Security Assurance Service Provider:

(a) may in its discretion, and shall where directed to do so by the Security Sub-Committee:

(i) in relation to a User which acts in more than one User Role, determine that a single User Security Assessment may be carried out in relation to that User in respect of any two or more such User Roles; and

(ii) in carrying out any User Security Assessment, take into account any relevant security accreditation or certification held by the relevant User; and

(b) shall, where any Shared Resources form part of the User Systems of more than one User, have regard to information obtained in relation to such Shared Resources in the User Security Assessment of one such User when carrying out a User Security Assessment of any other such User.

Initial Full User Security Assessment: User Entry Process

G8.31 Sections G8.33 to G8.39 set out the applicable security requirements referred to in Section H1.10(c) (User Entry Process Requirements).

G8.32 For the purposes of Sections G8.33 to G8.39, any reference in Sections G3 to G6 or the preceding provisions of this Section G8 to a 'User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for any User Role.

Initial Full User Security Assessment

G8.33 For the purpose of completing the User Entry Process for a User Role, a Party wishing to act as a User in that User Role shall be subject to a Full User Security Assessment in respect of the User Role.

Panel: Setting the Assurance Status

G8.34 Following the completion of that initial Full User Security Assessment, the Security Sub-Committee shall ensure that copies of both the User Security Assessment Report and User Security Assessment Response are provided to the Panel.

G8.35 Following the receipt by it of the User Security Assessment Report and User Security Assessment Response, the Panel shall promptly consider both documents and (having regard to any advice of the Security Sub-Committee) set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections G3 to G6 in the relevant User Role, in accordance with Section G8.36.

G8.36 The Panel shall set the assurance status of the Party as one of the following:

(a) approved;

(b) approved, subject to the Party:

(i) taking such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or

(ii) both taking such steps and being subject to a Follow-up Security Assessment by such date as the Panel may specify,

(c) provisionally approved, subject to:

(i) the Party having first taking such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b) and been subject to a Follow-up Security Assessment; and

(ii) the Panel having determined that it is satisfied, on the evidence of the Follow-up Security Assessment, that such steps have been taken; or

(d) deferred, subject to:

(i) the Party amending its User Security Assessment Response to address any issues identified by the Panel as being, in the opinion of the Panel, not adequately addressed in that response as submitted to the Security Sub-Committee; and

(ii) the Panel reconsidering the assurance status in accordance with Section G8.35 in the light of such amendments to the User Security Assessment Response.

Approval

G8.37 For the purposes of Sections H1.10(c) and H1.11 (User Entry Process Requirements):

(a) a Party shall be considered to have successfully demonstrated that it meets the applicable security requirements of this Section G8 when:

(i) the Panel has set its assurance status to 'approved' in accordance with either Section G8.36(a) or (b); or

(ii) the Panel has set its assurance status to 'provisionally approved' in accordance with Section G8.36(c) and the requirements specified in that Section have been met; and

(b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

G8.38 Where the Panel has set the assurance status of a Party to 'approved' subject to one of the requirements specified in Section G8.36(b), the Party shall take the steps to which that approval is subject.

Disagreement with Panel Decisions

G8.39 Where a Party disagrees with any decision made by the Panel in relation to it under Section G8.36, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Security Assurance Assessments: Post-User Entry Process

G8.40 Following its initial Full User Security Assessment for the purposes of the User Entry Process, a User shall be subject to annual security assurance assessments in respect of each of its User Roles in accordance with the provisions of Sections G8.41 to G8.46.

Supplier Parties

G8.41 Where a User is a Supplier Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 250,000, it shall be subject to a Full User Security Assessment in each year after the year of its initial Full User Security Assessment.

G8.42 Where a User is a Supplier Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier is equal to or less than 250,000, it shall be subject:

(a) in the first year after the year of its initial Full User Security Assessment, to a Verification Security Assessment;

(b) in the immediately following year, to a User Security Self-Assessment;

(c) in the next following year, to a Full User Security Assessment; and

(d) in each year thereafter, to a category of security assurance assessment which repeats the same annual sequence as that of paragraphs (a) to (c).

G8.43 In assessing for the purposes of Sections G8.41 and G8.42 the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Responsible Supplier, that number shall, where any Shared Resources form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Responsible Supplier.

Network Parties

G8.44 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter exceeds 250,000, it shall be subject:

(a) in the first year after the year of its initial Full User Security Assessment, to a Verification Security Assessment;

(b) in the immediately following year, to a Verification Security Assessment;

(c) in the next following year, to a Full User Security Assessment; and

(d) in each year thereafter, to a category of security assurance assessment which repeats the same annual sequence as that of paragraphs (a) to (c).

G8.45 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter is equal to or less than 250,000, it shall be subject:

(a) in the first year after the year of its initial Full User Security Assessment, to a Verification Security Assessment;

(b) in the immediately following year, to a User Security Self-Assessment;

(c) in the next following year, to a Full User Security Assessment; and

(d) in each year thereafter, to a category of security assurance assessment which repeats the same annual sequence as that of paragraphs (a) to (c).

G8.46 In assessing for the purposes of Sections G8.44 and G8.45 the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Electricity Distributor and/or the Gas Transporter, that number shall, where any Shared Resources form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Electricity Distributor and/or the Gas Transporter.

Other Users

G8.47 Where a User is neither a Supplier Party nor a Network Party, it shall be subject:

(a) in the first year after the year of its initial Full User Security Assessment, to a User Security Self-Assessment;

(b) in the immediately following year, to a User Security Self-Assessment;

(c) in the next following year, to a Full User Security Assessment; and

(d) in each year thereafter, to a category of security assurance assessment which repeats the same annual sequence as that of paragraphs (a) to (c).

Interpretation

G8.48 Section G8.49 applies where:

(a) pursuant to Sections G8.41 to G8.43, it is necessary to determine, in relation to any Supplier Party, the number of Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier; or

(b) pursuant to Sections G8.44 to G8.46, it is necessary to determine, in relation to any Network Party, the number of Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter.

G8.49 Where this Section applies:

(a) the determination referred to in Section G8.48 shall be made at the time at which the nature of each annual security assurance assessment for the relevant User falls to be ascertained; and

(b) the DCC shall provide all reasonable assistance that may be requested by that User or the Security Sub-Committee for the purposes of making that determination.

User Security Self-Assessment

G8.50 Where, in accordance with the requirements of this Section G8, a User is subject to a User Security Self-Assessment in any year, that User shall:

(a) carry out the User Security Self-Assessment during that year;

(b) do so in accordance with the User Security Assessment Methodology that is applicable to User Security Self-Assessments; and

(c) ensure that the outcome of the User Security Self-Assessment is documented and is submitted to the User Independent Security Assurance Service Provider for review by no later than the date which is 13 months after the date of the commencement of the previous User Security Assessment or (if more recent) User Security Self-Assessment.

Users: Obligation to Pay Explicit Charges

G8.51 Each User shall pay to the DCC all applicable Charges in respect of:

(a) all User Security Assessments and Follow-up Security Assessments carried out in relation to it by the User Independent Security Assurance Service Provider;

(b) the production by the User Independent Security Assurance Service Provider of any User Security Assessment Reports following such assessments; and

(c) all related activities of the User Independent Security Assurance Service Provider in respect of that User in accordance with this Section G8.

G8.52 Expenditure incurred in relation to Users in respect of the matters described in Section G8.51 shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

G8.53 For the purposes of Section G8.51 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

(a) the expenditure incurred in respect of the matters described in Section G8.51 that is attributable to individual Users, in order to facilitate Explicit Charges designed to pass-through the expenditure to such Users pursuant to Section K7 (Determining Explicit Charges); and

(b) any expenditure incurred in respect of the matters described in Section G8.51 which cannot reasonably be attributed to an individual User.

Events of Default

G8.54 In relation to an Event of Default which consists of a material breach by a User of any of its obligations under Sections G3 to G6, the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G8.55 to G8.60.

G8.55 Where in accordance with Section M8.2 the Panel receives notification that a User is in material breach of any requirements of Sections G3 to G6, it shall refer the matter to the Security Sub-Committee.

G8.56 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "Security Sub-Committee".

G8.57 Where the Security Sub-Committee has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a report from the User Independent Security Assurance Service Provider, following a User Security Assessment, concluding that a User is in actual or potential non-compliance with any of its obligations under Sections G3 to G6,

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any obligations under Sections G3 to G6 has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G8.58 Where the Panel determines that an Event of Default has occurred, it shall:

(a) notify the relevant User and any other Party it considers may have been affected by the Event of Default; and

(b) determine the appropriate steps to take in accordance with Section M8.4.

G8.59 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G8.60 Where the Panel determines that a User is required to give effect to a remedial action

plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

G9 DCC SECURITY ASSURANCE

The DCC Independent Security Assessment Arrangements

G9.1 The DCC shall establish, give effect to, maintain and comply with arrangements, to be known as the "**DCC Independent Security Assessment Arrangements**", which shall:

(a) have the purpose specified in Section G9.2; and

(b) make provision for the DCC to take the actions specified in Section G9.3.

G9.2 The purpose specified in this Section G9.2 shall be the purpose of procuring SOC2 assessments of:

(a) all security risk assessments undertaken by the DCC in relation to itself and any DCC Service Providers;

(b) the effectiveness and proportionality of the security controls that are in place in order to identify and mitigate security risks in relation to the DCC Total System; and

(c) the DCC's compliance with:

(i) the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;

(ii) the requirements of Sections G2 and G4 to G6;

(iii) such other requirements relating to the security of the DCC Total System as may be specified by the Panel (having considered the advice of the Security Sub-Committee) from time to time.

G9.3 The actions specified in this Section G9.3 shall be actions taken by the DCC to:

(a) procure the provision of security assurance services by the DCC Independent Security Assurance Service Provider (as further described in Section G9.4);

(b) ensure that the DCC Independent Security Assurance Service Provider carries out SOC2 assessments for the purpose specified in Section G9.2:

(i) annually;

(ii) on any material change to the DCC Total System; and

(iii) at any other time specified by the Panel;

(c) consult with the Panel, and obtain its approval, in respect of the scope of each such assessment before that assessment is carried out;

(d) procure that the DCC Independent Security Assurance Service Provider produces a DCC Security Assessment Report following each such assessment that has been carried out;

(e) ensure that the Panel and the Security Sub-Committee are provided with a copy of each such DCC Security Assessment Report;

(f) produce a DCC Security Assessment Response in relation to each such report; and

(g) provide to the Panel and the Security Sub-Committee a copy of each DCC Security Assessment Response and, as soon as reasonably practicable thereafter, a report on its implementation of any action plan that is set out in that DCC Security Assessment Response.

The DCC Independent Security Assurance Service Provider

G9.4 For the purposes of Section G9.3, the "**DCC Independent Security Assurance Service Provider**" shall be a person who is appointed by the DCC to provide security assurance services and who:

(a) is qualified to perform SOC2 assessments;

(b) has been approved by the Security Sub-Committee, following consultation with it by the DCC, as otherwise being suitably qualified to provide security assurance services for the purposes of this Section G9; and

(c) satisfies the independence requirement specified in Section G9.5.

G9.5 The independence requirement specified in this Section G9.5 is that the DCC Independent Security Assurance Service Provider must be independent of the DCC and of each DCC Service Provider from whom the DCC may acquire capability for any purpose related to its compliance with the obligations referred to at Section G9.2(c) (but excluding any provider of corporate assurance services to the DCC).

G9.6 For the purposes of Section G9.5, the DCC Independent Security Assurance Service Provider is to be treated as independent of the DCC (and of a relevant DCC Service Provider) only if:

(a) neither the DCC nor any of its subsidiaries (or such a DCC Service Provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assurance Service Provider;

(b) no director of the DCC (or of any such DCC Service Provider) is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assurance Service Provider;

(c) the DCC Independent Security Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC (or in any such DCC Service Provider); and

(d) the DCC Independent Security Assurance Service Provider is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has or may in future have with the DCC.

DCC Security Assessment Reports and Responses

G9.7 For the purposes of this Section G9:

(a) a "**DCC Security Assessment Report**" means a written report produced by the DCC Independent Security Service Provider following a SOC2 assessment

carried out by it for the purpose specified in Section G9.2, which:

(i) sets out the findings of the DCC Independent Security Assurance Service Provider on all the matters within the scope of that assessment;

(ii) specifies any instances of actual or potential non-compliance of the DCC with the obligations referred to at Section G9.2(c) which have been identified by the DCC Independent Security Assurance Service Provider; and

(iii) sets out the evidence which, in the opinion of the DCC Independent Security Assurance Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified; and

(b) a "**DCC Security Assessment Response**" means a written response to a DCC Security Assessment Report which is produced by the DCC, addresses the findings set out in the report and, where that report specifies any instances of actual or potential non-compliance of the DCC with the obligations referred to at Section G9.2(c):

(i) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assurance Service Provider and, where it does not, explains why this is the case;

(ii) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance specified in the DCC Security Assessment Report; and

(iii) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.

Events of Default

G9.8 In relation to an Event of Default which consists of a material breach by the DCC of any of the obligations referred to at Section G9.2(c), the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G9.9 to G9.15.

G9.9 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section G9.8, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any of the obligations referred to at Section G9.2(c) (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

G9.10 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any of the obligations referred to at Section G9.2(c), it shall refer the matter to the Security Sub-Committee.

G9.11 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "Security Sub-Committee".

G9.12 Where the Security Sub-Committee has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a DCC Security Assessment Report concluding that the DCC is in actual or potential non-compliance with any of the obligations referred to at Section G9.2(c),

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any of the obligations referred to at Section G9.2(c) has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G9.13 Where the Panel determines that an Event of Default has occurred, it shall:

(a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and

(b) determine the appropriate steps to take in accordance with Section M8.4.

G9.14 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G9.15 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

SECTION H: DCC SERVICES

H1 USER ENTRY PROCESS

Eligibility Generally

H1.1 Many of the Services described in this Section H are described as being available only to Users. A Party is not entitled to receive those Services until that Party has become a User by completing the User Entry Process.

H1.2 Only persons that are Parties are eligible to complete the User Entry Process and to become Users.

User Role Eligibility

H1.3 The Services provided over the DCC User Interface are available only to Users within certain User Roles. A Party wishing to act as a User in one or more User Roles must first complete the User Entry Process for that User Role.

User IDs

H1.4 When accessing Services a User must operate in a particular User Role using the applicable User ID.

H1.5 A Party wishing to act as a User in one or more User Roles shall propose to the DCC one or more identification numbers, issued to it by the Panel, to be used by that Party when acting in each such User Role. Each such identification number must be EUI-64 Compliant, and the same identification number cannot be used for more than one User Role, save that a Party may use the same identification number when acting in the User Roles of 'Import Supplier', 'Export Supplier' and 'Gas Supplier'.

H1.6 The DCC shall accept each identification number proposed by each Party in respect of each of its User Roles (and record such numbers as identifying, and use such numbers to identify, such Party in such User Role); provided that the DCC shall only accept the proposed number if it has been issued by the Panel, and if (at the time of the Party's proposal) the Party:

(a) holds for the User Role of 'Import Supplier' or 'Export Supplier', an Electricity Supply Licence;

(b) holds for the User Role of 'Gas Supplier', a Gas Supply Licence;

(c) holds for the User Role of 'Electricity Distributor', an Electricity Distribution Licence;

(d) holds for the User Role of 'Gas Transporter', a Gas Transportation Licence; and

(e) is for the User Role of 'Registered Supplier Agent', identified in the Registration Data as a Meter Operator or a Meter Asset Manager for at least one MPAN or MPRN.

H1.7 A Party may from time to time replace or withdraw its User ID for each of its User Roles on notice to the DCC; provided that any such replacement shall be subject to acceptance by the DCC in accordance with Section H1.6.

User Entry Guide

H1.8 The Code Administrator shall establish and publish on the Website a guide to the User Entry Process. Such guide shall:

(a) identify the persons that a Party is required to contact to commence the steps required pursuant to the User Entry Process for each User Role; and

(b) include a recommendation that each Party undertakes a privacy impact assessment in accordance with the Information Commissioner's guidance concerning the same (but there shall be no obligation under this Code to do so).

User Entry

H1.9 Where a Party wishing to become a User in a particular User Role commences the User Entry Process, it must notify the Code Administrator that it has done so (and in respect of which User Role).

User Entry Process Requirements

H1.10 The User Entry Process for each User Role requires that the Party has:

(a) received confirmation from the DCC of its acceptance of at least one User ID for the Party and that User Role in accordance with Section H1.6;

(b) successfully completed the User Entry Process Tests for that User Role in accordance with Section H14 (Testing Services);

(c) successfully demonstrated in accordance with the procedure set out in Section G8 (User Security Assurance) that the Party meets the applicable security requirements required by that Section;

(d) (in the case only of the User Role of Other User) successfully demonstrated in accordance with the procedure set out in Section I2 (Other User Privacy Audits) that the Party meets the applicable privacy requirements required by that Section; and

(e) provided the Credit Support or additional Credit Support (if any) that the DCC requires that Party to provide, to be calculated by the DCC in accordance with Section J3 (Credit Cover) as if that Party were a User for that User Role (which calculation will include the DCC's reasonable estimates of the Charges that are likely to be incurred by that Party in that User Role in the period until the first Invoice for that Party is due to be paid by that Party in that User Role).

H1.11 A Party will have successfully completed the User Entry Process for a particular User Role once the Code Administrator has received confirmation from the body responsible for each of the requirements set out in Section H1.10 that the Party has met each and every requirement set out in Section H1.10, and once the Code Administrator has confirmed the same to the Party.

H1.12 Once a Party has successfully completed the User Entry Process for a particular User Role, the Code Administrator shall confirm the same to the DCC and the Panel. A Party who has successfully completed the User Entry Processes in one User Role shall

not be considered to be a User in relation to any other User Role until it has completed the User Entry Processes in relation to such other User Role.

Disputes Regarding User Entry Process

H1.13 Where a Party wishes to raise a dispute in relation to its application to become a User, and to the extent that the dispute relates to:

(a) the matters described in Section H1.10(b), then the dispute shall be determined in accordance with the applicable dispute resolution procedure set out in Section H14 (Testing Services);

(b) the matters described in Section H1.10(c), then the dispute shall be determined in accordance with the dispute resolution procedure set out in Section G8 (User Security Assurance);

(c) the matters described in Section H1.10(d), then the dispute shall be determined in accordance with the dispute resolution procedure set out in Section I2 (Other User Privacy Audits);

(d) the matters described in Section H1.10(e), then the dispute shall be determined in accordance with Section J3.15 (Disputes); or

(e) any matters other than those referred to above, then the dispute may be referred to the Panel for determination.

H1.14 Where a Party disagrees with any decision of the Panel made pursuant to Section H1.13(e), then that Party may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

Ceasing to be a User in a User Role

H1.15 Where a User wishes to cease acting as a User in a User Role, the User shall notify the Code Administrator in writing of the date from which the User wishes to cease acting as a User in that User Role.

H1.16 Where a User notifies the Code Administrator in accordance with Section H1.15, the User shall cease to be a User in the specified User Role with effect from the date specified in such notification.

H1.17 The Code Administrator shall, as soon as reasonably practicable after receipt of a notification from a User in accordance with Section H1.15, notify the Panel and the DCC of the date from which that User will cease to be a User in the specified User Role.

H1.18 Following any notification received from the Code Administrator under Section H1.17 in respect of a User and a User Role, the DCC shall cease to treat that User as a User in that User Role; provided that the DCC shall be allowed up to 24 hours from receipt of such notification to update the DCC Systems.

H2 REGISTERED SUPPLIER AGENTS

Rights and Obligations of Registered Supplier Agents

H2.1 Registered Supplier Agents are Parties to this Code in their own right, and as such have rights and obligations as Other SEC Parties or as Users acting in the User Role of Registered Supplier Agent.

Responsibility for Registered Supplier Agents

H2.2 It is acknowledged that the following Services (as described in the DCC User Interface Services Schedule) are only available to Users acting in the User Role of Registered Supplier Agent by virtue of their appointment by the Responsible Supplier as a Meter Operator or Meter Asset Manager in respect of the relevant MPAN or MPRN:

(a) Read Device Configuration;

(b) Read Event or Security Log;

(c) Read Supply Status; and

(d) Read Firmware Version.

H2.3 Without prejudice to the rights and obligations of each Registered Supplier Agent (as described in Section H2.1), the Supplier Party described in Section H2.4 shall ensure that each Registered Supplier Agent that sends Service Requests for the Services described in Section H2.2 shall only do so for the purposes of providing services to that Supplier Party in a manner consistent with that Supplier Party's Energy Supply Licence.

H2.4 The Supplier Party referred to in Section H2.3 is, in respect of a Service relating to a Smart Metering System or Device, the Responsible Supplier for that Smart Metering System or Device.

H2.5 Nothing in this Code obliges Supplier Parties to contract with Meter Operators and/or

Meter Asset Managers in order to procure from the Meter Operator and/or Meter Asset Manager services that result in the need for the Meter Operator and/or Meter Asset Manager to send Service Requests.

H2.6 Each Supplier Party shall be responsible for controlling the ability of the Registered Supplier Agent to send the Service Requests referred to in Section H2.2 in circumstances where that Supplier Party would be liable under Section H2.3.

H3 DCC USER INTERFACE

Obligation to Maintain DCC User Interfaces

H3.1 The DCC shall maintain the DCC User Interface in accordance with the DCC User Interface Specification, and make it available via DCC Gateway Connections to Users to send and receive communications in accordance with the DCC User Interface Specification and the DCC User Interface Code of Connection.

H3.2 The DCC shall ensure that the DCC User Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

Communications to be sent via DCC User Interface

H3.3 The DCC and each User shall use the DCC User Interface for the following communications:

(a) Service Requests from a User to the DCC;

(b) Signed Pre-Commands from a User to the DCC;

(c) Acknowledgements from the DCC to a User;

(d) Pre-Commands from the DCC to a User;

(e) Service Responses from the DCC to a User;

(f) Device Alerts and DCC Alerts from the DCC to a User;

(g) Commands from the DCC to the User pursuant to the Local Command Services; or

(h) any other communications expressly required in this Code to be sent via the DCC User Interface.

H3.4 The communications required to be sent via the DCC User Interface under Section H3.3 shall only be validly sent for the purposes of this Code if sent in accordance with this Section H3, Section H4 (Processing Service Requests) and the DCC User

Interface Specification.

H3.5 No Party may use the DCC User Interface for any purpose other than to meet the requirements of Section H3.3. Only the DCC and Users may use the DCC User Interface.

Eligibility for Services Over the DCC User Interface

H3.6 A User shall not send a Service Request in respect of a Smart Metering System (or a Device forming, or to form, part of a Smart Metering System) unless it is an Eligible User for that Service and Smart Metering System (save that a User may send a Service Request in circumstances where it is not an Eligible User in order to rectify errors, as further described in the Service Request Processing Document).

H3.7 Whether or not a User is an Eligible User for the following Services is determined as follows:

(a) for Enrolment Services, Core Communication Services and Local Command Services, the entitlement is described in Section H3.8; or

(b) for Elective Communication Services, the entitlement is described in the relevant Bilateral Agreement.

H3.8 Subject to Sections H3.9 and H3.10, the following Users are entitled to receive the following Services in respect of a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System):

(a) the Import Supplier for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the 'Import Supplier';

(b) the Export Supplier for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the 'Export Supplier';

(c) the Gas Supplier for that Smart Metering System is entitled to those Services

described in the DCC User Interface Services Schedule as being available to the 'Gas Supplier';

(d) the Electricity Distributor for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the 'Electricity Distributor';

(e) the Gas Transporter for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the 'Gas Transporter';

(f) the Registered Supplier Agent for that Smart Metering System is entitled to those Services described in the DCC User Interface Services Schedule as being available to the 'Registered Supplier Agent';

(g) any User acting in the User Role of Other User is entitled to those Services described in the DCC User Interface Services Schedule as being available to an 'Other User'; and

(h) in respect of certain Services (where specified in the DCC User Interface Services Schedule) and where an electricity Smart Metering System and a gas Smart Metering System share a Communications Hub Function, the Import Supplier is entitled to those Services in respect of the gas Smart Metering System.

H3.9 Subject to Section H3.10, a User's eligibility for a Service in respect of a Smart Metering System (or a Device forming, or to form, part of that Smart Metering System) is also dependent upon the status of that Smart Metering System (or such a Device), such that:

(a) the Responsible Supplier may send Service Requests in respect of Devices that have an SMI Status of 'pending', 'whitelisted', 'installed not commissioned', 'commissioned', or 'suspended';

(b) Users that are not the Responsible Supplier may only send Service Requests in

respect of Devices that have an SMI Status of 'installed not commissioned' or 'commissioned'; and

(c) Communication Services are not available in respect of a Smart Metering System until it has been Enrolled.

H3.10 Certain Services are available on the basis of Eligible User Role (rather than a User's status as an Eligible User in respect of a particular Smart Metering System or Device). In respect of these Services, references in the DCC User Interface Services Schedule to 'Electricity Import Supplier', 'Electricity Export Supplier', 'Gas Import Supplier', 'Electricity Network Operator', 'Gas Network Operator', 'Registered Supplier Agent' and 'Other Users' are to the corresponding User Roles. The Services in question are those described in the DCC User Interface Services Schedule as:

(a) 'Request WAN Matrix';

(b) 'Device Pre-notifications';

(c) 'Read Inventory';

(d) 'Communications Hub Status Update - Install Success';

(e) 'Communications Hub Status Update - Install No SM WAN';

(f) 'Communications Hub Status Update - Fault Return'; and

(g) 'Communications Hub Status Update - No Fault Return'.

Categories of Service

H3.11 Enrolment Services, Local Command Services and Core Communication Services fall into the following categories (and corresponding categories may be established in respect of Elective Communication Services under Bilateral Agreements):

(a) Services identified in the DCC User Interface Services Schedule to be available as 'on-demand' services, and which a User requests on such basis ("On-Demand Services");

(b) Services identified in the DCC User Interface Services Schedule to be available as 'future-dated' services, and which a User requests on such basis specifying the relevant time and date for execution ("Future-Dated Services"); and

(c) Services identified in the DCC User Interface Services Schedule to be available as 'scheduled' services, and which a User requests on such basis specifying the initial time and date for execution as well as the frequency at which execution is to recur ("Scheduled Services").

H3.12 The DCC shall only accept a Service Request for a Future-Dated Service or a Scheduled Service that has an execution date that is later than the time on the date at which the Service Request is received by the DCC. No User may request a Future-Dated Service that has an execution date of more than 30 days after the date on which the Service Request is sent to the DCC.

Sequenced Services

H3.13 An On-Demand Service or a Future-Dated Service may also be requested on the basis that it is only to be provided following the successful execution of a specified Service Request ("**Sequenced Services**").

Target Response Times

H3.14 The DCC shall undertake the following activities within the following time periods (each such time period being, in respect of each such activity, the "**Target Response Time**" for that activity):

(a) Transforming Critical Service Requests into Pre-Commands and sending to the relevant User, within 3 seconds from receipt of the Service Request;

(b) sending a User a Service Response in respect of a Non-Critical Service Request for an On-Demand Service that is not a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from receipt of the Service Request from the User;

(c) sending a User a Service Response in respect of a Critical Service Request for

an On-Demand Service that is not a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from receipt of the Signed Pre-Command from the User;

(d) sending a User a Service Response in respect of a Service Request for an On-Demand Service that is a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from the receipt by the DCC of the Service Response for the Service Request upon which the Sequenced Service is dependent;

(e) sending a User a Service Response in respect of a Service Request for a Future-Dated Service that is not a Sequenced Service or for a Scheduled Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from the time and date for execution specified in the Service Request;

(f) sending a User a Service Response in respect of a Service Request for a Future-Dated Service that is a Sequenced Service, within the applicable time period set out in the DCC User Interface Services Schedule measured from the receipt by the DCC of the Service Response for the Service Request upon which the Sequenced Service is dependent;

(g) (except for the Alerts referred to in (h) below) sending a User an Alert, within 60 seconds measured from the Alert being communicated to (Device Alerts) or generated by (Non-Device Alerts) the Communications Hub Function; or

(h) for the Services Request 'Update Device Configuration (Billing Calendar)', in addition to the above response times applicable to the Service Response confirming the configuration, periodic Alerts will be generated as a result of such configuration, for which the response time for sending the Alert to the User shall be within 24 hours from the relevant data having been communicated to the Communications Hub Function.

H3.15 For the purposes of Section H3.14:

(a) the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the DCC User Interface Specification;

(b) any time during which an anomalous communication is quarantined by the DCC in accordance with Section H4 (Processing Service Requests) shall be disregarded for the purpose of measuring Response Times; and

(c) the time taken by the Communications Hub Function in communicating with the other Devices forming part of a Smart Metering System shall be disregarded.

Inherent Restrictions Linked to Technical Specifications

H3.16 The Services set out in the DCC User Interface Services Schedule are available only insofar as the minimum functionality of Devices as described in the Technical Specifications (or, to the extent required to support that minimum functionality, the GB Companion Specification) allows for such Services. Any Services required in respect of additional functionality of Devices should be requested as Elective Communication Services. This Section H3.16 does not apply in respect of Services to which Non-Device Service Requests apply.

Change of Tenancy

H3.17 As soon as reasonably practicable after a Responsible Supplier for an Enrolled Smart Metering System relating to a premises becomes aware of a change of occupancy at that premises, that Responsible Supplier shall send a 'Restrict Access for Change of Tenancy' Service Request to the DCC in relation to the Smart Meter and any Gas Proxy Function forming part of that Smart Metering System (except where the out-going Energy Consumer has indicated that they wish historic information on the Smart Metering System to remain available to be viewed).

Cancellation of Future-Dated and Scheduled Services

H3.18 As soon as reasonably practicable after receipt by the DCC of a Service Response from a Smart Metering System in respect of a 'Restrict Access for Change of Tenancy' Service Request, the DCC shall cancel any and all Service Requests for

Future-Dated Services or Scheduled Services in respect of any Device forming part of that Smart Metering System for which the Command has not yet been sent and which are being processed on behalf of an Other User (and shall notify the relevant User of such cancellation via the DCC User Interface).

H3.19 The DCC shall cancel any and all Service Requests for Scheduled Services due to be undertaken in respect of a Device forming part of a Smart Metering System after the Withdrawal of that Smart Metering System (and shall notify the relevant User of such cancellation via the DCC User Interface).

H3.20 The DCC shall cancel any and all Service Requests for Future-Dated Services or Scheduled Services for which the Command has not yet been sent and which are due to be undertaken in respect of a Device after the Decommissioning or Suspension of that Device (and shall notify the relevant User of such cancellation via the DCC User Interface).

H3.21 [Not Used]

Managing Demand for DCC User Interface Services

H3.22 By the 15th Working Day of the months of January, April, July and October, each User shall provide the DCC with a forecast of the number of Service Requests that the User will send in each of the 8 months following the end of the month in which such forecast is provided. Such forecast shall contain a breakdown of the total number of Service Requests by reference to each Service listed in the DCC User Interface Services Schedule and the category of Service (i.e. Future Dated, On Demand or Scheduled).

H3.23 The DCC shall monitor and record the aggregate number of Service Requests sent by each User in total, and also the aggregate number of Service Requests sent by each User in respect of each Service listed in the DCC User Interface Services Schedule.

H3.24 By no later than the 10th Working Day following the end of each month, the DCC shall provide:

(a) each User with a report that sets out the number of Service Requests sent by that User during that month (in total and broken down by reference to each Service listed in the DCC User Interface Services Schedule), and comparing the actual numbers sent against the numbers most recently forecast for the applicable month;

(b) each User with a report setting out the current value (calculated at the end of the previous month) for every Monthly Service Metric for that User and a comparison of the current value against the relevant Monthly Service Threshold; and

(c) a report to the Panel that sets out:

(i) the aggregate number of Service Requests sent by all Users collectively during that month (in total and broken down by reference to each Service listed in the DCC User Interface Services Schedule), and comparing the actual numbers for that month sent against the numbers most recently forecast for the applicable month;

(ii) where the number of Service Requests sent by any User during that month is less than or equal to 90% or greater than or equal to 110% of the User's most recent monthly forecast for the applicable month, the identity of each such User and the number of Service Requests sent by each such User (in total and broken down by reference to each Service listed in the DCC User Interface Services Schedule); and

(iii) where the measured value of any Monthly Service Metric for any User and that month is greater than or equal to 110% of Monthly Service Threshold, the identity of that User and the values of such Monthly Service Metrics during that month.

H3.25 The Panel shall publish the reports provided to it pursuant to Section H3.24(c) on the Website. The Panel may decide not to publish one or more parts of a report concerning under-forecasting or over-forecasting as referred to in Section H3.24(c)(ii) where the

Panel considers that the under-forecasting or over-forecasting was reasonable in the circumstances (including where it arose as a result of matters beyond the User's reasonable control).

H3.26 The DCC shall, on or around each anniversary of the date on which it first started providing Services over the DCC User Interface, review (and report to the Panel on) each Monthly Service Metric and associated Monthly Service Threshold to establish whether they are still an appropriate mechanism to illustrate User behaviour that may utilise a significant element of the capacity requirements of the Services.

H3.27 The DCC shall, as soon as is reasonably practicable, submit a Modification Proposal containing rules that it considers appropriate to enable the prioritisation by the DCC of Service Requests and Service Responses across the DCC User Interface and the prioritisation by the DCC of Commands to be sent to Communications Hub Functions, in circumstances where the aggregate demand for the same cannot be satisfied simultaneously.

H3.28 The DCC shall not be considered to be in breach of this Code with regard to the obligation to achieve Target Response Times if, during the month in question, the aggregate Service Requests sent by all Users exceeds 110% of the aggregate demand most recently forecast for that month by all Users pursuant to Section H3.22 (provided that the DCC shall nevertheless in such circumstances take reasonable steps~~use its reasonable endeavours~~ to achieve the Target Response Times).

H4 PROCESSING SERVICE REQUESTS

Introduction

H4.1 The request by Users, and the provision by the DCC, of certain Services is achieved by means of the sending of communications in accordance with Section H3.3 (Communications to be Sent via the DCC User Interface) and this Section H4. The Services in question are:

(a) Enrolment Services;

(b) Local Command Services;

(c) Core Communication Services; and

(d) Elective Communication Services.

Processing Obligations

H4.2 Each User and the DCC shall each comply with the applicable obligations set out in the Service Request Processing Document concerning the secure processing of the communications required to be sent via the DCC User Interface.

DCC IDs

H4.3 The DCC shall obtain and use EUI-64 Compliant identification numbers for the purposes of its communications under this Code. Where it is expedient to do so, the DCC may use different identification numbers to identify different DCC roles.

H4.4 The DCC shall:

(a) where Section G (Security) requires it to Separate one part of the DCC Systems from another part of the DCC Systems, use different identification numbers for the purposes of its communications from each such part of the DCC Systems; and

(b) use different identification numbers for the purposes of becoming a Subscriber

for different Organisation Certificates or OCA Certificates with different Remote Party Role Codes.

H5 SMART METERING INVENTORY AND ENROLMENT SERVICES

Overview of Enrolment

H5.1 Enrolment of a Smart Metering System occurs:

(a) in the case of electricity, on the Commissioning of the Electricity Smart Meter forming part of that Smart Metering System; or

(b) in the case of gas, on the Commissioning of both the Gas Smart Meter and the Gas Proxy Function forming part of that Smart Metering System.

H5.2 No Device that is to form part of a Smart Metering System (other than the Communications Hub Function) can be Commissioned before the Communications Hub Function that is to form part of that Smart Metering System has been Commissioned.

H5.3 No Device can be Commissioned unless it is:

(a) listed on the Smart Metering Inventory; and

(b) other than for Type 2 Devices, listed with an SMI Status which is not 'withdrawn' or 'decommissioned'.

Statement of Service Exemptions

H5.4 In accordance with Condition 17 of the DCC Licence (and notwithstanding any other provision of this Section H5), the DCC is not obliged to Commission Communications Hub Functions (or therefore to Enrol Smart Metering Systems) where it is exempted from the requirement to do so in accordance with a Statement of Service Exemptions.

Smart Metering Inventory

H5.5 The DCC shall establish and maintain the Smart Metering Inventory in accordance with the Inventory, Enrolment and Withdrawal Procedures.

H5.6 Each User and the DCC shall each comply with the applicable obligations set out in the Inventory, Enrolment and Withdrawal Procedures, which must include obligations concerning:

(a) the addition and removal of Devices to and from the Smart Metering Inventory; and

(b) changes to the SMI Status of the Devices recorded on the Smart Metering Inventory from time to time.

Enrolment of Smart Metering Systems

H5.7 Each User and the DCC shall each comply with the applicable obligations set out in the Inventory, Enrolment and Withdrawal Procedures Document, which must include obligations concerning:

(a) steps to be taken before a Device that is listed on the Smart Metering Inventory is installed and/or Commissioned at a premises;

(b) steps to be taken in order to Commission such a Device;

(c) steps to be taken following the Commissioning of such a Device; and

(d) steps to be taken on the removal and/or replacement of any Device forming part of a Smart Metering System.

H6 DECOMMISSIONING, WITHDRAWAL AND SUSPENSION OF DEVICES

Decommissioning

H6.1 Where a Device other than a Type 2 Device is no longer to form part of a Smart Metering System otherwise than due to its Withdrawal, then that Device should be Decommissioned. A Device may be Decommissioned because it has been uninstalled and/or is no longer operating (whether or not it has been replaced, and including where the Device has been lost, stolen or destroyed).

H6.2 Only the Responsible Supplier(s) for a Communications Hub Function, Smart Meter, Gas Proxy Function or Type 1 Device may Decommission such a Device.

H6.3 Where a Responsible Supplier becomes aware that a Device has been uninstalled and/or is no longer operating (otherwise than due to its Withdrawal), that User shall send a Service Request requesting that it is Decommissioned.

H6.4 On successful processing of a Service Request from a Responsible Supplier in accordance with Section H6.3, the DCC shall:

(a) set the SMI Status of the Device to 'decommissioned';

(b) where relevant, amend the Smart Metering Inventory so that the Device is no longer Associated with any other Devices; and

(c) where the Device in question is a Communications Hub Function, notify any and all Responsible Suppliers (other than the Responsible Supplier that procured such Decommissioning) for that Communications Hub Function of such Decommissioning.

H6.5 Where the DCC receives a Service Request from a User that does not satisfy the requirements of Section H6.2, the DCC shall reject the Service Request.

H6.6 On the Decommissioning of a Communications Hub Function, the other Devices forming part of a Smart Metering System should~~all~~ also be ~~deemed to be~~ Decommissioned ~~(and the DCC shall update their SMI Status accordingly)~~; provided

that the Devices forming part of a Smart Metering System (other than the Gas Proxy Function) may remain Commissioned notwithstanding the Decommissioning of the Communications Hub Function if a replacement Communications Hub Function is Commissioned within a reasonable period.

Withdrawal

H6.7 Where the Responsible Supplier for an Enrolled Smart Metering System for a Designated Premises no longer wishes that Smart Metering System to be Enrolled (and so no longer wishes to receive Communication Services in respect of that Smart Metering System), the Responsible Supplier may request that the Smart Metering System is Withdrawn. Where the Responsible Supplier:

(a) is a User, the Responsible Supplier shall send that request as a Service Request to withdraw each of the Devices comprising that Smart Metering System (but subject to Section H6.9 in relation to the Communications Hub Function); and

(b) is not a User (and does not wish to become a User), [TBC].

H6.8 On the successful processing of a request in accordance with Section H6.7 in respect of a Smart Metering System, the Smart Metering System shall no longer be Enrolled and the DCC shall:

(a) in respect of those Devices forming part of that Smart Metering System and no other Smart Metering System, set the SMI Status of the Devices to 'withdrawn';

(b) to the extent that there are other Devices with which the Withdrawn Devices were previously Associated, amend the Smart Metering Inventory so that the remaining Devices are no longer Associated with the Withdrawn Devices; and

(c) remove the Withdrawn Devices from the Device Log of the Communications Hub Function.

H6.9 For the avoidance of doubt, Section H6.8(a) prevents the Withdrawal of a Communications Hub Function where that Communications Hub Function forms part of more than one Smart Metering System.

Suspension

H6.10 Where a Device's Device Model is removed from the Certified Products List, that Device shall be Suspended and the DCC shall set the SMI Status of the Device to 'suspended'.

H6.11 Where a Communications Hub Device Model is removed from the Certified Products List, both the Communications Hub Function and the Gas Proxy Function shall be deemed to be Suspended (and Section H6.10 shall apply accordingly).

Ancillary Obligations

H6.12 Each User and the DCC shall each comply with the obligations set out in the Inventory, Enrolment and Withdrawal Procedures concerning Decommissioning, Suspension and Withdrawal of Devices (and the Smart Metering Systems of which such Devices form part), including (where applicable) notifying other Users of such Decommissioning, Suspension and Withdrawal.

H7 ELECTIVE COMMUNICATION SERVICES

Eligible Smart Metering Systems

H7.1 Elective Communication Services can only be provided in respect of Smart Metering Systems that have been Enrolled.

Entitlement to Elective Communication Services

H7.2 Only a User is entitled to receive Elective Communication Services. A Party that is not a User is not entitled to receive Elective Communication Services.

H7.3 A User shall not be entitled to request or receive (and the DCC shall not provide to such User) any Elective Communication Services that would constitute a Restricted Communication Service.

Preliminary Assessment of Elective Communication Services

H7.4 Notwithstanding Section E7.2, any Party may request an initial evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service (a "**Preliminary Assessment**").

H7.5 Requests for a Preliminary Assessment shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC.

H7.6 The DCC shall respond to requests for a Preliminary Assessment in accordance with the time period prescribed by Condition 17 of the DCC Licence, and shall either (in accordance with Condition 17 of the DCC Licence):

(a) provide an initial evaluation of the technical feasibility and the likely Charges for a proposed Elective Communication Service; or

(b) give notice that a further and more detailed evaluation of the request is required.

Detailed Evaluation of Elective Communication Services

H7.7 Any Party that has requested a Preliminary Assessment and obtained a response as

described in Section H7.6(b) may request a more detailed evaluation of the technical feasibility and likely Charges for a proposed Elective Communication Service (a "**Detailed Evaluation**").

H7.8 Requests for a Detailed Evaluation shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC. Following receipt of any such request (or purported request), the DCC shall:

(a) where the request is incomplete or the DCC reasonably requires further information in order to assess the request, notify the Party that this is the case and provide reasonable assistance to the Party in re-submitting its request;

(b) once the DCC has received all the information it reasonably requires in order to assess the request, confirm the applicable Charges payable in respect of the Detailed Evaluation; and

(c) once the Party has agreed to pay the applicable Charges, provide the Detailed Evaluation to the requesting Party (in accordance with the time period prescribed by Condition 17 of the DCC Licence).

Request for an Offer for an Elective Communication Service

H7.9 Any Party that has requested a Preliminary Assessment in respect of a proposed Elective Communication Service, and obtained a response as described in Section H7.6(a), may request a formal offer for that proposed Elective Communication Service.

H7.10 Any Party that has requested and obtained a Detailed Evaluation in respect of a proposed Elective Communication Service may request a formal offer for that proposed Elective Communication Service.

H7.11 Following a request pursuant to Section H7.9 or H7.10, the DCC shall (in accordance with the time period prescribed by Condition 17 of the DCC Licence):

(a) make an offer to provide the Elective Communication Service in question; or

(b) notify the Party that the DCC is not willing to make such an offer (provided that the DCC may only do so where the DCC is not obliged to make such an offer in accordance with Condition 17 of the DCC Licence).

Formal Offer

H7.12 An offer to provide the Elective Communication Service made by the DCC pursuant to this Section H7 shall:

(a) include details of the Charges that would apply to the Elective Communication Service, as determined in accordance with the Charging Methodology;

(b) where the proposed Charges have been calculated (in accordance with the Charging Methodology) on the assumption that one or more other Parties accept offers made pursuant to this Section H7, provide for two alternative sets of Charges, one of which is contingent on acceptance of all the other such offers and one of which is not; and

(c) include an offer by the DCC to enter into a Bilateral Agreement with the Party requesting the Elective Communication Service.

H7.13 Each Bilateral Agreement must:

(a) be based on the Specimen Bilateral Agreement, subject only to such variations from such specimen form as are reasonable in the circumstances;

(b) not contradict or seek to override any or all of this Section H or Sections G (Security), I (Data Privacy), J (Charges), L (Smart Metering Key Infrastructure) or M (General);

(c) where reasonably necessary in accordance with the Charging Methodology, provide for Charges that include or comprise a standing charge that is payable by the recipient of the Elective Communication Service regardless of whether or not the Elective Communication Service is requested or provided;

(d) where reasonably necessary in accordance with the Charging Methodology,

require the recipient of the Elective Communication Service to pay compensation to DCC in the event of the early termination of the Bilateral Agreement (except in the case of termination as envisaged by Section H7.13(e));

(e) allow the recipient of the Elective Communication Services to terminate the Bilateral Agreement without paying compensation to the extent that such compensation is intended to recover investments made for the purposes of providing the Elective Communication Service where (and to the extent that) the DCC subsequently offers a Service listed in the DCC User Interface Services Schedule that relies upon such investments (and each Bilateral Agreement must provide for disputes regarding this provision to be subject to an initial Panel determination, but to ultimately be determined by arbitration); and

(f) where reasonably necessary, require the recipient of the Elective Communication Services to provide credit support in respect of its obligation to pay the compensation referred to in Section H7.13(d).

H7.14 The parties to each Bilateral Agreement shall ensure that the Bilateral Agreement describes the Elective Communication Services in a manner consistent with the description of the Core Communication Services in this Code, including so as to identify (to the extent appropriate) equivalents of the following concepts: Service Requests; Non-Device Service Requests; Pre-Commands; Signed Pre-Commands; Commands; Services Responses; Alerts; and Target Response Times. To the extent that an Elective Communication Service comprises equivalents of such concepts, references to such concepts in this Code shall be construed as including the equivalent concepts under each Bilateral Agreement (and the DCC and the relevant User under the Bilateral Agreement shall comply with Sections H3 (DCC User Interface) and H4 (Processing Service Requests) in respect of the same). For the purposes of each Elective Communication Service (unless the Panel otherwise determined on a User's application):

(a) the applicable Service Request shall be deemed to be a Critical Service Request,

unless it results only in the sending of a Command to a Device that would arise were a Non-Critical Service Request listed in the DCC User Interface Service Schedule to be requested;

(b) the applicable Service Request (and any associated Pre-Command) shall be deemed to contain Data that requires Encryption, unless it contains only Data described in the GB Companion Specification as capable of being sent without Encryption.

H7.15 Elective Communication Services shall be provided in accordance with this Code and the applicable Bilateral Agreement. In the event of any inconsistency between this Code and a Bilateral Agreement, the provisions of this Code shall prevail.

H7.16 The DCC shall not agree to any variations to a Bilateral Agreement that would cause that agreement to become inconsistent with the requirements of this Section H7.

Disputes Regarding Offers for Elective Communication Services

H7.17 Where the requirements of Condition 20 of the DCC Licence are met, a Party that has requested an offer for a proposed Elective Communication Service may refer a dispute regarding such request to the Authority for determination under and in accordance with that Condition.

Publication of Details of Elective Communication Services

H7.18 Once the DCC has commenced provision of an Elective Communication Service pursuant to a Bilateral Agreement, the DCC shall notify the Code Administrator of the date on which the provision of such service commenced (but shall not provide any details regarding such agreement to the Code Administrator).

H7.19 The DCC shall, on or around the date falling six months after it commenced provision of an Elective Communication Service pursuant to a Bilateral Agreement, provide to the Code Administrator the following details:

(a) a brief description of the Elective Communication Service;

(b) the frequency with which, and (where stated) the period during which, the Elective Communication Service is to be provided; and

(c) the Target Response Time within which the Elective Communication Service is to be provided.

H7.20 The Code Administrator shall arrange for the publication on the Website of the details provided to it pursuant to Section H7.19. The Code Administrator shall monitor and report to the Panel on whether the DCC has provided details pursuant to Section H7.18 in respect of Elective Communication Services of which the Code Administrator is notified under Section H7.18.

H7.21 Without prejudice to the DCC's obligations under Section H7.19, the existence and contents of each Bilateral Agreement shall constitute Confidential Information which the DCC is obliged to keep confidential in accordance with Section M4 (Confidentiality).

H8 SERVICE MANAGEMENT, SELF-SERVICE INTERFACE AND SERVICE DESK

General

H8.1 The DCC shall provide the Services in a manner that is consistent with:

(a) the Service Management Standards; or

(b) any other methodology for service management identified by the DCC as being more cost efficient than the Service Management Standards, and which has been approved by the Panel for such purpose.

Maintenance of the DCC Systems

H8.2 The DCC shall (insofar as is reasonably practicable) undertake Maintenance of the DCC Systems in such a way as to avoid any disruption to the provision of the Services (or any part of them).

H8.3 Without prejudice to the generality of Section H8.2, the DCC shall (unless the Panel agrees otherwise):

(a) undertake Planned Maintenance of the DCC Systems only between 20.00 hours and 08.00 hours;

(b) limit Planned Maintenance of the Self-Service Interface to no more than four hours in any month; and

(c) limit Planned Maintenance of the DCC Systems generally (including of the Self-Service Interface) to no more than six hours in any month.

H8.4 At least 20 Working Days prior to the start of each month, the DCC shall make available to Parties, to Registration Data Providers and to the Technical Architecture and Business Architecture Sub-Committee a schedule of the Planned Maintenance for that month. Such schedule shall set out (as a minimum) the following:

(a) the proposed Maintenance activity (in reasonable detail);

(b) the parts of the Services that will be disrupted (or in respect of which there is a Material Risk of disruption) during each such Maintenance activity;

(c) the time and duration of each such Maintenance activity; and

(d) any associated risk that may subsequently affect the return of normal Services.

H8.5 The Panel may (whether or not at the request of a Party) request that the DCC reschedules any Planned Maintenance set out in a monthly schedule provided pursuant to Section H8.4. In making any such request, the Panel shall provide the reasons for such request to the DCC in support of the request. The DCC will take all reasonable steps to accommodate any such request.

H8.6 As soon as reasonably practicable after the DCC becomes aware of any Unplanned Maintenance, the DCC shall notify the Technical Architecture and Business Architecture Sub-Committee, Parties and (insofar as they are likely to be affected by such Unplanned Maintenance) Registration Data Providers of such Unplanned Maintenance (and shall provide information equivalent to that provided in respect of Planned Maintenance pursuant to Section H8.4).

H8.7 During the period of any Planned Maintenance or Unplanned Maintenance, the DCC shall provide Parties and (insofar as they are likely to be affected by such maintenance) Registration Data Providers with details of its duration and the expected disruption to Services to the extent they differ from the information previously provided.

DCC Internal System Changes

H8.8 Where the DCC is proposing to make a change to DCC Internal Systems, the DCC shall:

(a) undertake an assessment of the likely impact on:

(i) Parties in respect~~ers~~ of any potential disruption to Services; and/or

~~(i)~~(ii) RDPs in relation to the sending or receipt of data pursuant to Section E

(Registration Data),

that may arise as a consequence of the Maintenance required to implement the contemplated change;

(b) where such assessment identifies that there is a Material Risk of disruption to Parties and/or RDPs~~Services~~, consult with Parties and/or RDPs (as applicable)~~Users~~ and with the Technical Architecture and Business Architecture Sub-Committee regarding such risk;

(c) provide the Parties and RDPs~~Users~~ the opportunity to be involved in any testing of the change to the DCC Internal Systems prior to its implementation; and

(d) undertake an assessment of the likely impact of the contemplated change upon the security of the DCC Total System, ~~Users' Systems and~~ Smart Metering Systems, and the Systems of Parties and/or RDPs.

Release Management

H8.9 The DCC shall ensure that it plans, schedules and controls the building, testing and deployment of releases of IT updates, procedures and processes in respect of the DCC Internal Systems and/or the Parse and Correlate Software in accordance with a policy for Release Management (the "**DCC Release Management Policy**").

H8.10 The DCC shall ensure that the DCC Release Management Policy:

(a) defines the scope of the matters that are to be subject to the policy in a manner consistent with the Service Management Standards;

(b) includes a mechanism for setting priorities for different types of such matters;

(c) defines periods of change-freeze where no such matters may be implemented; and

(d) defines periods of notice to be given to Parties and RDPs~~the Users~~ prior to the implementation of such matters.

H8.11 The DCC shall make the DCC Release Management Policy available to Parties, RDPs~~Users~~ and ~~to~~ the Technical Architecture and Business Architecture Sub-Committee. The DCC shall consult with Parties, RDPs~~Users~~ and the Technical Architecture and Business Architecture Sub-Committee before making any changes to the DCC Release Management Policy.

H8.12 The DCC's obligation under Section H8.11 is in addition to its obligations in respect of Planned Maintenance and changes to DCC Internal Systems to the extent that the activity in question involves Planned Maintenance or changes to DCC Internal Systems.

Self-Service Interface and Service Desk: General

H8.13 Each User shall take reasonable steps ~~use its reasonable endeavours~~ to access the information it needs, and to seek to resolve any queries it may have, via the Self-Service Interface in the first instance. A User shall only contact the Service Desk where it cannot reasonably obtain the information it needs, or resolve its query, via the Self-Service Interface.

H8.14 A Party that is not a User will be unable to access the Self-Service Interface, but may contact the Service Desk.

Self-Service Interface

H8.15 The DCC shall maintain and keep up-to-date an interface (the **Self-Service Interface**) which:

(a) complies with the specification required by the Self-Service Interface Design Specification;

(b) is made available to Users in accordance with the Self-Service Interface Code of Connection via DCC Gateway Connections; and

(c) allows Users to access the information described in Section H8.16.

H8.16 The Self-Service Interface must (as a minimum) allow the following categories of

User to access the following:

(a) the Smart Metering Inventory, which shall be available to all Users and capable of being searched by reference to the following (provided that there is no requirement for the DCC to provide information held on the inventory in respect of Type 2 Devices other than IHDs):

(i) the Device ID, in which case the User should be able to extract all information held in the inventory in relation to (I) that Device, (II) any other Device Associated with the first Device, (III) any Device Associated with any other such Device; and (IV) any Device with which any of the Devices in (I), (II) or (III) is Associated;

(ii) the MPAN or MPRN, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meter to which that MPAN or MPRN relates, or in relation to any Device Associated with that Smart Meter or with which it is Associated;

(iii) post code and premises number or name, in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked to that postcode and premises number or name, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(iv) the UPRN (where this has been provided as part of the Registration Data), in which case the User should be able to extract all information held in the inventory in relation to the Smart Meters for the MPAN(s) and/or MPRN linked by that UPRN, or in relation to any Device Associated with those Smart Meters or with which they are Associated;

(b) a record of the Service Requests and Signed Pre-Commands sent by each User, and of the Acknowledgments, Pre-Commands, Service Responses and Alerts received by that User (during a period of no less than three months prior to any date on which that record is accessed), which shall be available only to that

User;

(c) a record, which (subject to the restriction in Section I1.4 (User Obligations)) shall be available to all Users:

(i) of all 'Read Profile Data' and 'Retrieve Daily Consumption Log' Service Requests in relation to each Smart Meter (or Device Associated with it) that were sent by any User during a period of no less than three months prior to any date on which that record is accessed; and

(ii) including, in relation to each such Service Request, a record of the type of the Service Request, whether it was successfully processed, the time and date that it was sent to the DCC, and the identity of the User which sent it;

(d) the Incident Management Log, for which the ability of Users to view and/or amend data shall be as described in Section H9.4 (Incident Management Log);

(e) the CH Order Management System, which shall be available to all Users;

(f) the following information in respect of the SM WAN, which shall be available to all Users (and which shall be capable of interrogation by post code and postal outcode):

(i) whether a Communications Hub Function installed in a premises at any given location:

(A) is expected to be able to connect to the SM WAN;

(B) is expected to be able to connect to the SM WAN from a particular date before 1 January 2021, in which case the date shall be specified; or

~~(A)~~(C) cannot be confirmed as being able to connect to the SM WAN before 1 January 2021;

~~(ii) any locations included within a geographical area which is for the time~~

~~being the subject of a Service Exemption Category 2 (as defined in the DCC Licence), and (where applicable) the date from which such locations will cease to be so included;~~

~~(iii)~~(ii) any known issues giving rise to poor connectivity at any given location (and any information regarding their likely resolution); and

~~(iv)~~(iii) any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM WAN;

(g) additional information made available by the DCC to assist with the use of the Services and diagnosis of problems, such as service status (including information in respect of Planned Maintenance and Unplanned Maintenance) and frequently asked questions (and the responses to such questions), which shall be available to all Users; and

(h) anything else expressly required by a provision of this Code.

H8.17 Without prejudice to the requirements of Sections H8.16(b) and (c), to the extent that the Self-Service Interface does not allow a User to access a record of the information referred to in those Sections in respect of the preceding 7 years, then:

(a) subject (in the case of the information referred to in Section H8.16(c)) to the restriction in Section I1.4 (User Obligations), that User shall be entitled to request such information from the DCC; and

(b) the DCC shall provide such information to that User as soon as reasonably practicable following such request.

H8.18 The DCC shall ensure that the Self-Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

Service Desk

H8.19 The DCC shall ensure that a team of its representatives (the **Service Desk**) is available to be contacted as follows:

(a) the Service Desk shall be contactable via the following means (to be used by Parties and Registration Data Providers, to the extent available to them, in the following order of preference, save as otherwise provided for in the Incident Management Policy):

(i) the Self-Service Interface;

(ii) a dedicated email address published on the DCC Website; and

(iii) a dedicated telephone number published on the DCC Website;

(b) the Service Desk can be used by Parties to seek resolution of queries relating to the Services (provided that Users shall seek resolution via the Self-Service Interface in the first instance); and

(c) the Service Desk can be used by Incident Parties that are not Users to raise Incidents (or by Users, where the Incident Management Log is not available via the Self-Service Interface, to raise or provide information in respect of Incidents), which the DCC shall then reflect in the Incident Management Log.

H8.20 The DCC shall ensure that the Service Desk is available at all times, and shall provide alternative arrangements (a different telephone number and email address) where the usual Service Desk in not available. Where a different telephone number and email address is to be used, the DCC shall publish details of the alternative number and address at least 20 Working Days in advance.

H9 INCIDENT MANAGEMENT

Incident Management Policy

H9.1 The Incident Management Policy must (as a minimum) make provision for the following matters:

(a) raising an Incident by recording it in the Incident Management Log;

(b) categorisation of Incidents into 5 categories of severity ("**Incident Category 1, 2, 3, 4 and 5**" respectively, such that Incident Category 1 is the most severe and Incident Category 5 the least);

(c) prioritisation of Incidents, and (in those cases where the DCC is responsible for resolving an Incident) the time period within which an Incident in each Incident Category should be resolved (the "**Target Resolution Time**");

(d) prioritising and timescale for closure of Problems;

(e) allocation of responsibility for Incidents and Problems in accordance with Section H9.2;

(f) identification of other interested persons who are to be kept informed regarding Incidents;

(g) courses of action to be undertaken in seeking to resolve Incidents and close Problems, including the need to update the Incident Management Log to record activity carried out (or planned to be carried out);

(h) rules for the escalation of Incidents;

(i) rules for the declaration of a Major Incident, and for the appointment of managers to coordinate resolution of Major Incidents;

(j) rules for the closure of a resolved Incident;

(k) rules for opening and closing Problem records by the DCC;

(l) rules for reopening closed Incidents; and

(m) describe the roles and responsibilities of the following persons in respect of different types of Incident: Users, Eligible Subscribers, DCC Gateway Parties and Registration Data Providers (such persons being the "Incident Parties").

Incident and Problem Management Responsibility

H9.2 The Incident Management Policy must allocate responsibility for resolution of Incidents and closure of Problems in accordance with the following principles:

(a) where an Incident Party becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed), and:

(i) where such Incident is reasonably capable of being resolved via the Self-Service Interface or via a Service Request which that Incident Party has the right to send, that Incident Party shall exercise such rights with a view to resolving the Incident;

(ii) where the CH Support Materials are relevant to the Incident and require the Incident Party to take any steps prior to raising an Incident, that Incident Party shall take such steps with a view to resolving the Incident; or

(iii) where the Incident Party is a Supplier Party and it is already at the premises when it first becomes aware of the Incident, and to the extent the Incident is caused by a Communications Hub and is not capable of being resolved via communications over the SM WAN, then that Incident Party shall be responsible for resolving that Incident;

(b) subject to Section H9.2(a), the DCC shall be responsible for resolving Incidents and closing Problems to the extent they are caused by:

(i) the DCC Systems;

(ii) the Parse and Correlate Software; or

(iii) a Communications Hub, and are capable of being resolved via communications over the SM WAN;

(c) subject to Section H9.2(a), the Lead Supplier for a Communications Hub shall be responsible for resolving Incidents and closing Problems to the extent they are caused by that Communications Hub and not capable of being resolved or closed via communications over the SM WAN;

(d) subject to Section H9.2(a), the Responsible Supplier for a Smart Metering System shall be responsible for resolving Incidents and closing Problems to the extent caused by Devices (other than the Communications Hub) forming part of that Smart Metering System;

(e) in the case of Incidents arising in respect of the exchange of Data under Section E (Registration Data):

(i) the relevant Registration Data Provider shall be responsible for resolving those Incidents arising on its side of the Registration Data Interface; and

(ii) the DCC shall be responsible for resolving all other such Incidents; and

(f) in the case of Incidents other than those referred to elsewhere in this Section H9.2, the Incident Party assigned responsibility in accordance with the Incident Management Policy shall be responsible for resolving the Incident.

Incident Management Log

H9.3 The DCC shall maintain and keep up-to-date an electronic log (the **Incident Management Log**) that records the following in respect of each Incident:

(a) a unique reference number (to be allocated to each Incident that is identified by, or reported to, the DCC);

(b) the date and time that the Incident was identified by, or reported to, the DCC;

(c) the nature of the Incident and the location at which it occurred;

(d) whether the Incident was identified by the DCC, or otherwise the person that reported the Incident to the DCC;

(e) the categorisation of the Incident in accordance with the Incident Management Policy;

(f) the person to whom the Incident has been allocated for resolution;

(g) the course of action to be taken, or taken, to resolve the Incident;

(h) the DCC's Good Industry Practice assessment of which Incident Parties and/or Services are affected by the Incident;

(i) details of any communications with Incident Parties in respect of the Incident;

(j) comments regarding any mitigating circumstances regarding the Incident;

(k) the potential impact of the Incident on the DCC's ability to meet the Target Service Levels;

(l) the current status of the Incident, and (once applicable) the date and time that the Incident was closed; and

(m) a reference to any related Problem logged.

H9.4 The following shall apply in respect of the Incident Management Log:

(a) (subject to paragraphs (c) and (d) below) the DCC shall provide Users with the ability to view and amend the Incident Management Log via the Self Service Interface;

(b) (subject to paragraphs (c) and (d) below) the DCC shall provide Incident Parties that are not Users with the ability to obtain information from, and report information which the DCC shall then add to, the Incident Management Log via the Service Desk;

(c) only the following Incident Parties shall be entitled to view or obtain information from the Incident Management Log in respect of an Incident:

(i) the Incident Party that raised the Incident;

(ii) the Incident Party that is assigned responsibility for resolving the Incident;

(iii) (subject to any further rules in the Incident Management Policy) the following persons:

(A) the Lead Supplier for each Communications Hub that is affected by the Incident;

(B) the Responsible Supplier for each Smart Metering System that is affected by the Incident;

(C) the Electricity Distributor or Gas Transporter (as applicable) for each Smart Metering System that is affected by the Incident;

(D) the DCC Gateway Party for, and any Party notified to the DCC in accordance with Section H15.17 (Use of a DCC Gateway Connection) as entitled to use, a DCC Gateway Connection shall be able to view matters relating to any Incident affecting that DCC Gateway Connection;

(E) the Registration Data Providers entitled to use a DCC Gateway Connection as provided for in Section E3 (DCC Gateway Connections for Registration Data Providers) shall be able to view matters relating to any Incident affecting that DCC Gateway Connection; and

(F) any other Incident Party that is reasonably likely to be affected by the Incident;

(d) only the following Incident Parties shall be entitled to amend and report

information to be added to the Incident Management Log:

(i) the Incident Party that raised the Incident;

(ii) the Incident Party that is assigned responsibility for resolving the Incident; and

(iii) (subject to any further rules in the Incident Management Policy) the following persons:

(G) the Lead Supplier for each Communications Hub that is affected by the Incident (but such amending and reporting shall be limited to matters relating to the Communications Hub Function); and

(H) the Responsible Supplier(s) for each Smart Metering System that is affected by the Incident (but such amending and reporting shall exclude matters relating to the Communications Hub Function); and

(e) to the extent that an Incident Party does not have the necessary rights in accordance with paragraph (d) above to amend the Incident Management Log, an Incident Party shall report the matter to the DCC, which shall then amend the Incident Management Log to reflect such matters.

Access to data regarding Problems

H9.5 Where an Incident refers to a Problem, the DCC or any Incident Party may request that the person assigned responsibility for the Problem supplies to the DCC or Incident Party making the request reasonable information regarding the Problem, provided that information in respect of any other Incident shall only be supplied to an Incident Party where that Incident Party would be allowed access to that information in accordance with Section H9.4.

Addition of Incidents to the Incident Management Log

H9.6 Where an Incident Party becomes aware of an Incident that is not yet logged on the

Incident Management Log (or, if logged, is incorrectly logged as closed):

(a) (where the Incident Party is a User) to the extent such Incident is reasonably capable of being resolved via the Self-Service Interface or via a Service Request which that User has the right to send, then the User shall exercise such rights with a view to resolving the Incident;

~~(a)~~(b) (where the Incident Party is an RDP) to the extent such Incident is reasonably capable of being resolved by re-submitting a subset of Registration Data in accordance with the Registration Data Interface Documents, then the RDP shall re-submit such Data; or

~~(b)~~(c) where neither paragraph (a) nor (b) above apply~~the Incident Party is not a User~~ (or to the extent the Incident ~~is not reasonably capable of being resolved in such manner, or~~ is not resolved despite compliance with paragraph (a) or (b) above~~such exercise of rights~~), then the Incident Party shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident) via the Self-Service Interface (or, in the case of non-Users, the Service Desk).

H9.7 Where the DCC becomes aware of an Incident that is not yet logged on the Incident Management Log (or, if logged, is incorrectly logged as closed), then the DCC shall add the Incident to the Incident Management Log (or, if incorrectly logged as closed, reopen the Incident).

Resolving Incidents and Closing Problems

H9.8 Where an Incident has been added to the Incident Management Log (or reopened) pursuant to Section H9.6 or H9.7, then (until such time as that Incident is closed) the DCC and each relevant Incident Party shall each take all the steps allocated to them under and in accordance with the Incident Management Policy in respect of an Incident of the relevant type, so as to:

(a) in the case of Incidents for which an Incident Party is responsible, resolve the Incident as soon as reasonably practicable; or

(b) in the case of Incidents for which the DCC is responsible, resolve the Incident in accordance with the applicable Target Resolution Time.

H9.9 Where a Problem has been assigned to the DCC or an Incident Party, then (until such time as that Problem is closed) the DCC and each relevant Incident Party shall each take all the steps allocated to it under and in accordance with the Incident Management Policy so as to close the Problem in accordance with priority for resolution and closure set out in the Incident Management Policy.

Major Incident Notification and Reports

H9.10 Where an Incident Party is identified as responsible for resolution of an Incident, and where that Incident Party considers (or should reasonably have considered) that the Incident constitutes a Major Incident, then such Incident Party shall notify the DCC of such fact (in accordance with the Incident Management Policy).

H9.11 Where the DCC becomes aware of a Major Incident, the DCC shall notify all Incident Parties that are likely to be affected by such Major Incident (in accordance with the Incident Management Policy).

H9.12 In the event of a Major Incident:

(a) where the DCC is responsible for resolving that Incident, each Incident Party shall provide the DCC with all reasonable assistance as the DCC may request; and

(b) where an Incident Party is responsible for resolving that Incident, the DCC and all other Incident Parties shall provide all reasonable assistance to the Incident Party responsible for resolving that Incident as such Incident Party may request,

(in each case) in relation to the resolution of that Incident, including as set out in the Incident Management Policy.

H9.13 Within two Working Days following resolution of a Major Incident, the DCC or the Incident Party responsible for resolving that Major Incident shall provide a summary report to the Panel in respect of that Major Incident. Such summary report must

include (as a minimum):

(a) the nature, cause and impact (and likely future impact) of the Major Incident (including, where the DCC is responsible for resolving the Major Incident, details of the impact the Major Incident had on provision of the Services and over what period, and details of any Data that may have been lost); and

(b) the action taken in the resolution of the Major Incident.

H9.14 Within 20 Working Days following resolution of a Major Incident, the DCC or Incident Party responsible for resolving that Major Incident shall conduct a review regarding that Major Incident and its resolution, and shall report to the Panel and the Authority (and, on request, the Secretary of State) on the outcome of such review. Such report must include (as a minimum):

(a) a copy of the summary report produced in respect of the Major Incident pursuant to Section H9.13;

(b) (where the DCC is responsible for resolving the Major Incident) any Services which were not restored within the Target Resolution Time for the Major Incident;

(c) (where the DCC is responsible for resolving the Major Incident) where any Services were not restored within the Target Resolution Time, the reason why this was the case and the steps the DCC is taking to prevent the re-occurrence of such an event;

(d) a review of the response to the Major Incident and its effectiveness;

(e) any failures by Incident Parties to comply with their obligations under Energy Licences and/or this Code that caused or contributed to the Major Incident or its consequences;

(f) (where the DCC is responsible for resolving the Major Incident) whether there is likely to be a reduction (and, to the extent reasonably capable of being determined at that time, the amount of the anticipated reduction) in the DCC's

External Costs (as defined in the DCC Licence) arising as a consequence of the DCC Service Providers failing to achieve a restoration of any Services within the Target Resolution Time; and

(g) any Modifications that could be made to this Code to mitigate against future Incidents and/or their consequences.

H9.15 The Panel shall make each report produced by the DCC pursuant to Section H9.14 available to the other Parties, subject to any redactions it considers necessary to avoid a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

Disputes

H9.16 Where Disputes arise between the Incident Parties regarding whether or not the DCC and/or an Incident Party has complied with its obligations under this Section H9, then such Dispute shall be subject to determination by the Panel (which determination shall be final and binding).

H10 BUSINESS CONTINUITY

Emergency Suspension of Services

H10.1 Section H10.2 applies in respect of any Party or RDP which has an established DCC Gateway Connection where, by virtue of the action or failure to act of that Party or RDP, or of any event occurring on or in relation to the Systems of that Party or RDP:

(a) the DCC Systems are being Compromised to a significant extent; or

(b) the DCC has reason to believe that there is an immediate threat of the DCC Systems being Compromised to a significant extent.

H10.2 Where this Section H10.2 applies, the DCC may, to the extent that it is necessary to do so in order to avoid or mitigate the potential impact of any Comprise to the DCC Systems, temporarily suspend:

(a) in respect of a Party whose actions or Systems are giving rise to the actual or threatened Compromise:

(i) the provision (in whole or in part) of the Services to that Party;

(ii) the rights of that Party to receive (in whole or in part) the Services; and/or

(iii) the ability of that Party to use any DCC Gateway Connection; or

(b) in respect of an RDP whose actions or Systems are giving rise to the actual or threatened Compromise, the ability of that RDP to use any DCC Gateway Connection.

H10.3 Where the DCC commences any temporary suspension of the provision of Services or rights, or of the ability to use a DCC Gateway Connection in accordance with Section H10.2, it shall promptly (and in any event within 24 hours) notify the Panel of the suspension and the reasons for it, and shall provide the Panel with such information

relating to the suspension as may be requested.

H10.4 Where the Panel receives a notification in accordance with Section H10.3, it shall promptly consider the circumstances of the suspension, and:

(a) shall either confirm the suspension, or determine that the suspension is to cease to have effect (in which case the suspended Services, rights or ability to use any DCC Gateway Connection shall be reinstated); and

(b) may in either case give such directions as it considers appropriate:

(i) to the DCC in relation to the continuing suspension or the reinstatement of the Services, rights or ability to use any DCC Gateway Connection (as the case may be); and/or

(ii) to the Party or RDP whose Services, rights or ability to use any DCC Gateway Connection were suspended by the DCC, for the purpose of remedying any actual or potential cause of Compromise to the DCC Systems or for preventing its recurrence.

H10.5 The DCC shall comply with any direction given to it by the Panel in accordance with Section H10.4, and shall provide such reasonable support and assistance to the Party or RDP whose Services, rights or ability to use any DCC Gateway Connection were suspended by the DCC as that Party or RDP may request for the purpose of remedying any actual or potential cause of Compromise to the DCC Systems or for preventing its recurrence.

H10.6 A Party shall comply with any direction given to it by the Panel in accordance with Section H10.4.

H10.7 Each Electricity Network Party and each Gas Network Party shall ensure that its RDP shall (when acting in its capacity as the Network Party's RDP) comply with any direction given to it by the Panel in accordance with Section H10.4.

H10.8 Where the DCC or any Party or RDP which is directly affected by a decision of the Panel made pursuant to Section H10.4 disagrees with that decision, it may refer the

matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

The Business Continuity and Disaster Recovery Procedure

H10.9 Subject to Section H10.10, the DCC shall comply with the requirements of the Business Continuity and Disaster Recovery Procedure for the purposes of ensuring so far as reasonably practicable that:

(a) there is no significant disruption to the provision of any of the Services by the DCC; and

(b) where there is any such significant disruption, the provision of those Services is restored as soon as is reasonably practicable.

H10.10 Where, in the case of Disasters, taking a different course of action to following the BCDR Procedure would (in accordance with Good Industry Practice) be a more effective course of action in order to achieve the objectives set out in Section H10.9, then the DCC may take such steps to achieve such objectives (rather than complying with the BCDR Procedure). Where the DCC takes a course of action that does not comply with the BCDR Procedure, the DCC must inform the Panel as soon as possible thereafter of the steps taken and the reasons why the DCC considered that they were more effective.

Testing the Business Continuity and Disaster Recovery Procedure

H10.11 The DCC shall:

(a) from time to time, and at least once each year, carry out a test of the operation of its disaster recovery and business continuity arrangements in order to assess whether the Business Continuity and Disaster Recovery Procedure remains suitable for achieving the objectives described at Section H10.9; and

(b) following any such test, report to the Panel and the Authority on the outcome of the test, and on any proposals made by the DCC in relation to the Business Continuity and Disaster Recovery Procedure having regard to that outcome.

H10.12 Each Party shall provide the DCC with any such assistance and co-operation as it may reasonably request for the purpose of testing its disaster recovery and business continuity arrangements and confirming the operation of the Business Continuity and Disaster Recovery Procedure.

Business Continuity and Disaster Recovery Targets

H10.13 The DCC shall, on the occurrence of a Disaster:

(a) take all reasonable steps to ensure that any and all affected Services are restored in accordance with the Target Resolution Time for a Major Incident; ~~and~~

(b) ensure in any event that those Services are restored within eight hours of the occurrence of that Disaster (except in the case of a Disaster that directly affects a DCC Gateway Connection and where the DCC Gateway Party for that DCC Gateway Connection has not procured a backup DCC Gateway Connection, in which case the DCC shall take all reasonable steps to restore Services in relation to that DCC Gateway Connection at the earliest opportunity); and

~~(b)~~(c) ensure in any event that Services are restored such that the loss of Data arising as a consequence of the Disaster is not in excess of that prescribed by the relevant Service Provider Performance Measures.

H11 PARSE AND CORRELATE SOFTWARE

Provision of Parse and Correlate Software

H11.1 On receipt of a request to do so from any person, the DCC shall supply to that person a copy of the most recently released version of computer software (the "**Parse and Correlate Software**") which:

(a) has the functionality specified in Section H11.2;

(b) has the characteristics specified in Section H11.3; and

(c) is provided in the format specified in Section H11.4.

H11.2 The functionality specified in this Section H11.2 is that the software must enable any User to:

(a) convert all Service Responses and Alerts into the format that is set out in respect of them in the Message Mapping Catalogue; and

(b) confirm that any Pre-Command is substantively identical to its associated Critical Service Request.

H11.3 The characteristics specified in this Section H11.3 are that:

(a) the software is written using the Java programming language; and

(b) the software is capable of operating on the version of the Java Virtual Machine/Run-time Environment prevailing at the time at which the design of that version of the software was finalised.

H11.4 The format specified in this Section H11.4 is that the software:

(a) is provided as both:

(i) an executable file which includes everything required to enable the software to be installed on the systems of the person to whom it is provided in such a manner as not to have a material adverse effect on the

operation of other software deployed within the same system environment; and

(ii) source software code; and

(b) can be confirmed, on receipt by the person to whom it is provided:

(c) as having been provided by the DCC; and

(i) as being authentic, such that any tampering with the software would be apparent.

Maintenance of the Parse and Correlate Software

H11.5 The DCC shall:

(a) maintain the Parse and Correlate Software supplied by it to any person so as to ensure that it at all times continues to have the functionality specified in Section H11.2; and

(b) for that purpose develop and release to such persons, where it is reasonably necessary from time to time, new versions of the Parse and Correlate Software which shall have the characteristics specified in Section H11.3 and be provided in the format specified in Section H11.4.

Development of the Parse and Correlate Software

H11.6 When proposing to develop any version of the Parse and Correlate Software, the DCC shall consult with Users, having regard in particular to their views in relation to:

(a) the need for a new version of the software;

(b) the potential impact of the proposed new version of the software on the security of the DCC Total System, User Systems and Smart Metering Systems;

(c) the design of the software generally; and

(d) the required operational performance of the proposed version of the software on

a standard system configuration specified by the DCC for the purposes of the consultation.

H11.7 Following any consultation with Users, the DCC shall inform all Users of the design of the version of the Parse and Correlate Software that it intends to develop.

H11.8 Before supplying any version of the Parse and Correlate Software to any person, the DCC shall:

(a) ensure that that version of the software has been adequately tested for the purpose of ensuring that it satisfies the requirements of Sections H11.2 to H11.4;

(b) provide suitable opportunities for Acceptance Testing of that version of the software;

(c) take reasonable steps~~use its reasonable endeavours~~ to ensure that any User who wishes to participate in that Acceptance Testing is able to do so; and

(d) ensure that the version of the software has been subject to a software code review, by an individual or organisation with the professional competence to carry out such a review, for the purpose of identifying any vulnerabilities in the code that were not intended as a feature of its design.

Provision of Support and Assistance to Users

H11.9 The DCC shall, having consulted with Users, determine two Application Servers in respect of which it will provide support for the executable file referred to in Section H11.4(a)(i).

H11.10 Any User may appeal to the Panel a decision of the DCC made under Section H11.9, in which case:

(a) the Panel shall determine the Application Servers in respect of which the DCC must provide support; and

(b) the determination of the Panel shall be final and binding for the purposes of this

Code.

H11.11 The DCC shall make available to each person to whom any version of the Parse and Correlate Software is provided a copy of an installation guide and release notes relevant to that version.

H11.12 Requests by any User for the DCC to provide that User with further assistance in relation to its use or implementation of the Parse and Correlate Software shall be made in such format as the DCC may specify from time to time, and shall be submitted to the DCC. Following receipt of any such request (or purported request), the DCC shall:

(a) where the request is incomplete or the DCC reasonably requires further information in order to assess the request, notify the User that this is the case and provide reasonable assistance to the User in re-submitting its request;

(b) once the DCC has received all the information it reasonably requires in order to assess the request, confirm the reasonable terms upon which the DCC will provide the requested assistance (which terms may not be inconsistent with the provisions of this Code) and the Charges payable in respect of the same; and

(c) once the Party has agreed to such terms and to pay such Charges, provide the requested assistance to the User in accordance with such terms.

H11.13 Section H11.12 does not apply to the provision of assistance that is the responsibility of the DCC in accordance with the Incident Management Policy.The assistance referred to in Section H11.12 may include in particular assistance in respect of:

(a) the development and testing of, and the provision of support for, a version of the Parse and Correlate Software which is capable of operating on a version of the Java Virtual Machine/Run-time Environment other than that prevailing at the time at which the design of the most recently released version of the Parse and Correlate Software was finalised;

(b) the development and testing of, and the provision of support for, a version of the Parse and Correlate Software which meets any other User-specific

requirements; and

(c) the provision, in respect of more than two Application Servers, of support for the executable file referred to in Section H11.4(a)(i).

Separation of Resources

H11.14 The DCC shall ensure that no staff or other resources of its own or of any third party which are directly used in the development of the Parse and Correlate Software are resources which are also used in the development or provision of the Transform functionality.

Right to Use the Parse and Correlate Software

H11.15 The DCC shall ensure that any person shall have the right to use the Parse and Correlate Software source software code on a non-proprietary and royalty-free basis, except insofar as royalties are due in respect of any Intellectual Property Rights the use of which is mandated by the Code.

H12 INTIMATE COMMUNICATIONS HUB INTERFACE SPECIFICATION

Maintenance of the ICHIS

H12.1 The DCC shall maintain the ICHIS and ensure that the ICHIS meets the requirements of Section H12.2 and H12.3.

H12.2 The requirements of this Section H12.2 are that the ICHIS describes a specification for the physical interface (including the electrical and data connection) between:

(a) the Communications Hub (which shall incorporate the male components of the physical interface); and

(b) either a Smart Meter or a Communications Hub Hot Shoe (which shall, in either case, incorporate the female components of the physical interface).

H12.3 The requirement of this Section H12.3 is that the specification described by the ICHIS only requires the use of tangible and intangible property (including physical components and Intellectual Property Rights) that is readily available on a reasonable and non-discriminatory basis.

Publication of the ICHIS

H12.4 The DCC shall publish the ICHIS on the DCC Website, and ensure that all persons are free to use the ICHIS without charge (whether for the purposes of this Code or otherwise); provided that the DCC shall limit its liability to persons other than the Parties on the same terms as apply in respect of the ICHIS under Section M2 (Limitations of Liability).

Consultation Regarding ICHIS

H12.5 The DCC shall keep the ICHIS under review to ascertain whether the ICHIS remains fit for the purposes envisaged by this Code. The DCC may from time to time at its discretion (and shall where directed to do so by the Panel) consult with Parties as to whether they consider that the ICHIS remains fit for the purposes envisaged by this Code.

H12.6 Following each consultation pursuant to Section H12.5, the DCC shall publish on the DCC Website (and notify all Parties of) a report on the outcome of such consultation, setting out:

(a) the process undertaken in respect of such consultation;

(b) whether (and, if so, how and from what implementation date) the DCC proposes to amend the ICHIS as a result of such consultation;

(c) a detailed summary of the consultation responses received from Parties, identifying in particular those responses that raised objections to the position adopted by the DCC;

(d) the DCC's rationale for the position it has adopted;

(e) the costs and expenses that are likely to arise as a result of the position adopted by the DCC (including the costs and expenses likely to arise as a result of any modifications that will be required to be made to Smart Meters, Communications Hubs and Communications Hub Hot Shoes); and

(f) the steps it has taken (including any testing or prototype development) to ensure that the ICHIS (if amended as proposed) remains fit for the purposes envisaged by this Code.

Referral to the Authority

H12.7 Within 10 Working Days following notification by the DCC to a Party of a report published in accordance with Section H12.6, that Party may refer the report to the Authority to consider whether the consultation to which that report relates was undertaken in accordance with the DCC's obligations under this Code or whether the notice period provided for implementation of the amendment was reasonable given the circumstances.

H12.8 Where the Authority determines that the relevant consultation was not undertaken in accordance with the DCC's obligations under this Code or that the notice period provided for implementation of the amendment was not reasonable given the

circumstances, the DCC shall repeat the consultation and comply with any directions made by the Authority in respect of the same. Where the Authority determines both (where both of the following were referred to the Authority) or either (where only one of the following was so referred) that:

(a) the relevant consultation was undertaken in accordance with the DCC's obligations under this Code; and/or

(b) the notice period provided for implementation of the amendment was reasonable given the circumstances,

the consultation and proposed course of action shall stand.

Amendments to the ICHIS

H12.9 No amendment may be made to the ICHIS unless:

(a) the DCC has first undertaken such prototype development and testing in respect of the proposed amendment as the DCC reasonably considers necessary to ensure that the ICHIS is fit for the purposes envisaged by this Code;

(b) the DCC has first consulted with Parties regarding the proposed amendment and proposed date of implementation, published a report on the outcome of such consultation, and notified the Parties of such publication (all in accordance with Section H12.6); and

(c) such report has not been referred to the Authority in accordance with Section H12.7, or the Authority has determined both (where both of the following were so referred) or either (where only one of the following was so referred) that:

(i) the relevant consultation was undertaken in accordance with the DCC's obligations under this Code; and/or

(ii) the notice period provided for implementation of the amendment was reasonable given the circumstances.

H13 PERFORMANCE STANDARDS AND REPORTING

Code Performance Measures

H13.1 Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period):

No.	Code Performance Measure	Performance Measurement Period	Target Service Level	Minimum Service Level
1	Percentage of On-Demand Service Responses delivered within the applicable Target Response Time.	monthly	99%	96%
2	Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time.	monthly	99%	96%
3	Percentage of Alerts delivered within the applicable Target Response Time.	monthly	99%	96%
4	Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.	monthly	100%	85%
5	Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 3, 4 or 5 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.	monthly	90%	80%
6	Percentage of time (in minutes) when the Self-Service Interface is available to be accessed by all Users during the Target Availability Period.	monthly	99.5%	98%

Service Provider Performance Measures

H13.2 The DCC may modify the Reported List of Service Provider Performance Measures where it has:

(a) undertaken reasonable consultation with the Parties regarding the proposed modification;

(b) given due consideration to, and taken into account, any consultation responses received; and

(c) provided to the Panel, the Parties, the Authority and (on request) the Secretary of State a statement of its reasons for the modification together with copies of any consultation responses received,

(d) and as soon as reasonably practicable following any such modification, the DCC shall provide an up-to-date copy of the Reported List of Service Provider Performance Measures to the Panel, the Parties, the Authority and (on request) the Secretary of State.

H13.3 Prior to agreeing any changes to the DCC Service Provider Contracts that will alter the Service Provider Performance Measures, the DCC shall:

(a) undertake reasonable consultation with the Panel and Parties regarding such changes;

(b) give due consideration to, and take into account, any consultation responses received; and

(c) provide to the Panel, the Parties, the Authority and (on request) the Secretary of State a statement of its reasons for proposing to agree such changes.

Reporting

H13.4 The DCC shall, within 25 Working Days following the end of each Performance Measurement Period, produce a report setting out the Service Levels achieved in

respect of each Performance Measure. Such report must identify:

(a) those Performance Measures (if any) for which the Service Level was less than the Target Service Level and/or the Minimum Service Level;

(b) where a Service Level is less than the Target Service Level, the reason for the Service Level achieved;

(c) where a Service Level is less than the Minimum Service Level, the steps the DCC is taking to prevent the re-occurrence or continuation of the reason for the Service Level achieved; and

(d) any anticipated reductions in the DCC's Internal Costs and/or External Costs (as both such expressions are defined in the DCC Licence) arising as a consequence of the DCC Service Providers failing to achieve the Target Service Levels in respect of the Service Provider Performance Measures.

H13.5 A copy of the report produced pursuant to Section H13.4:

(a) shall be provided by DCC, immediately following its production, to the Panel, the Parties, the Authority and (on request) the Secretary of State; and

(b) may be provided by the Panel, at its discretion, to any other person.

Performance Measurement Methodology

H13.6 The DCC shall:

(a) establish and periodically review the Performance Measurement Methodology in accordance with Good Industry Practice and in consultation with the Panel, the Parties and the Authority; and

(b) as soon as reasonably practicable following any modification which it may make to the Performance Measurement Methodology, provide an up to date copy of the Performance Measurement Methodology to the Panel, the Parties, the Authority and (on request) the Secretary of State.

H14 TESTING SERVICES

General Testing Requirements

H14.1 The DCC shall provide the following testing services (the "**Testing Services**"):

(a) User Entry Process Tests;

(b) SMKI and Repository Entry Process Tests;

(c) Device and User System Tests;

(d) Modification Proposal implementation testing (as described in Section H14.34); and

(e) DCC Internal Systems change testing (as described in Section H14.36).

H14.2 The DCC shall make the Testing Services available, and shall provide the Testing Services:

(a) in accordance with the Enduring Testing Approach Document and Good Industry Practice; and

(b) between 08:00 hours and 18.00 hours Monday to Friday, and at any other time that it is reasonably practicable to do so (including where any DCC Service Provider has agreed to provide services at such time).

H14.3 The DCC shall act reasonably in relation to its provision of the Testing Services and shall facilitate the completion (in a timely manner) of tests pursuant to the Testing Services by each such person which is entitled to do so in accordance with this Section H14. Each Testing Participant shall comply with the Enduring Testing Approach Document with respect to the relevant Testing Services. The DCC shall publish on the DCC Website a guide for Testing Participants describing which persons are eligible for which Testing Services, and on what basis (including any applicable Charges).

H14.4 To the extent it is reasonably practicable to do so, the DCC shall allow persons who are eligible to undertake tests pursuant to the Testing Services to undertake those tests

concurrently, or shall (otherwise) determine, in a non-discriminatory manner, the order in which such persons will be allowed to undertake such tests. Where any Testing Participant disputes the order in which persons are allowed to undertake tests pursuant to this Section H14.4, then the Testing Participant may refer the matter to the Panel. Where the DCC or any Testing Participant wishes to do so, it may refer the Panel's decision on such matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.5 Each Party which undertakes tests pursuant to the Testing Services shall do so in accordance with Good Industry Practice. To the extent that such tests involve a Party accessing the DCC's premises, the Party shall do so in compliance with the site rules and reasonable instructions of the DCC.

H14.6 The DCC shall be liable for any loss of or damage to the equipment of Testing Participants (fair wear and tear excepted) that occurs while such equipment is within the DCC's possession or control pursuant to the Testing Services; save to the extent that such loss or damage is caused by a breach of this Code (or the equivalent agreement under Section H14.7) by the Testing Participant.

H14.7 Where (in accordance with this Section H14) a person that is not a Party is eligible to undertake a category of Testing Services as a Testing Participant, the DCC shall not provide those Testing Services to that person unless it is bound by an agreement entered into with the DCC pursuant to this Section H14.7. Where a person who is a Testing Participant (but not a Party) requests a Testing Service, the DCC shall offer terms upon which such Testing Service will be provided. Such offer shall be provided as soon as reasonably practicable after receipt of the request, and shall be based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances).

General: Forecasting

H14.8 Each Testing Participant shall provide the DCC with as much prior notice as is reasonably practicable of that Testing Participant's intention to use any of the following Testing Services: User Entry Process Tests, SMKI and Repository Entry

Process Tests, and Device and User System Tests.

General: Systems and Devices

H14.9 The DCC shall provide such facilities as are reasonably required in relation to the Testing Services, including providing:

(a) for access to the Testing Services either at physical test laboratories and/or remotely; and

(b) a reasonable number of Devices for use by Testing Participants at the DCC's physical test laboratories which Devices are to be of the same Device Models as those selected pursuant to the Device Selection Methodology and/or such other Device Models as the Panel approves from time to time (provided that, where Test Stubs (or other alternative arrangements) were used then such Tests Stubs (or other alternative arrangements) will be used in place of Devices until the DCC agrees with the Panel which Device Models to use).

H14.10 Without prejudice to Section H14.9(b), the DCC shall allow Testing Participants to use Devices they have procured themselves when using the Testing Services. The DCC shall make storage facilities available at the DCC's physical test laboratories for the temporary storage by Testing Participants of such Devices (for no more than 30 days before and no more than 30 days after completion of the Testing Service for which such Devices may be expected to be used). The DCC shall ensure that such storage facilities are secure and only capable of access by persons authorised by the relevant Testing Participant.

General: SMKI Test Certificates

H14.11 The following shall apply in relation to Test Certificates:

(a) the DCC shall, in accordance with the Enduring Testing Approach Document, issue and make available to Testing Participants copies of such Test Certificates as are reasonably necessary for the purposes of the Testing Participants undertaking Testing Services and testing pursuant to Section T (Testing During

Transition);

(b) the DCC shall only use Test Certificates for the purposes envisaged by this Section H14.11 (and shall not use actual Certificates when providing the Testing Services or undertaking tests pursuant to Section T (Testing During Transition), except to such extent as is approved, and subject to any conditions imposed, by the SMKI PMA);

(c) each Testing Participant to which Test Certificates are made available pursuant to this Section H14.11 shall only use those Test Certificates for the purposes for which such Test Certificates are made available (and shall not use actual Certificates when undertaking the tests referred to in this Section H14.11);

(d) each Testing Participant to which Test Certificates are made available pursuant to this Section H14.11 shall be entitled to make those certificates available to others provided that such others only use them for the purposes for which such certificates were made available to the Testing Participant;

(e) the DCC shall ensure that the Test Certificates are clearly distinguishable from actual Certificates; and

(f) the DCC shall act in accordance with Good Industry Practice in providing the Test Certificates;

(g) each Testing Participant shall act in accordance with Good Industry Practice in using the Test Certificates; and

(h) each Testing Participant hereby, subject to Section M2.1 (Unlimited Liabilities):

(i) waives all rights, remedies and claims it would otherwise have (whether for breach of contract, in tort or delict or otherwise) against the DCC in respect of the Test Certificates;

(ii) undertakes not to bring any claim against the DCC in respect of the Test Certificates; and

(iii) where it makes the Test Certificates available to others, undertakes to ensure that no such others bring any claim against the DCC in respect of such Test Certificates.

User Entry Process Tests

H14.12 Parties seeking to become Users in accordance with Section H1 (User Entry Process) are entitled to undertake User Entry Process Tests.

H14.13 In respect of a Party seeking to become eligible as a User in a particular User Role, the purpose of the User Entry Process Tests is to test the capability of that Party and the Party's Systems to interoperate with the DCC and the DCC System, to the extent necessary in order that the Party:

(a) has established a connection to the DCC User Interface via the Party's chosen DCC Gateway Connection;

(b) can use the DCC User Interface for the purposes set out in Section H3.3 (Communications to be sent via DCC User Interface) in respect of the Services for which Users in that User Role are eligible; and

(c) can use the Self-Service Interface for the purposes set out in Section H8 (Service Management, Self-Service Interface and Service Desk).

H14.14 The User Entry Process Tests will:

(a) test the sending of communications from the proposed User System via the DCC System to be received by Devices and from Devices via the DCC System to be received by the proposed User System, recognising that such tests may involve a simulation of those Systems rather than the actual Systems;

(b) be undertaken in accordance with the Common Test Scenarios Document; and

(c) be undertaken using Devices selected and provided by the DCC as referred to in Section H14.9(b).

H14.15 Only Parties who the DCC considers meet any entry requirements (for a particular

User Role) set out in the Common Test Scenarios Document shall be entitled to undertake the User Entry Process Tests for that User Role.

H14.16 Where the DCC is not satisfied that a Party meets such entry requirements (for a particular User Role), that Party may refer the matter to the Panel for its determination. Where the Party disagrees with any such determination of the Panel, then the Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.17 Each Party seeking to undertake the User Entry Process Tests shall develop its own test scripts and demonstrate how those test scripts meet the requirements of the relevant scenarios set out in the Common Test Scenarios Document. Each Party shall obtain the DCC's approval that such test scripts meet those requirements before the User Entry Process Tests can commence. Any disputes regarding the approval of such test scripts may be referred to the Panel for determination (which determination shall be final and binding for the purposes of this Code).

H14.18 Each Party will have the right to determine the sequencing of the tests that comprise the User Entry Process Tests; save to the extent that a particular sequence is mandated in the Common Test Scenarios Document.

H14.18A The DCC or the Party undertaking the User Entry Process Tests may suspend testing in accordance with the requirements set out in the Common Test Scenarios Document. Any dispute between the DCC and a Party regarding the suspension (or consequent resumption) of such testing may be referred to the Panel for its determination. Where the DCC or the Party disagrees with any such determination of the Panel, then the DCC or the Party may refer the matter to the Authority for its determination (which determination shall be final and binding for the purposes of this Code).

H14.19 A Party will have successfully completed the User Entry Process Tests (for a particular User Role), once the DCC considers that the Party has demonstrated that it has satisfied the requirements set out in the Common Test Scenarios Document for that User Role. Where requested by a Party, the DCC shall provide written

confirmation to the Party confirming whether or not the DCC considers that the Party has successfully completed the User Entry Process Tests (for a particular User Role).

H14.20 Where Systems have been proven to meet the requirements of this Code as part of one Party's successful completion of the User Entry Process Tests or tests under Section H14.32 that are equivalent to all or part of the User Entry Process Tests (and where the substance of the relevant part of the User Entry Process Tests have not changed in the interim), then:

(a) any Party that has use of those Systems shall be entitled to submit proof to the DCC that this is the case when seeking to meet any applicable entry and/or exit requirements set out in the Common Test Scenarios Document; and

(b) the DCC shall take into account such proof when considering whether such Party meets such entry and/or exit requirements.

H14.21 Where the DCC is not satisfied that a Party has successfully completed the User Entry Process Tests (for a particular User Role), that Party may refer the matter to the Panel for its determination. Where the Party disagrees with any such determination of the Panel, then the Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

SMKI and Repository Entry Process Tests

H14.22 Each Party or Registration Data Provider seeking to complete the entry process described in Section L7 (SMKI and Repository Entry Process Tests) is entitled to undertake the SMKI and Repository Entry Process Tests to become either or both of:

(a) an Authorised Subscriber under either or both of the Organisation Certificate Policy and/or the Device Certificate Policy; and/or

(b) eligible to access the SMKI Repository.

H14.23 The SMKI and Repository Entry Process Tests will be undertaken in accordance with the SMKI and Repository Test Scenarios Document.

H14.24 A Testing Participant seeking to undertake the SMKI and Repository Entry Process Tests for the purposes of either or both of Section H14.22(a) and/or (b) shall notify the DCC of the purposes for which it is undertaking those tests. Only Testing Participants that meet any applicable entry requirements set out in the SMKI and Repository Tests Scenarios Document shall be entitled to undertake those SMKI and Repository Entry Process Tests for the purposes described in Section H14.22(a) and/or (b).

H14.25 Where the DCC is not satisfied that a Testing Participant meets such entry requirements, that Testing Participant may refer the matter to the Panel for its determination. Where the Testing Participant disagrees with any such determination of the Panel, then the Testing Participant may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.26 Each Testing Participant seeking to undertake the SMKI and Repository Entry Process Tests shall develop its own test scripts and demonstrate how those test scripts meet the requirements of the relevant scenarios set out in the SMKI and Repository Tests Scenarios Document (for the purposes described in Section H14.22(a) and/or (b), as applicable). Each Testing Participant shall obtain the DCC's approval that such test scripts meet those requirements before the SMKI and Repository Entry Process Tests can commence. Any disputes regarding the approval of such test scripts may be referred to the Panel for determination (which determination shall be final and binding for the purposes of this Code).

H14.27 Each Testing Participant seeking to undertake the tests will have the right to determine the sequencing of the tests that comprise the SMKI and Repository Entry Process Tests; save to the extent that a particular sequence is mandated in the SMKI and Repository Tests Scenarios Document.

H14.27A The DCC or the Testing Participant undertaking the SMKI and Repository Entry Process Tests may suspend testing in accordance with the requirements set out in the SMKI and Repository Test Scenarios Document. Any dispute between the DCC and a Testing Participant regarding the suspension (or consequent resumption) of such testing may be referred to the Panel for its determination. Where the DCC or the

Testing Participant disagrees with any such determination of the Panel, then the DCC or the Testing Participant may refer the matter to the Authority for its determination (which determination shall be final and binding for the purposes of this Code).

H14.28 A Testing Participant will have successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable), once the DCC considers that the Testing Participant has demonstrated that it has satisfied the requirements set out in the SMKI and Repository Tests Scenarios Document for those purposes. Where requested by a Testing Participant, the DCC shall provide written confirmation to the Testing Participant confirming whether or not the DCC considers that the Testing Participant has successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable).

H14.29 Where Systems have been proven to meet the requirements of this Code as part of one Testing Participant's successful completion of the SMKI and Repository Entry Process Tests or tests under Section H14.32 that are equivalent to all or part of the SMKI and Repository Entry Process Tests (and where the substance of the relevant part of the SMKI and Repository Entry Process Tests have not changed in the interim), then:

(a) any Testing Participant that has use of those Systems shall be entitled to submit proof to the DCC that this is the case when seeking to meet any applicable entry and/or exit requirements set out in the SMKI and Repository Tests Scenarios Document; and

(b) the DCC shall take into account such proof when considering whether such Testing Participant meets such entry and/or exit requirements.

H14.30 Where the DCC is not satisfied that a Testing Participant has successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable), that Testing Participant may refer the matter to the Panel for its determination. Where the Testing Participant disagrees with any such determination of the Panel, then the Testing Participant may refer the matter to the

Authority for its determination (which shall be final and binding for the purposes of this Code).

Device and User System Tests

H14.31 The DCC shall provide a service to enable Testing Participants:

(a) to test the interoperability of Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs provided as part of the Testing Services, such that those Devices are able to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification;

(b) to test the interoperability of User Systems with the DCC Systems, including via the DCC User Interface and the Self-Service Interface; and

(c) to test simultaneously the interoperability of User Systems and Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs provided as part of the Testing Services,

which Testing Services in respect of (a) and (c) above shall (subject to the Testing Participant agreeing to pay any applicable Charges, as further described in the Enduring Testing Approach Document) include the provision of a connection to a simulation of the SM WAN for the purpose of such tests as further described in the Enduring Testing Approach Document (save to the extent the connection is required where the DCC is relieved from its obligation to provide Communication Services pursuant to the Statement of Service Exemptions). References to particular Systems in this Section H14.31 may include a simulation of those Systems (rather than the actual Systems).

H14.32 Each Party is eligible to undertake Device and User System Tests. Any Manufacturer (whether or not a Party) is eligible to undertake those Device and User System Tests described in Section H14.31(a); provided that, in the case of any such tests that require the use of a DCC Gateway Connection, the Manufacturer must be a Party. Any person providing (or seeking to provide) goods or services to Parties or Manufacturers in

respect of Devices is eligible to undertake those Device and User System Tests described in Section H14.31(a); provided that, in the case of any such tests that require the use of a DCC Gateway Connection, the person must be a Party. A Party undertaking the Device and User System Tests described in Section H14.31(b) is entitled to undertake tests equivalent to any or all of the User Entry Process Tests and SMKI and Repository Entry Process Tests, in respect of which:

(a) the DCC shall, at the Party's request, assess whether the test results would meet the requirements of all or part of the applicable User Entry Process Tests and/or SMKI and Repository Entry Process Tests;

(b) the DCC shall, at the Party's request, provide a written statement confirming the DCC's assessment of whether the test results would meet the requirements of all or part of the applicable tests; and

(c) the Party may, where it disputes the DCC's assessment, refer the matter to the Panel for its determination (which shall be final and binding for the purposes of this Code).

H14.33 The DCC shall, on request by a Testing Participant, offer reasonable additional support to that Testing Participant (subject to such Testing Participant agreeing to pay any applicable Charges) in understanding and resolving issues associated with:

(a) the DCC Total System and the results of such Testing Participant's Device and User System Tests ~~(subject to such Testing Participant agreeing to pay any applicable Charges)~~;

(b) where the Testing Participant is a Party, the Systems of the Testing Participant that are (or are intended to be) User Systems; and/or

~~(a)~~(c) communications between the DCC and any Device or between Devices which comprise (or which the Testing Participant intends will comprise) a Smart Metering System.

H14.33A The~~Such~~ additional Testing Services provided for in Section H14.33 are without prejudice to the DCC's obligations in respect of Testing Issues, Incidents and Problems.

Modification Implementation Testing

H14.34 Where the Panel determines, in accordance with Section D10 (Implementation), that testing is required in relation to the implementation of a Modification Proposal, then such testing shall be undertaken as a Testing Service pursuant to this Section H14.34 and the implementation timetable approved in accordance with Section D10 (Implementation).

H14.35 The persons eligible to participate in such testing shall be determined by the Panel in accordance with Section D10 (Implementation).

DCC Internal System Change Testing

H14.36 Where, pursuant to Section H8.8 (DCC Internal Systems Changes), a Party or an RDP~~User~~ is involved in testing of changes to the DCC Internal Systems, then such testing shall not be subject to the requirements of Section H14.3, Section H14.4 and Sections H14.6 to H14.11 (inclusive), but such Party or RDP~~a User~~ may nevertheless raise a Testing Issue in respect of the tests (and the references to Testing Participant in Sections H14.37 to H14.44 shall be interpreted accordingly).

General: Testing Issue Resolution Process

H14.37 Each Testing Participant undertaking tests pursuant to this Section H14 is entitled to raise a Testing Issue in respect of those tests. Each Testing Participant shall take reasonable steps to diagnose and resolve a Testing Issue before raising it in accordance with this Section H14.

H14.38 A Testing Participant that wishes to raise a Testing Issue shall raise it with the relevant DCC Service Provider (as identified by the DCC from time to time) in accordance with a reasonable and not unduly discriminatory procedure, which is to be established by the DCC and provided to the Panel from time to time (which the Panel

shall publish on the Website).

H14.39 Where a Testing Participant raises a Testing Issue, the DCC shall ensure that the relevant DCC Service Provider shall (as soon as reasonably practicable thereafter):

(a) determine the severity level and priority status of the Testing Issue;

(b) inform the Testing Participant of a reasonable timetable for resolution of the Testing Issue consistent with its severity level and priority status; and

(c) provide its determination (in accordance with such timetable) to the Testing Participant on the actions (if any) to be taken to resolve the Testing Issue.

H14.40 Pursuant to H14.39, the DCC shall share with categories of Testing Participant any information (provided that the identities of the Testing Participant and, where relevant, the Device's Manufacturer are anonymised) relating to the Testing Issue which is likely to be of use to those categories of Testing Participants (provided that no such information should be shared to the extent it poses a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices).

H14.41 Where a Testing Participant is dissatisfied with any of the determinations under Section H14.39 (or the speed with which any such determination is made), the Testing Participant may refer the matter to the DCC. On such a referral to the DCC, the DCC shall (as soon as reasonably practicable thereafter):

(a) consult with the Testing Participant and any other person as the DCC considers appropriate;

(b) either, depending on the subject matter of the disagreement:

(i) direct the DCC Service Provider to more quickly provide its determination of the matters set out in Section H14.39(a), (b) and/or (c); or

(ii) make the DCC's own determination of the matters set out in Section H14.39(a), (b) and/or (c);

(c) notify the Panel of the DCC's direction or determination under (b) above; and

(d) share with categories of Testing Participant any information (provided that the identities of the Testing Participant and, where relevant, the Device's Manufacturer are anonymised) relating to the Testing Issue which is likely to be of use to those categories of Testing Participants (provided that no such information should be shared to the extent it poses a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices).

H14.42 Where the Testing Participant (or any Party) disagrees with the DCC's determination pursuant to Section H14.41 of the matters set out at Section H14.39(c) (but not otherwise), then the Testing Participant (or Party) may request that the DCC refers the matter to the Panel for its consideration (provided that the identities of the Testing Participant and, where relevant, the Device's Manufacturer are anonymised).

H14.43 Where a matter is referred to the Panel for its consideration pursuant to Section H14.42, the Panel shall consider the matter further to decide upon the actions (if any) to be taken to resolve the Testing Issue, unless the matter relates to testing undertaken pursuant to Section T (Testing During Transition), in which case the Panel shall notify the Secretary of State and shall consider the matter further and make such a decision only where, having received such a notification, the Secretary of State so directs. Where the Panel considers the matter further, it may conduct such further consultation as it considers appropriate before making such a decision. Such a decision may include a decision that:

(a) an aspect of the Code could be amended to better facilitate achievement of the SEC Objectives;

(b) an aspect of the DCC Systems is inconsistent with the requirements of this Code;

(c) an aspect of one or more Devices is inconsistent with the requirements of this Code; or

(d) an aspect of the User Systems or the RDP Systems is inconsistent with the

requirements of this Code.

H14.44 The Panel shall publish each of its decisions under Section H14.43 on the Website; provided that the identities of the Testing Participant and (where relevant) the Device's Manufacturer are anonymised, and that the Panel shall remove or redact information where it considers that publishing such information would be prejudicial to the interests of one or more Parties, or pose a risk of Compromise to the DCC Total System, User Systems, RDP Systems and/or Devices.

H14.45 A decision of the Panel under Section H14.43 is merely intended to facilitate resolution of the relevant Testing Issue. A decision of the Panel under Section H14.43 is without prejudice to any future decision by the Change Board and/or the Authority concerning a Modification Proposal, by the Secretary of State in exercising its powers under section 88 of the Energy Act 2008, by the Authority concerning the DCC's compliance with the DCC Licence, or by the Panel under Section M8 (Suspension, Expulsion and Withdrawal).

H15 DCC GATEWAY CONNECTIONS

Obligation to Maintain DCC Gateway Connections

H15.1 The DCC shall maintain each DCC Gateway Connection and make it available subject to and in accordance with the provisions of this Section H15.

H15.2 The DCC shall ensure that each DCC Gateway Connection is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3).

H15.3 No Party may use a DCC Gateway Connection for any purposes other than accessing, and sending and receiving Data via, the DCC Interfaces (and subject to the provisions of this Code applicable to each DCC Interface).

Requests for DCC Gateway Connections

H15.4 Each Party other than the DCC may request (in accordance with this Section H15 and as further described in the DCC Gateway Code of Connection) as many DCC Gateway Connections as the Party wishes, in each case using the DCC Gateway Bandwidth Option of the Party's choice.

H15.5 In order to assist a Party in determining which DCC Gateway Bandwidth Option to request (or, in the case of connections using a DCC Gateway HV Connection, the size of the bandwidth required), the DCC shall (on request) provide any Party with information regarding the size of the different message types that can be sent via the DCC User Interface.

H15.6 Within 5 Working Days following receipt of any request from a Party for a DCC Gateway Connection at a premises, the DCC shall:

(a) where the request does not include all the information required in accordance with the DCC Gateway Connection Code of Connection, notify the Party that this is the case and provide reasonable assistance to the Party in re-submitting its request; or

(b) undertake a desk-based assessment as described in the DCC Gateway

Connection Code of Connection, and provide a response to the Party in respect of that premises under Section H15.7, H15.8 or H15.9 (as applicable).

H15.7 In the case of a request for a DCC Gateway LV Connection, and where the DCC's desk-based assessment indicates that a physical site assessment is not required, the DCC shall provide an offer to the Party setting out:

(a) the DCC's reasonable estimate of the likely bandwidth of the connection once made;

(b) the date from which the DCC will provide the connection;

(c) the connection Charges and annual Charges that will apply in respect of the connection; and

(d) the connection period for which the connection will be made available.

H15.8 In the case of a request for a DCC Gateway LV Connection, and where the DCC's desk-based assessment indicates that a physical site assessment is required, the DCC shall notify the requesting Party that this is the case, and (unless the DCC is not reasonably able to do so without undertaking a physical site assessment, and subject to further information which may become available as a result of the physical site assessment) notify the Party of:

(a) the DCC's reasonable estimate of the likely bandwidth of the connection once made;

(b) the date from which the DCC will provide the connection;

(c) the connection Charges and annual Charges that will apply in respect of the connection; and

(d) the connection period for which the connection will be made available.

H15.9 In the case of a request for a DCC Gateway HV Connection, the DCC shall notify the Party that a physical site assessment is required, and (unless the DCC is not reasonably able to do so without undertaking a physical site assessment, and subject to

further information which may become available as a result of the physical site assessment) notify the Party of:

(a) the date from which the DCC will provide the connection;

(b) the connection Charges and annual Charges that will apply in respect of the connection; and

(c) the connection period for which the connection will be made available.

Physical Site Assessments

H15.10 In the case of a notice to a Party under Section H15.8 or H15.9, the Party has 30 days following receipt of such notice to confirm to the DCC that the Party wishes the DCC to proceed with the physical site assessment. In the absence of such confirmation, the Party shall be deemed to have opted not to proceed.

H15.11 Where the DCC has received a confirmation in accordance with Section H15.10, then the DCC shall, within 30 days thereafter, complete the physical site assessment. The Party requesting the connection shall ensure that the DCC has such access to the Party's premises as the DCC may reasonably require in order to undertake such site assessment. The DCC shall ensure that all persons exercising such rights of access do so in compliance with the applicable site rules and reasonable instructions of those in control of the premises.

H15.12 The DCC shall, within 10 Working Days after completing a physical site assessment pursuant to Section H15.11, provide an offer to the Party that requested a connection at that premises setting out:

(a) any supplementary conditions which will apply in respect of the connection (in addition to the provisions of this Code) required as a consequence of matters identified in the site assessment;

(b) (in the case of DCC Gateway LV Connections) the DCC's reasonable estimate of the likely bandwidth of the connection once made;

(c) the date from which the DCC will provide the connection;

(d) the connection Charges and annual Charges that will apply in respect of the connection; and

(e) the connection period for which the connection will be made available.

Initial Provision of a DCC Gateway Connection

H15.13 In the case of an offer to a Party under Section H15.7 or H15.12, the Party has 30 days following receipt of such offer to confirm to the DCC that the Party accepts that offer. In the absence of such confirmation, the Party shall be deemed to have opted not to accept the offer (which shall lapse).

H15.14 Where a Party accepts an offer as described in Section H15.13, the DCC shall take all reasonable steps to provide the requested DCC Gateway LV Connection or DCC Gateway HV Connection by the date set out in the accepted offer (subject to payment of any applicable Charges).

H15.15 In the event that the DCC will be delayed in providing the requested DCC Gateway Connection, the DCC shall notify the relevant Party of the delay (including reasons for the delay) and of the revised connection date (being as soon a reasonably practicable thereafter), and shall take all reasonable steps to provide the requested connection by that revised date.

Use of a DCC Gateway Connection

H15.16 Subject to Section H15.3, the Party that requested a DCC Gateway Connection at a premises shall be entitled to use that connection for as long as the DCC is obliged to make it available in accordance with Section H15.18 (provided that such Party may transfer its right in respect of that DCC Gateway Connection to another Party on both such Parties giving notice to the DCC referring to this Section H15.16).

H15.17 The DCC Gateway Party may notify the DCC of the other Parties (if any) that are (subject to Section H15.3) entitled to share (or no longer entitled to share) use of that DCC Gateway Connection, and in respect of which DCC Interfaces.

Ongoing Provision of a DCC Gateway Connection

H15.18 Once a DCC Gateway Connection has been established at a premises on behalf of a DCC Gateway Party:

(a) the DCC shall make the connection available to the DCC Gateway Party in accordance with this Code until the DCC Gateway Party notifies the DCC that the Party wishes to cancel the connection (on not less than three months' prior notice);

(b) the DCC shall give the DCC Gateway Party four months' advance notice of the date on which the period of connection referred to in the accepted connection offer is due to expire (or of the date on which any period of extension pursuant to paragraph (c) below is due to expire), and shall at the same time confirm the annual Charges that will apply if the connection is not cancelled;

(c) on the expiry of a period referred to in paragraph (b) above, unless the DCC Gateway Party cancels the connection in accordance with paragraph (a) above, the period of connection shall be extended for a year (which will give rise to an additional annual Charge);

(d) the DCC Gateway Party and the DCC shall comply with the provisions of the DCC Gateway Connection Code of Connection applicable to the DCC Gateway Bandwidth Option utilised at the connection (and the DCC may limit the use of the connection where the DCC Gateway Party fails to do so and where this is provided for in the DCC Gateway Connection Code of Connection);

(e) the DCC shall, on request, provide the DCC Gateway Party with a report on the performance of its connection as further set out in the DCC Gateway Connection Code of Connection; and

(f) in the case of DCC Gateway HV Connections, the DCC Gateway Party may increase or decrease the bandwidth of its connection in accordance with (and subject to the limitation provided in) the DCC Gateway Code of Connection (provided that, in the case of decreases, the applicable Charges may not alter as

a result).

H15.19 The cancellation of any DCC Gateway Connection pursuant to Section H15.18(a), is without prejudice to:

(a) the right of the DCC Gateway Party to apply for another connection under Section H15.4; and

(b) the obligation of the DCC Gateway Party to pay the applicable Charges for the full duration of the period of connection referred to in the accepted connection offer or any period of extension under Section H15.18(c).

DCC Gateway Equipment

H15.20 In first providing a DCC Gateway Connection at a premises, the DCC shall procure that the DCC Gateway Equipment is installed at the relevant premises, and that the DCC Gateway Equipment is installed in accordance with Good Industry Practice and all applicable Laws and Directives.

H15.21 Following its installation at a premises, the DCC shall ensure that the DCC Gateway Equipment is operated and maintained in accordance with Good Industry Practice, and that it complies with all applicable Laws and Directives. The DCC shall maintain a record of the DCC Gateway Equipment installed at each DCC Gateway Party's premises from time to time, and of the point of its connection to that Party's Systems.

H15.22 The DCC Gateway Party at whose premises the DCC Gateway Equipment is (or is to be) installed shall provide the DCC with such access to that premises as the DCC may reasonably require in order to allow it to undertake the installation, maintenance, relocation or removal of the DCC Gateway Equipment. The DCC shall ensure that all persons exercising such rights of access do so in compliance with the site rules and reasonable instructions of the DCC Gateway Party.

H15.23 The DCC Gateway Party at whose premises the DCC Gateway Equipment is (or is to be) installed shall be entitled to witness and inspect the installation, maintenance, relocation or removal of the DCC Gateway Equipment. No such witnessing or

assessment shall relieve the DCC of its obligations under this Code.

H15.24 Each DCC Gateway Party shall ensure that no damage is deliberately or negligently caused to the DCC Gateway Equipment installed at its premises (save that such a Party may take emergency action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property).

H15.25 The DCC Gateway Equipment shall (as between the DCC and each other Party) remain the property of the DCC. The DCC Gateway Equipment is installed at the DCC's risk, and no other Party shall have liability for any loss of or damage to the DCC Gateway Equipment unless and to the extent that such loss or damage arose as a result of that Party's breach of this Code (including that Party's obligations under Section H15.24).

H15.26 No Party other than the DCC shall hold itself out as the owner of the DCC Gateway Equipment, or purport to sell or otherwise dispose of the DCC Gateway Equipment.

H15.27 Where a DCC Gateway Party wishes to alter the location of the DCC Gateway Equipment at the Party's premises, then that Party shall make a request to the DCC, and the DCC shall either (in accordance with any provisions of the DCC Gateway Connection Code of Connection concerning the same):

(a) notify such Party that it is entitled to relocate the DCC Gateway Equipment within the Party's premises, in which case the Party may move such equipment (and, where it does so, it shall do so in accordance with Good Industry Practice and all applicable Laws and Directives); or

(b) notify such Party that the DCC Gateway Equipment must be relocated by the DCC, in which case the DCC shall (subject to payment of any applicable Charges) move the DCC Gateway Equipment in accordance with Good Industry Practice and all applicable Laws and Directives.

H15.28 Where the DCC's obligation to make a DCC Gateway Connection available ends in accordance with Section H15.18(a) or the DCC Gateway Party for a DCC Gateway Connection ceases to be a Party in accordance with Section M8 (Suspension,

Expulsion and Withdrawal), then the DCC shall, within 30 days thereafter:

(a) cease to make that DCC Gateway Connection available; and

(b) remove the DCC Gateway Equipment from the relevant premises in accordance with Good Industry Practice and all applicable Laws and Directives.

DCC Gateway Connection Disputes

H15.29 Where a DCC Gateway Party wishes to raise a dispute in relation to its request for a DCC Gateway Connection (or the extension of its period of connection or increases or decreases in the bandwidth of its connection, in each case under Section H15.18), then the dispute may be referred to the Panel for determination. Where that Party or the DCC disagrees with any such determination, then it may refer the matter to the Authority for its determination, which shall be final and binding for the purposes of this Code.

SECTION I: DATA PRIVACY

I1 DATA PROTECTION AND ACCESS TO DATA

Without Prejudice

I1.1 The obligations of the DCC and each User under this Section I1 are without prejudice to any other obligations they each may have under the Relevant Instruments, including any such obligations they each may have concerning Processing of Personal Data.

User Obligations

Consumption Data

I1.2 Each User undertakes that it will not request, in respect of a Smart Metering System, a Communication Service or Local Command Service that will result in it obtaining Consumption Data, unless:

(a) the User has the Appropriate Permission in respect of that Smart Metering System; and

(b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) the User has, at the point of obtaining Appropriate Permission and at such intervals as are reasonably determined appropriate by the User for the purposes of ensuring that the Energy Consumer is regularly updated of such matters, notified the Energy Consumer in writing of:

(i) the time periods (by reference to length) in respect of which the User obtains or may obtain Consumption Data;

(ii) the purposes for which that Consumption Data is, or may be, used by the User; and

(iii) the Energy Consumer's right to object or withdraw consent (as the case may be) to the User obtaining or using that Consumption Data, and the

process by which the Energy Consumer may object or withdraw consent.

Service Requests

I1.3 Each User undertakes that it will not send either a 'Join Service' or 'Unjoin Service' Service Request (respectively to join a Type 2 Device to, or unjoin it from, any Smart Meter or Device Associated with a Smart Meter) unless:

(a) the User is the Responsible Supplier for the Smart Meter or Associated Device to which the Service Request is sent, and sends that Service Request for the purpose of complying with an obligation under its Energy Supply Licence; or

(b) the Energy Consumer at the premises at which the Smart Meter is located has given the User ~~explicit~~ Explicit ~~consent~~ Consent to join that Type 2 Device to, or unjoin it from (as the case may be), the Smart Meter or Associated Device, and such consent has not been withdrawn.

Access to Records

I1.4 Each User undertakes that it will not access (pursuant to Section H8.16) or request (pursuant to Section H8.17) the information described in Section H8.16(c), unless:

(a) the Energy Consumer at the premises at which the relevant Smart Meter is located has given the User ~~explicit~~ Explicit ~~consent~~ Consent to do so and such consent has not been withdrawn; and

(b) the information is accessed solely for the purpose of its provision to that Energy Consumer.

Good Industry Practice

I1.5 Each User shall put in place and maintain arrangements designed in accordance with Good Industry Practice to ensure that each person from whom it has obtained consent pursuant to Section I1.2 to I1.4 is the Energy Consumer.

Processing of Personal Data by the DCC

I1.6 It is acknowledged that, in providing the Services to a User, the DCC may act in the capacity of 'data processor' (as defined in the Data Protection Act) on behalf of that User in respect of the Personal Data for which that User is the 'data controller' (as defined in the Data Protection Act).

I1.7 The DCC undertakes for the benefit of each User in respect of the Personal Data for which that User is the 'data controller' (as defined in the Data Protection Act) to:

(a) only Process that Personal Data for the purposes permitted by the DCC Licence and this Code;

(b) undertake the Processing of that Personal Data in accordance with this Code, (to the extent consistent with this Code) the instructions of the User and (subject to the foregoing requirements of this Section I1.7(b)) not in a manner that the DCC knows (or should reasonably know) is likely to cause the User to breach its obligations under the Data Protection Act;

(c) implement appropriate technical and organisational measures to protect that Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure (such measures to at least be in accordance with Good Industry Practice and the requirements of Section G (Security));

(d) not Process that Personal Data outside the European Economic Area;

(e) provide reasonable assistance to the User in complying with any subject access request with which the User is obliged to comply under the Data Protection Act and which relates to the Processing of that Personal Data pursuant to this Code;

(f) provide reasonable assistance to the User in complying with any enquiry made, or investigation or assessment initiated, by the Information Commissioner or any other Competent Authority in respect of the Processing of that Personal Data pursuant to this Code;

(g) promptly notify the User in the event that the DCC Processes any of that Personal Data otherwise than in accordance with this Code (including in the event of unauthorised access to such Personal Data);

(h) notify the User of any complaint or subject access request or other request received by the DCC with respect to the Processing of that Personal Data pursuant to this Code, and to do so within 5 Working Days following receipt of the relevant complaint or request; and

(i) notify the User of any a complaint or request relating to the DCC's obligations (if any) under the Data Protection Act in respect of the Processing of that Personal Data pursuant to this Code.

Records

I1.8 The DCC and each User will each maintain in accordance with Good Industry Practice all such records and other information as is necessary to enable the DCC and each such User to demonstrate that it is complying with its respective obligations under Sections I1.2 to I1.5 and I1.7.

I2 OTHER USER PRIVACY AUDITS

Procurement of the Independent Privacy Auditor

I2.1 The Panel shall procure the provision of privacy audit services:

(a) of the scope specified in Section I2.3;

(b) from a person who:

(i) is suitably qualified, and has the necessary experience and expertise, to provide those services; and

(ii) is suitably independent in accordance with Section I2.4,

and that person is referred to in this Section I2 as the "**Independent Privacy Auditor**".

I2.2 Except where the contrary is required by the provisions of Section X (Transition), the Panel may appoint more than one person to carry out the functions of the Independent Privacy Auditor.

Scope of Privacy Audit Services

I2.3 The privacy audit services specified in this Section I2.3 are services in accordance with which, for the purpose of providing reasonable assurance that Other Users are complying with their obligations under Sections I1.2 to I1.5 (User Obligations), the Independent Privacy Auditor shall:

(a) carry out Privacy Assessments at such times and in such manner as is provided for in this Section I2;

(b) produce Privacy Assessment Reports in relation to Other Users that have been the subject of a Privacy Assessment;

(c) receive and consider Privacy Assessment Responses;

(d) otherwise, at the request of, and to an extent determined by, the Panel carry out an assessment of the compliance of any Other User with its obligations under

Sections I1.2 to I1.5;

(e) provide to the Panel such advice and support as may be requested by it from time to time, including in particular advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

(f) provide to the Authority such advice and support as it may request in relation to any disagreements with a decision of the Panel in respect of which the Authority is required to make a determination in accordance with this Section I2; and

(g) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section I2.

Independence Requirement

I2.4 The Independent Privacy Auditor shall be treated as suitably independent in accordance with this Section I2.4 only if it satisfies:

(a) the requirements specified in Section I2.6; and

(b) the requirement specified in Section I2.7.

I2.5 For the purposes of Sections I2.6 and I2.7:

(a) a "**Relevant Party**" means any Party in respect of which the Independent Privacy Auditor carries out functions under this Section I2; and

(b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as an Other User under Section I1.2 to I1.5.

I2.6 The requirements specified in this Section I2.6 are that:

(a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent Privacy

Auditor;

(b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent Privacy Auditor; and

(c) the Independent Privacy Auditor does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the Independent Privacy Auditor where it acts in that capacity).

I2.7 The requirement specified in this Section I2.7 is that the Independent Privacy Auditor is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall include a relationship established by virtue of the Independent Privacy Auditor itself being a Relevant Service Provider to any Relevant Party).

Compliance of the Independent Privacy Auditor

I2.8 The Panel shall be responsible for ensuring that the Independent Privacy Auditor carries out its functions in accordance with the provisions of this Section I2.

Other Users: Duty to Cooperate in Assessment

I2.9 Each Other User shall do all such things as may be reasonably requested by the Panel, or by any person acting on behalf of or at the request of the Panel (including in particular the Independent Privacy Auditor), for the purposes of facilitating an assessment of that Other User's compliance with its obligations under Sections I1.2 to I1.5.

I2.10 For the purposes of Section I2.9, an Other User shall provide the Panel (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;

(b) all such other forms of cooperation as may reasonably be requested, including in particular:

(i) access at all reasonable times to such parts of the premises of that Other User as are used for, and such persons engaged by that Other User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections I1.2 to I1.5; and

(ii) such cooperation as may reasonably by requested by the Independent Privacy Auditor for the purposes of carrying out any Privacy Assessment in accordance with this Section I2.

Categories of Assessment

I2.11 For the purposes of this Section I2, there shall be the following three categories of privacy assessment:

(a) a Full Privacy Assessment (as further described in Section I2.12);

(b) a Random Sample Privacy Assessment (as further described in Section I2.13); and

(c) a Privacy Self-Assessment (as further described in Section I2.14).

I2.12 A "**Full Privacy Assessment**" shall be an assessment carried out by the Independent Privacy Auditor in respect of an Other User to identify the extent to which that Other User:

(a) is compliant with each of its obligations under Sections I1.2 to I1.5; and

(b) has in place the systems and processes necessary for ensuring that it complies with each such obligation.

I2.13 A "**Random Sample Privacy Assessment**" shall be an assessment carried out by the Independent Privacy Auditor in respect of an Other User to identify the extent to

which the Other User is compliant with each of its obligations under Sections I1.2 to I1.5 in relation to a limited (sample) number of Energy Consumers.

I2.14 A " **Privacy Self-Assessment**" shall be an assessment carried out by an Other User to identify the extent to which, since the last occasion on which a Privacy Assessment was carried out in respect of that Other User by the Independent Privacy Auditor, there has been any material change:

(a) in the arrangements that the Other User has in place to comply with its obligations under Sections I1.2 to I1.5; or

(b) in the quantity of Consumption Data being obtained by the Other User.

The Privacy Controls Framework

I2.15 The Panel shall develop and maintain a document to be known as the "**Privacy Controls Framework**" which shall:

(a) set out arrangements designed to ensure that Privacy Assessments are carried out appropriately for the purpose of providing reasonable assurance that Other Users are complying with (or, for the purposes of Section H1.10(d) (User Entry Process Requirements), are capable of complying with) their obligations under Sections I1.2 to I1.5; and

(b) for that purpose, in particular, specify the principles and criteria to be applied in the carrying out of any Privacy Assessment, including principles designed to ensure that Privacy Assessments take place on a consistent basis across all Other Users; and

(c) make provision for determining the timing, frequency and selection of Other Users for the purposes of Random Sample Privacy Assessments.

I2.16 In developing the Privacy Controls Framework, and prior to making any subsequent change to it, the Panel shall consult with and have regard to the views of all Parties, Citizens Advice and Citizens Advice Scotland, and the Authority.

I2.17 The Panel shall ensure that an up to date copy of the Privacy Controls Framework is

made available to all Parties and is published on the Website.

Privacy Assessments: General Procedure

Privacy Controls Framework

I2.18 Each Privacy Assessment carried out by the Independent Privacy Auditor or an Other User shall be carried out in accordance with the Privacy Controls Framework.

The Privacy Assessment Report

I2.19 Following the completion of a Full Privacy Assessment or Random Sample Privacy Assessment, the Independent Privacy Auditor shall, in discussion with the Other User to which the assessment relates, produce a written report (a "**Privacy Assessment Report**") which shall:

(a) set out the findings of the Independent Privacy Auditor on all the matters within the scope of the Privacy Assessment;

(b) specify any instances of actual or potential non-compliance of the Other User with its obligations under Sections I1.2 to I1.5 which have been identified by the Independent Privacy Auditor;

(c) set out the evidence which, in the opinion of the Independent Privacy Auditor, establishes each of the instances of actual or potential non-compliance which it has identified.

I2.20 The Independent Privacy Auditor shall submit a copy of each Privacy Assessment Report to the Panel and to the Other User to which that report relates.

The Privacy Assessment Response

I2.21 Following the receipt by any Other User of a Privacy Assessment Report which relates to it, the Other User shall as soon as reasonably practicable, and in any event by no later than such date as the Panel may specify:

(a) produce a written response to that report (a "**Privacy Assessment Response**") which addresses the findings set out in the report; and

(b) submit a copy of that response to the Panel and the Independent Privacy Auditor.

I2.22 Where a Privacy Assessment Report specifies any instance of actual or potential non-compliance of an Other User with its obligations under Sections I1.2 to I1.5, the Other User shall ensure that its Privacy Assessment Response includes the matters referred to in Section I2.23.

I2.23 The matters referred to in this Section are that the Privacy Assessment Response:

(a) indicates whether the Other User accepts the relevant findings of the Independent Privacy Auditor and provides an explanation of the actual or potential non-compliance that has been identified; and

(b) sets out any steps that the Other User proposes to take in order to remedy and/or mitigate the actual or potential non-compliance, and identifies a timetable within which the Other User proposes to take those steps.

I2.24 Where a Privacy Assessment Response sets out any steps that an Other User proposes to take in accordance with Section I2.23(b), the Panel (having considered the advice of the Independent Privacy Auditor) shall review that response and either:

(a) notify the Other User that it accepts that the steps that the Other User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance specified in the Privacy Assessment Report; or

(b) seek to agree with the Other User such alternative steps and/or timetable as would, in the opinion of the Panel, be more appropriate for that purpose.

I2.25 Where a Privacy Assessment Response sets out any steps that an Other User proposes to take in accordance with Section I2.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Panel, or alternative steps and/or an alternative timetable are agreed between it and the Other User in accordance with Section I2.24, the Other User shall:

(a) take the steps that have been accepted or agreed (as the case may be) within

the timetable that has been accepted or agreed (as the case may be); and

(b) report to the Panel:

(i) on its progress in taking those steps, at any such intervals or by any such dates as the Panel may specify;

(ii) on the completion of those steps in accordance with the timetable; and

(iii) on any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

The Privacy Self-Assessment Report

I2.26 Following the completion of a Privacy Self-Assessment, the Other User which carried out that self-assessment shall as soon as reasonably practicable produce a written report (a "**Privacy Self-Assessment Report**") which shall set out the findings of the Other User, and describe the nature of any material change, since the last occasion on which a Privacy Assessment was carried out in respect of the Other User by the Independent Privacy Auditor, in respect of:

(a) the arrangements that the Other User has in place to comply with its obligations under Sections I1.2 to I1.5; or

(b) the quantity of Consumption Data being obtained by the Other User.

I2.27 A Other User which produced a Privacy Self-Assessment Report shall:

(a) ensure that the report is accurate, complete and not misleading; and

(b) submit a copy of the report to the Panel and the Independent Privacy Auditor.

I2.28 Within the period of time specified in the Privacy Controls Framework following the receipt by it of a Privacy Self-Assessment Report, the Independent Privacy Auditor shall either:

(a) notify the Other User that it accepts that report; or

(b) inform the Other User that it will be subject to an additional Privacy

Assessment of such nature by such date as the Panel may specify.

Initial Full Privacy Assessment: User Entry Process

I2.29 Sections I2.31 to I2.36 set out the applicable privacy requirements referred to in Section H1.10(d) (User Entry Process Requirements).

I2.30 For the purposes of Sections I2.31 to I2.36, any reference in Sections I1.2 to I1.5 or the preceding provisions of this Section I2 to a 'User' or 'Other User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for the User Role of Other User.

Initial Full Privacy Assessment

I2.31 For the purpose of completing the User Entry Process for the User Role of Other User, a Party wishing to act in that User Role shall be subject to a Full Privacy Assessment.

Panel: Setting the Assurance Status

I2.32 Following the receipt by it of the Privacy Assessment Report and Privacy Assessment Response produced after the initial Full Privacy Assessment, the Panel shall promptly consider both documents and set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections I1.2 to I1.5, in accordance with Section I2.33.

I2.33 The Panel shall set the assurance status of the Party as one of the following:

(a) approved;

(b) approved, subject to the Party:

(i) taking such steps as it proposes to take in its Privacy Assessment Response in accordance with Section I2.23(b); or

(ii) both taking such steps and being subject to a further Privacy Assessment of such nature and by such date as the Panel may specify;

(c) provisionally approved, subject to:

(i) the Party having first taken such steps as it proposes to take in its Privacy Assessment Response in accordance with Section I2.23(b) and been subject to a further Privacy Assessment; and

(ii) the Panel having determined that it is satisfied, on the evidence of the further Privacy Assessment, that such steps have been taken; or

(d) deferred, subject to:

(i) the Party amending its Privacy Assessment Response to address any issues identified by the Panel as being, in the opinion of the Panel, not adequately addressed in that response as submitted to Panel; and

(ii) the Panel reconsidering the assurance status in accordance with Section I2.32 in the light of such amendments to the Privacy Assessment Response.

Approval

I2.34 For the purposes of Sections H1.10(d) and H1.11 (User Entry Process Requirements):

(a) a Party shall be considered to have successfully demonstrated that it meets the applicable privacy requirements of this Section I2 when:

(i) the Panel has set its assurance status to 'approved' in accordance with either Section I2.33(a) or (b); or

(ii) the Panel has set its assurance status to 'provisionally approved' in accordance with Section I2.33(c) and the requirements specified in that Section have been met; and

(b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

I2.35 Where the Panel has set the assurance status of a Party to 'approved' subject to one of

the requirements specified in Section I2.33(b), the Party shall take the steps to which that approval is subject.

Disagreement with Panel Decisions

I2.36 Where a Party disagrees with any decision made by the Panel in relation to it under Section I2.33, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Privacy Assessments: Post-User Entry Process

I2.37 Following its initial Full Privacy Assessment for the purposes of the User Entry Process, an Other User shall be subject to annual Privacy Assessments as follows:

(a) in the first year after the year of its initial Full Privacy Assessment, to a Privacy Self-Assessment;

(b) in the immediately following year, to a Privacy Self-Assessment;

(c) in the next following year, to a Full Privacy Assessment; and

(d) in each year thereafter, to a category of Privacy Assessment which repeats the same annual sequence as that of paragraphs (a) to (c),

but these requirements shall be subject to the provisions of Section I2.38.

I2.38 An Other User:

(a) may, on the instruction of the Panel, or otherwise in accordance with the provisions of the Privacy Controls Framework, be subject to a Full Privacy Assessment or Random Sample Privacy Assessment at any time; and

(b) where it is subject to such a Privacy Assessment in a year in which it would otherwise have been required to carry out a Privacy Self-Assessment in accordance with Section I2.37, shall not be required to carry out that self-assessment in that year.

Privacy Self-Assessment

I2.39 Where, in accordance with the requirements of this Section I2, an Other User is subject to a Privacy Self-Assessment in any year, that Other User shall:

(a) carry out the Privacy Self-Assessment during that year;

(b) do so in accordance with the Privacy Controls Framework; and

(c) ensure that the outcome of the Privacy Self-Assessment is documented and is submitted to the Independent Privacy Auditor for review by no later than the date which is 13 months after the date of the commencement of the previous Full Privacy Assessment or (if more recent) Privacy Self-Assessment.

Other Users: Obligation to Pay Explicit Charges

I2.40 Each Other User shall pay to the DCC all applicable Charges in respect of:

(a) all Privacy Assessments (other than Random Sample Privacy Assessments) carried out in relation to it by the Independent Privacy Auditor;

(b) the production by the Independent Privacy Auditor of any Privacy Assessment Reports following such assessments; and

(c) all related activities of the Independent Privacy Auditor in respect of that Other User in accordance with this Section I2.

I2.41 Expenditure incurred in relation to Other Users in respect of the matters described in Section I2.40, and in respect of Random Sample Privacy Assessments, shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

I2.42 For the purposes of Section I2.40 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

(a) the expenditure incurred in respect of the matters described in Section I2.40 that is attributable to individual Other Users, in order to facilitate Explicit Charges designed to pass-through the expenditure to such Other Users pursuant to Section K7 (Determining Explicit Charges); and

(b) any expenditure incurred in respect of:

(i) the matters described in Section I2.40 which cannot reasonably be attributed to an individual Other User; and

(ii) Random Sample Privacy Assessments.

SECTION J: CHARGES

J1 PAYMENT OF CHARGES

Charges

J1.1 Each Party shall pay the Charges to the DCC, which Charges shall be determined in accordance with the Charging Statement applicable from time to time.

Invoicing of Charges

J1.2 Following the end of each month in which one or more Parties incurs Charges in accordance with the Charging Statement, the DCC shall prepare and submit to each such Party one or more invoices or one or more invoices with a separate accompanying statement (in either case, an "**Invoice**") showing:

(a) in respect of all Charges other than the Communications Hub Finance Charges:

(i) the date by which payment is due pursuant to Section J1.5;

(ii) a breakdown (in reasonable detail) of the Charges incurred by that Party in that month;

(iii) subject to Section J1.4, the amount of VAT payable on the above amounts;

(iv) any adjustment required pursuant to Section J1.9; and

(v) the total amount payable by that Party in respect of the above; and

(b) in respect of Communications Hub Finance Charges (such that there is a separate Invoice for the charges relating to each Approved Finance Party):

(i) the date by which payment is due pursuant to Section J1.5;

(ii) a breakdown (in reasonable detail) of the Charges incurred by that Party in that month;

(iii) subject to Section J1.4, the amount of VAT payable on the above amounts;

(iv) any adjustment required pursuant to Section J1.9; and

(v) the total amount payable by that Party in respect of the above.

J1.3 The DCC is not obliged to issue an Invoice to a Party in respect of a month under Section J1.2 where the aggregate Charges incurred by that Party in respect of that month are less than the Minimum Monthly Charge (inclusive of VAT). Where the DCC opts not to issue an Invoice to Party in respect of a month in reliance on this Section J1.3, the DCC shall carry forward the Charges incurred in respect of that month and aggregate them with the Charges incurred by that Party in respect of the following month for the purposes of Section J1.2. Notwithstanding the other provisions of this Section J1.3, the DCC must, in respect of each Party that has incurred Charges in respect of a Regulatory Year, issue at least one Invoice to that Party in respect of that Regulatory Year.

J1.4 The Charges stated in each Invoice shall be stated exclusive of VAT, which shall be added if appropriate at the rate prevailing at the relevant tax point. A Party shall only be required to pay VAT where the DCC provides an appropriate VAT invoice.

Payment of Charges

J1.5 Each Party shall pay the amount set out in an Invoice issued to it by the DCC by the "**Due Date**" for payment; being the later of:

(a) 5 Working Days following receipt of such invoice; and

(b) 8 Working Days following the end of the month to which such invoice relates.

J1.6 Without prejudice to a Party's right to dispute the Charges in accordance with Section J2 (Payment Default and Disputes), each Party shall pay the amount set out in each Invoice addressed to it by the Due Date for such payment regardless of any such dispute. Nevertheless, where the DCC agrees that an Invoice contains a manifest error, the DCC shall cancel that Invoice (which will not therefore be payable) and promptly issue a replacement Invoice.

J1.7 Payments shall be made in pounds sterling by transfer of funds to the credit of the account specified in the Invoice, and shall not be deemed to be made until the amount is available as cleared funds. Each payment shall identify within its reference the Invoice number to which that payment relates. The paying Party shall be responsible for all banking fees associated with the transfer of funds. The DCC shall specify a different account for amounts payable by way of the Communications Hub Finance Charges relating to each Approved Finance Party (separately from amounts payable in relation to each other Approved Finance Party and/or all other Charges). The accounts specified by the DCC for the purposes of amounts payable by way the Communications Hub Finance Charges may be accounts held in the name of the relevant Approved Finance Party.

Estimation of Charges

J1.8 If any information that the DCC requires in order to prepare an Invoice is not available at the time that Invoice is prepared, then the DCC may prepare that Invoice based on its reasonable estimate of that information.

Adjustment of Charges

J1.9 Where:

(a) the DCC prepared an Invoice based on its estimate of any information, and the actual information subsequently becomes available to the DCC;

(b) there is a change to the information used by the DCC to prepare an Invoice (including following a reconciliation or amendment of Registration Data); or

(c) it is agreed (or determined), in accordance with Section J2.4 (Resolution of Payment Default), that there was an error in an Invoice,

then the DCC shall include an adjustment in the next Invoice for the relevant Party to be produced thereafter (or, where no Invoice is due to be produced, the DCC shall produce a separate Invoice for such purpose).

J1.10 Each adjustment to be included pursuant to Section J1.9 shall be:

(a) the difference between the amount included in the previous Invoice, and the

amount that should have been included (being, as applicable, either an additional amount payable to the DCC, or a credit in favour of the relevant Party); plus

(b) interest on the amount of such difference calculated from day-to-day from the Due Date of the previous Invoice to (but excluding) the Due Date of the Invoice in which such adjustment is to be included (compounded monthly).

Interest Rate

J1.11 The interest rate applying for the purposes of Section J1.10 shall be the Non-Default Interest Rate.

Further Supporting Information

J1.12 The DCC shall, where requested by a Party, provide such additional information as that Party may reasonably request regarding the calculation of the Charges payable by that Party.

J2 PAYMENT DEFAULT AND DISPUTES

Notification of Payment Failure

J2.1 Where a Party fails to pay an amount set out in an Invoice by the relevant Due Date, then the DCC shall, on the Working Day following the Due Date, issue a notice to that Party:

(a) setting out the unpaid amount; and

(b) referring to the matters set out in Sections J2.2, J2.4, J2.5, J3.16 (where applicable), and M8.1(d) (Events of Default).

Default Interest

J2.2 Where a Party fails to pay an amount set out in an Invoice by the relevant Due Date, then that Party shall pay interest on that amount at the Default Interest Rate calculated from day-to-day from the Due Date to (but excluding) the date on which payment is made (compounded monthly).

Notification of Payment Disputes

J2.3 Where a Party wishes to dispute any amount set out in an Invoice addressed to it, then that Party shall nevertheless pay the full amount set out in the Invoice by the Due Date, and shall give notice to the DCC of the disputed amount and the reason for the dispute. A Party may not give notice under this Section J2.3 (or otherwise dispute an amount set out in an Invoice) more than 12 months after the Due Date for that Invoice.

Resolution of Payment Disputes

J2.4 Where a Party disputes, in accordance with Section J2.3, any amount set out in an Invoice addressed to it, then:

(a) such Party and the DCC shall each in good faith negotiate to resolve the dispute amicably and as soon as reasonably practicable after it arises;

(b) the DCC shall provide all such evidence in support of its position as the disputing Party may reasonably request, and the DCC shall provide such

evidence within 5 Working Days after such request;

(c) no earlier than 1 Working Day after receipt from the DCC of the information requested under Section J2.4(b) (or, where the DCC does not comply with such request, on the expiry of the period referred to in that Section), the disputing Party may refer the dispute to the Panel, in which case each of the DCC and the disputing Party shall be entitled to provide written submissions in support of its position;

(d) where a dispute is referred to the Panel in accordance with Section J2.4(c), the Panel shall convene a meeting and determine the dispute within 10 Working Days of the reference being made (to which meeting representatives of the disputing Party and the DCC may be invited in accordance with Section C (Governance)); and

(e) where the Panel determines that there has been an overpayment to the DCC, the DCC shall include an adjustment in accordance with Section J1.9(c) to address such overpayment (or comply with any direction of the Panel to repay the relevant amount together with interest at the rate that would have applied had the adjustment been made in accordance with Section J1.9(c)).

J2.5 Section J2.4, and any determination by the Panel pursuant thereto, are without prejudice to the following rights of the Parties:

(a) where the amount set out in an Invoice addressed to a Party is disputed on the grounds of whether or not the Charges were calculated and levied in accordance with the Charging Methodology and the Charging Statement, then either of that Party or the DCC may refer the matter to the Authority for determination pursuant to Condition 20 of the DCC Licence; or

(b) where the amount set out in an Invoice addressed to a Party is disputed on any other grounds, then either of that Party or the DCC may refer the matter to arbitration in accordance with Section M7 (Dispute Resolution).

Pursuing Non-Payment

J2.6 Where the DCC has served a notice in accordance with Section J2.1 in respect of

Charges payable by a Party, and such Charges have not been paid within three (3) Working Days following that notice, the DCC shall:

(a) as required by Section M8.2 (Notification of Events of Default), notify the Panel that an Event of Default has occurred in respect of that Party under Section M8.1(d); and

(b) the DCC shall take all reasonable steps and proceedings (in consultation with the Panel) to pursue and recover the unpaid amount (together with interest), unless and until the Panel (whether on the application of the DCC or otherwise) determines that it would not be worthwhile to do so in the circumstances (having regard to, amongst other things, the DCC's duties under part D of Condition 11 of the DCC Licence).

J2.7 Any Party may appeal the decision of the Panel under Section J2.6 to the Authority, and the DCC shall comply with any decision of the Authority in respect of such matter (which shall be final and binding, but without prejudice to the Panel's ability to make a further decision under Section J2.6 following a material change in circumstances).

Records

J2.8 Without prejudice to any other requirements under Laws or Directives, the DCC shall maintain records of each Invoice (together with reasonable supporting evidence for the Charges levied in the Invoice) for a period of at least 18 months following the date of the Invoice.

J3 CREDIT COVER

Obligation to Provide Credit Support

J3.1 Each Party shall procure that one or more of the following forms of Credit Support is delivered to the DCC, and thereafter maintained, such that the aggregate value of such Credit Support is equal to or greater than that Party's Credit Cover Requirement (as notified by the DCC to the Party from time to time):

(a) a Bank Guarantee;

(b) a Letter of Credit; and/or

(c) a Cash Deposit.

Calculation of Credit Cover Requirement

J3.2 The DCC shall calculate each Party's "**Credit Cover Requirement**" from time to time (and at least once a week) as follows:

(a) the Party's Value at Risk; multiplied by

(b) the Party's Credit Cover Factor,

provided that, where a Party's Credit Cover Requirement would otherwise be equal to or less than the Credit Cover Threshold, the Party's Credit Cover Requirement shall be deemed to be zero. Except where the Party's Credit Cover Requirement is zero (or deemed to be zero), the DCC shall notify each Party of the Credit Cover Requirement calculated in respect of that Party (and of the Value at Risk and Credit Cover Factor used in that calculation).

Party's Value at Risk

J3.3 Each Party's "**Value at Risk**" shall be calculated as the sum of:

(a) the Charges (inclusive of VAT) set out in Invoices addressed to, but not yet paid by, the Party; plus

(b) the Charges (inclusive of VAT) that the DCC reasonably estimates are likely to be incurred by the Party in the period until the next Invoice for that Party is

due to be produced by the DCC.

Party's Credit Cover Factor

J3.4 Each Party's "**Credit Cover Factor**" shall be determined in accordance with Section J3.5, J3.6 or J3.7 (as applicable); provided that, where a Party has failed to pay the Charges set out in an Invoice by the Due Date on 3 or more occasions during the 12 months preceding the date on which the Credit Cover Factor is being determined, then the Party's Credit Cover Factor shall be 100%.

J3.5 Where a Party has one or more Recognised Credit Ratings, the Party's Credit Cover Factor shall be determined on the basis of that Recognised Credit Rating from time to time as follows (based, where the Party has more than one such rating, on the lower of the ratings):

DBRS		Moody's		Fitch		Standard and Poor's		Credit Cover Factor (%)
Long-Term	Short-Term	Long-Term	Short-Term	Long-Term	Short-Term	Long-Term	Short-Term	
AAA	R-1 H	Aaa	P-1	AAA	F1+	AAA	A-1+	**0**
AA (high)	R-1 H	Aa1	P-1	AA+	F1+	AA+	A-1+	**0**
AA	R-1 M	Aa2	P-1	AA	F1+	AA	A-1+	**0**
AA (low)	R-1 M	Aa2	P-1	AA-	F1+	AA-	A-1+	**0**
A (high)	R-1 L	A1	P-1	A+	F1	A+	A-1	**0**
A	R-1 L	A2	P-1	A	F1	A	A-1	**0**
A (low)	R-1 L	A3	P-2	A-	F2	A-	A-2	**0**
BBB (high)	R-2 H	Baa1	P-2	BBB+	F2	BBB+	A-2	**50**
BBB	R-2 M	Baa2	P-3	BBB	F3	BBB	A-3	**50**
BBB (low)	R-2 L	Baa3	P-3	BBB–	F3	BBB–	A-3	**50**
lower	lower	lower	lower	lower	lower	lower	lower	**100**

J3.6 Where a Party's obligations are guaranteed by a Parent Company Guarantee, and where the provider of that Parent Company Guarantee has a Recognised Credit Rating, the Party's Credit Cover Factor shall be determined in accordance with Section J3.5; save that:

(a) Section J3.5 shall apply on the basis of the Recognised Credit Rating of the guarantor under the Parent Company Guarantee (rather than of the Party); and

(b) where the Parent Company Guarantee is capped at an amount lower than the Party's Value at Risk, then the Party's Credit Cover Factor shall be the weighted average of the amounts determined under Sections J3.6(a) and either

(as applicable) J3.5 or J3.7(a) (such average to be weighted by reference to the Parent Company Guarantee cap and the amount by which the Party's Value at Risk exceeds such cap).

J3.7 To the extent that neither Section J3.5 nor J3.6 applies to a Party, the Party's Credit Cover Factor shall be determined:

(a) where a Party's obligations are not guaranteed by a Parent Company Guarantee, on the basis of the Party's Credit Assessment Score;

(b) where a Party's obligations are guaranteed by a Parent Company Guarantee and that guarantee is capped at an amount higher than the Party's Value at Risk, on the basis of the guarantor's Credit Assessment Score; or

(c) where a Party's obligations are guaranteed by a Parent Company Guarantee and that guarantee is capped at an amount lower than the Party's Value at Risk, on the basis of the weighted average of the Party's Credit Assessment Score and the guarantor's Credit Assessment Score (weighted by reference to the Parent Company Guarantee cap and the amount by which the Party's Value at Risk exceeds such cap).

J3.8 For the purposes of Section J3.7, the Party's (and/or its guarantor's) "**Credit Assessment Score**" shall be determined in accordance with the table set out below (subject to Section J3.9(d)):

Check It (ICC) Credit Score Report	**Dunn & Bradstreet / N2 Check Comprehensive Report**	**Equifax**	**Experian Bronze, Silver or Gold Report**	**Graydons Level 1, Level 2, or Level 3 Report**	**Credit Cover Factor (%)**
95-100	5A1/	A+	95-100	1A	**50**
90-94	5A2/4A1	A /A-	90-94	1B/2A	**60**
80-89	5A3/4A2/3A1	B+	80-89	1C/2B/3A	**70**
70-79	4A3/3A2/2A1	B/B-	70-79	2C/3B/4A	**80**
60-69	3A3/2A2/1A1	C+	60-69	3C/4B/5A	**90**
50-59	2A3/1A2/A1	C/C-	50-59	4C/5B/6A	**100**
40-49	1A3/A2/B1	D+	40-49	5C/6B/7A	**100**
30-39	A3/B2/C1	D/D-	30-39	6C/7B/8A	**100**
20-29	B3/C2/D1	E+	20-29	8B	**100**
10-19	C3/D2/E1	E/E-	10-19	8C	**100**
Below 10	Below E1	Below E-	Below 10	Below 8C	**100**

J3.9 Where Section J3.7 applies to a Party:

(a) the cost of obtaining the Credit Assessment Score in respect of that Party (and/or its guarantor) shall be met by the Party;

(b) a revised Credit Assessment Score in respect of that Party (and/or its guarantor) shall be obtained as often as the Party reasonably requires and at least once every 12 months;

(c) where no valid Credit Assessment Score exists in respect of a Party (or its guarantor) the Party's Credit Cover Factor shall be deemed to be 100%; and

(d) where the Party's Value at Risk (and/or the guarantor's Parent Company Guarantee cap) exceeds the recommended exposure limit associated with its Credit Assessment Score, its Credit Assessment Score shall be the weighted average of the Credit Assessment Score that would otherwise have applied and 100% (weighted by reference to the recommended exposure limit, and the amount by which the Vale at Risk (or Parent Company Guarantee cap) exceeds such limit).

Increase or Decrease in Credit Cover Requirement

J3.10 On notifying a Party of its Credit Cover Requirement pursuant to Section J3.2, the DCC shall also specify the value of the Credit Support provided to the DCC on behalf of the Party at that time. Where the value of the Credit Support is less than the Party's Credit Cover Requirement, the Party shall, within two Working Days after receipt of such notification, procure that additional Credit Support is provided to the DCC on the Party's behalf so that the aggregate value of all such Credit Support is equal to or greater than the Party's Credit Cover Requirement.

J3.11 The DCC shall, within five Working Days after a request from a Party to do so, return that Party's Credit Support (or any part of it) to that Party; provided that the DCC shall never be obliged to return Credit Support to the extent that such return would reduce the aggregate value of the Party's Credit Support below the Party Credit Cover Requirement.

J3.12 Additions and reductions in Credit Support pursuant to Section J3.10 and J3.11 may (without limitation) be achieved by amending the terms of existing Credit Support or exchanging Credit Support.

J3.13 For the avoidance of doubt, where a Bank Guarantee, Letter of Credit or Parent Company Guarantee provided on behalf of a Party ceases to satisfy the requirements of the definitions of Bank Guarantee, Letter of Credit or Parent Company Guarantee (respectively), then the value of such Credit Support or of the Party's Credit Cover Factor (as applicable) shall be calculated as if no such document had been provided (and the DCC shall return such document to the Party within 5 Working Days after a request to do so).

Breach of Credit Cover Obligations

J3.14 Where a Party fails to procure that Credit Support (or additional Credit Support) is provided to the DCC on the Party's behalf in accordance with this Section J3, then the DCC shall issue a notice to that Party:

(a) setting out that fact; and

(b) referring to the matters set out in Section M8.1(e) (Events of Default).

Disputes

J3.15 Where a Party disputes the amount of Credit Support requested of it pursuant to this Section J3, that Party shall nevertheless procure that such amount of Credit Support is provided to the DCC, pending resolution of such dispute. In the case of such a dispute:

(a) such Party and the DCC shall each in good faith negotiate to resolve the dispute amicably and as soon as reasonably practicable after it arises;

(b) the DCC shall provide all such evidence in support of its position as the disputing Party may reasonably request, and the DCC shall provide such evidence within 5 Working Days after such request;

(c) no earlier than 1 Working Day after receipt from the DCC of the information requested under Section J3.15(b) (or, where the DCC does not comply with such request, on the expiry of the period referred to in that Section), the disputing Party may refer the dispute to the Panel, in which case each of the DCC and the disputing Party shall be entitled to provide written submissions in support of its position;

(d) where a dispute is referred to the Panel in accordance with Section J3.15(c), the Panel shall convene a meeting and determine the dispute within 10 Working Days of the reference being made (to which meeting representatives of the disputing Party and the DCC may be invited in accordance with Section C (Governance)); and

(e) the disputing Party and the DCC shall each give effect to any determination of the Panel pursuant to this Section J3.15, which shall be final and binding for the purposes of this Code.

Use of Credit Support

J3.16 Where a Party fails to pay the Charges set out in an Invoice addressed to that Party by the Due Date for that Invoice, and where the DCC has issued a notice to that Party pursuant to Section J2.1 (Notification of Payment Failure), the DCC shall (in addition to any other remedies available to it) on the Working Day following service of such notice:

(a) claim an amount equal to the unpaid Charges plus interest (or, if lower, as much as is available to be claimed) under any Bank Guarantee or Letter of Credit provided on behalf of that Party;

(b) remove an amount equal to the unpaid Charges plus interest (or, if lower, as much as is available to be removed) from any Cash Deposit account; or

(c) undertake a combination of the above in respect of a total amount equal to the unpaid Charges plus interest (or, if lower, as much as is available to be claimed or removed).

J3.17 The DCC shall notify the Party as soon as reasonably practicable after the DCC takes any action pursuant to Section J3.16.

J3.18 The DCC shall only exercise its rights in respect of a Party's Credit Support in accordance with Section J3.16.

J3.19 Any amount received by the DCC pursuant to the exercise of its rights in respect of a Party's Credit Support shall discharge the Party's payment obligations to the extent of the amount so received, and reduce the value of the Credit Support to the same extent.

Cash Deposit

J3.20 Interest that accrues on the funds deposited in a Cash Deposit account shall be added to and form part of such deposit.

J3.21 It is agreed that all right, title and interest in and to the Cash Deposit vests in the DCC absolutely free and clear of any liens, claims, charges, encumbrances or other security interests (but without prejudice to the DCC's obligation to return an equivalent amount of money to the Party subject to and in accordance with Section J3.11).

Letters of Credit and Bank Guarantees

J3.22 Where a Party has procured that Credit Support is delivered to the DCC in the form of a Letter of Credit or Bank Guarantee, and where that Letter of Credit or Bank Guarantee has 20 Working Days or less left until it expires, the DCC shall give notice of that fact to the Party (which notice must refer to the matters set out in Section J3.23).

J3.23 Where the DCC has given notice to a Party pursuant to Section J3.22, and where the Party has not (within 10 Working Days after such notice) procured that replacement Credit Support of equivalent value is provided to the DCC (to take effect on or before expiry of the current Letter of Credit or Bank Guarantee), then the DCC shall:

(a) prior to the expiry of the Letter of Credit or Bank Guarantee, claim the entire undrawn value of the Letter of Credit or Bank Guarantee; and

(b) hold any amount so claimed as if it had been paid to the DCC as a Cash Deposit.

J4 REVIEW AND FORECASTING OF CHARGES

Review of Charges

J4.1 The Charges payable from time to time are set out in the Charging Statement applicable at that time.

J4.2 The DCC shall only amend the Charges from time to time in accordance with the DCC Licence. The DCC shall only amend the Charges once in each calendar year, such amendments to have effect from the start of each Regulatory Year (save for amendments permitted or required in accordance with Condition 19.11 of the DCC Licence). This Section J4.2 is without prejudice to the requirements of Condition 19 of the DCC Licence, and (unless the Authority gives consent under Condition 19.10 of the DCC Licence) the DCC shall give notice of any proposed changes to Parties pursuant to Condition 19.9 of the DCC Licence.

Indicative Charging Statements

J4.3 Within the first five Working Days of April, July, October and January in each year, the DCC shall create and publish on the DCC Website an indicative Charging Statement for the first Regulatory Year due to start thereafter, setting out indicative Charges for that Regulatory Year based on the information available to the DCC at the start of the month of publication.

Indicative Budgets

J4.4 Within the first five Working Days of April, July, October and January in each year, the DCC shall create and publish on the DCC Website a budget for the second and third Regulatory Years due to start thereafter, setting out indicative figures for each such Regulatory Year based on the information available to the DCC at the start of the month of publication.

J4.5 Each such budget will contain indicative values for the following (as each such expression is defined in the Charging Methodology):

Acronym	Name
EAR_t	Estimated Allowed Revenue
EFR_t	Estimated Fixed Revenue
$EESR_t$	Estimated Elective Services Revenue

Acronym	Name
$EECR_t$	Estimated Explicit Charges Revenue
NFR_t	National Fixed Revenue
RFR_{rt}	Regional Fixed Revenue
EC_{it}	Explicit Charge for each Explicit Charging Metric
$RCHR_{rt}$	Regional Communications Hub Revenue

Working Model

J4.6 The DCC shall publish a working model which allows Parties to estimate their indicative Charges based on their view of input data relevant under the Charging Methodology, and which allows Parties to test potential modifications to the Charging Methodology. The DCC shall publish such model in an open-access or off-the-shelf software format, and hereby authorises the Parties to use and modify the model for the purposes set out in this Section J4.6 (subject to the relevant software licence). Such model shall not form part of the Charging Methodology.

Invoicing Timetable

J4.7 The DCC shall, from time to time, publish an indicative timetable of the dates on which the DCC intends to submit invoices pursuant to Section J1.2.

Minimum Monthly Charge and Credit Cover Threshold

J4.8 The DCC shall publish, with the indicative Charging Statement published in January and with the actual Charging Statement for each Regulatory Year, the values of the Minimum Monthly Charge and the Credit Cover Threshold for that Regulatory Year.

SECTION K: CHARGING METHODOLOGY

K1 INTRODUCTION

K1.1 This Section K constitutes the Charging Methodology that the DCC is required to have in force in accordance with the DCC Licence.

K1.2 The Charges payable to the DCC by the other Parties from time to time are those Charges set out in the Charging Statement at that time, which are payable in accordance with Section J.

K1.3 The DCC is obliged under the DCC Licence to prepare the Charging Statement in accordance with this Charging Methodology.

K1.4 This Charging Methodology is subject to modification in accordance with Section D (Modification Process), by reference to the Charging Objectives. This Section K is included in this Code in order to allow for such modification. This Section K is not intended to, and does not, create any contractual obligations between the Parties.

K1.5 This Charging Methodology provides for Fixed Charges, Fixed CH Charges, Fixed Alt HAN Charges, Explicit Charges and Elective Charges. The methodology for calculating Fixed Charges differs before, during, and after the UITMR Period (as set out in Sections K4, K5 and K6 respectively). The methodology for calculating Fixed Alt Han Charges differs during and after the UITMR Period (as set out in Sections K5A and K6B respectively).

K1.6 The DCC shall act reasonably and in a manner consistent with the Charging Objectives in undertaking all calculations and estimations required pursuant to this Charging Methodology.

K1.7 The expressions used in this Charging Methodology shall have the meanings given to them in Section K11.

K2 ESTIMATED REVENUES

Estimated Allowed Revenue

K2.1 In respect of each Regulatory Year, the DCC shall estimate the Allowed Revenue for that Regulatory Year. Such estimate for each Regulatory Year shall be the "**Estimated Allowed Revenue**" for that Regulatory Year.

Estimated Elective Service Revenue

K2.2 In respect of each Regulatory Year, the DCC shall estimate the amount that will be payable to it in respect of the provision of Elective Communication Services during that Regulatory Year. Such estimation shall be based on the Charges payable under the relevant Bilateral Agreements, the DCC's estimate of the frequency at which the DCC will provide such Services (to the extent such Charges are payable on that basis), and any other relevant factors.

K2.3 The DCC's estimate in accordance with paragraph K2.2 for each Regulatory Year shall be the "**Estimated Elective Service Revenue**" for that Regulatory Year.

Estimated Explicit Charges Revenue

K2.4 In respect of each Regulatory Year, the DCC shall estimate the amount that will be payable to it in respect of the Explicit Charging Metrics during that Regulatory Year, based on the Explicit Charges (calculated in accordance with Section K7) and the DCC's estimate of the frequency at which the Explicit Charging Metrics will occur during that year.

K2.5 The DCC's estimate in accordance with paragraph K2.4 for each Regulatory Year shall be the "**Estimated Explicit Charges Revenue**" for that Regulatory Year.

Estimated Fixed Revenue

K2.6 In respect of each Regulatory Year (t), the "**Estimated Fixed Revenue**" shall be calculated as follows:

$$EFR_t = EAR_t - EESR_t - EECR_t$$

Where:

EFR_t = the Estimated Fixed Revenue for the Regulatory Year t

EAR_t = the Estimated Allowed Revenue for the Regulatory Year t

$EESR_t$ = the Estimated Elective Services Revenue for the Regulatory Year t

$EECR_t$ = the Estimated Explicit Charges Revenue for the Regulatory Year t.

K3 FIXED CHARGE, FIXED CH CHARGE AND FIXED ALT HAN CHARGE CALCULATIONS

Introduction

K3.1 The DCC will determine the Fixed Charges, the Fixed CH Charges and the Fixed Alt HAN Charges for each Regulatory Year using the Estimated Fixed Revenue determined in accordance with Section K2, which is to be translated into:

(a) Fixed Charges in accordance with Section K4, K5 or K6 (depending upon whether the Regulatory Year occurs before, during or after the UITMR Period);

(b) Fixed CH Charges in accordance with Section K6A (which are payable in respect of Smart Metering Systems); and

(c) Fixed Alt HAN Charges in accordance with Sections K5A and K6B (depending upon whether the Regulatory Year occurs during or after the UITMR Period).

K3.2 The Fixed Charges and Fixed Alt HAN Charges are payable in respect of:

(a) (in the case of the Fixed Charges alone) prior to the UITMR Period, Mandated Smart Metering Systems for Domestic Premises;

(b) during the UITMR Period, Mandated Smart Metering Systems for Domestic Premises and Enrolled Smart Metering Systems for Designated Premises; and

(c) after the UITMR Period, Enrolled Smart Metering Systems (whether for Domestic Premises or Designated Premises),

and each reference in this Section K3 (or in the definitions of defined terms used directly or indirectly in this Section K3) to '**Smart Metering Systems**' shall accordingly be construed as a reference to Mandated Smart Metering Systems or Enrolled Smart Metering Systems (as applicable).

K3.3 As further described in this Section K3, the Fixed Charges potentially differ so as to distinguish between Smart Metering Systems for Domestic Premises and for Non-

Domestic Premises, between Smart Metering Systems in different Regions, and between persons within different Charging Groups.

Domestic or Non-Domestic Premises

K3.4 The Charging Objectives require the DCC to impose Charges in respect of Smart Metering Systems for Domestic Premises that do not distinguish (whether directly or indirectly) between Domestic Premises located in different parts of Great Britain. Consistent with the Charging Objectives, the methodology provides for different means of calculating the Fixed Charges, Fixed CH Charges and Fixed Alt HAN Charges depending upon whether a Smart Metering System is for Domestic Premises or for Non-Domestic Premises. The DCC shall estimate the numbers of Domestic Premises and Non-Domestic Premises based on Registration Data (using profile class in the case of Smart Metering Systems associated with an MPAN and market sector code in the case of Smart Metering Systems associated with an MPRN, or some other sensible proxy to the extent that the Registration Data does not readily identify whether a premises is a Domestic Premises and Non-Domestic Premises).

Cost-reflectivity

K3.5 One of the Charging Objectives is that the Charges are cost reflective (insofar as reasonably practicable in the circumstances of the case, having regard to the cost of implementing the methodology and subject to the objective referred to in Section K3.4). Consistent with the Charging Objectives, the methodology provides (subject to Section K3.4) for:

(a) the Fixed Charges in respect of a Smart Metering System to be set proportionately to the costs and expenses of providing the Services (other than the Communications Hub Services, the Elective Communication Services and the Explicit Charging Metrics) in respect of that Smart Metering System by Region and Charging Group;

(b) the Fixed CH Charges in respect of a Smart Metering System to be set proportionately to the costs and expenses of providing the Communications Hub Services (other than the Explicit Charging Metrics) in respect of that

Smart Metering System by Region and Charging Group; and

(c) the Fixed Alt HAN Charges in respect of a Smart Metering System to be set proportionately to the costs of reimbursing AltHANCo for the Alt HAN Costs (other than the Explicit Charging Metrics) in respect of that Smart Metering System by Charging Group,

in each case as set out in the remainder of this Section K3.

Regions

K3.6 The costs and expenses of providing the Services (ignoring the Elective Communication Services and ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges) in respect of a Smart Metering System for a premises may vary depending upon the Region in which such premises is located. For the reasons described in Section K3.4, the Fixed Charges and Fixed CH Charges in respect of Smart Metering Systems for Domestic Premises will not differ by Region, but those in respect of Smart Metering Systems for Non-Domestic Premises may.

K3.7 For the reasons described in Section K3.5 and K3.6, the DCC must split the Estimated Fixed Revenue for Regulatory Year (t) between:

(a) revenue relating to the cost and expenses of providing the Services that should be recovered on a uniform basis across all the Regions (the **National Fixed Revenue**);

(b) revenue relating to the reimbursement of Alt HAN Costs (the **Alt HAN Fixed Revenue**); and

(c) revenue relating to the cost and expenses of providing the Services that should be recovered on a basis that differentiates between Regions (for each Region, the **Regional Fixed Revenue**).

K3.8 Whilst neither Fixed Charges and Fixed CH Charges in respect of Domestic Premises, nor any Fixed Alt HAN Charges, will ultimately vary by Region, in order to determine the regional charges to apply in respect of Non-Domestic Premises, the

DCC must first apportion the entirety of the Estimated Fixed Revenue between those costs which do and those which do not vary by Region (initially disregarding the fact that the Fixed Alt HAN Charges and other charges in respect of Domestic Premises will ultimately be recovered on a uniform basis). For these purposes, the DCC shall apportion the Estimated Fixed Revenue between:

(a) the National Fixed Revenue, the Alt HAN Fixed Revenue and the Regional Fixed Revenue for each Region so as to reflect the relative proportion of the cost and expenses that the DCC incurs across all Regions or in particular Regions in providing the Services and in reimbursing the Alt HAN Costs (ignoring the Communications Hub Services and the Elective Communication Services and ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges); and

(b) the Regional Communications Hub Revenue for each Region so as to reflect the cost and expenses that the DCC incurs in providing the Communications Hub Services in that Region (ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges),

in each case, so that any revenue restriction correction factor adjustment contained within the Estimated Fixed Revenue is apportioned between (a) or (b) above on the basis of the extent to which it arose in relation either to the Services other than the Communications Hub Services and to the Alt HAN Costs, or to the Communications Hub Services (respectively).

K3.9 The apportionment described in Sections K3.7 and K3.8 shall be such that:

$$EFR_t = NFR_t + AHFR_t + \sum_{\forall r} RFR_{rt} + \sum_{\forall r} RCHR_{rt}$$

Where:

EFR_t = the Estimated Fixed Revenue (estimated in accordance with Section K2) for Regulatory Year (t).

NFR_t = the National Fixed Revenue (estimated in accordance with Section K3.7) for Regulatory Year (t).

$AHFR_t$ = the Alt HAN Fixed Revenue (estimated in accordance with Section K3.7) for Regulatory Year (t).

RFR_{rt} = the Regional Fixed Revenue (estimated in accordance with Section K3.7) within each Region (r) for Regulatory Year (t).

$RCHR_{rt}$ = the Regional Communications Hub Revenue (estimated in accordance with Section K3.7) within each Region (r) for Regulatory Year (t).

Charging Groups

K3.10 The methodology recognises the following five categories for Smart Metering Systems. The Fixed Charges are payable by Parties in all five categories (each a **Charging Group**). The Fixed CH Charges are payable by Parties in only the first three categories (each a **CH Charging Group**). The Fixed Alt HAN Charges are payable by Parties in only the first and third categories (each an **Alt HAN Charging Group**):

(a) the Import Suppliers (**Charging Group g1**);

(b) the Export Suppliers (**Charging Group g2**);

(c) the Gas Suppliers (**Charging Group g3**);

(d) the Electricity Distributors (**Charging Group g4**); and

(e) the Gas Transporters (**Charging Group g5**).

Application of Charging Group Weighting Factors

K3.11 For the reasons described in Section K3.5, the Fixed Charges, Fixed CH Charges and Fixed Alt HAN Charges payable by each Charging Group may need to differ. This is achieved through the Charging Group, CH Charging Group and Alt HAN Charging Group Weighting Factors.

K3.12 The Weighting Factors are designed:

(a) to reflect the relative proportion of the costs and expenses likely to be incurred by the DCC in providing the Services and in reimbursing the Alt HAN Costs (ignoring the Elective Communication Services and ignoring the costs and expenses designed to be recovered pursuant to the Explicit Charges) to the persons in each Charging Group;

(b) to specify the ratio of the costs and expenses to be incurred in respect of each Smart Metering System (without regard to the number of Smart Metering Systems); and

(c) so that the sum of the Charging Group, CH Charging Group and Alt HAN Charging Group Weighting Factors shall in each case be equal to one (1).

K3.13 For Fixed Charges, the "**Charging Group Weighting Factors**" to apply to each Charging Group in respect of each Regulatory Year are to be determined by the DCC in accordance with Section K3.12, and set out in the Charging Statement for that Regulatory Year. The DCC shall make such determination based on its estimate of the demand of persons within each Charging Group for each of the Services other than the Elective Communication Services. Prior to the start of the UITMR Period, such estimates of demand will be based on assumptions for the Regulatory Year starting on 1st April 2021. Once data on usage becomes available the estimates will be determined as the average of the previous two full Regulatory Years of actual data plus the DCC's forecasts for the two Regulatory Years ahead.

K3.14 For Fixed CH Charges, the "**CH Charging Group Weighting Factors**" to apply to each CH Charging Group in respect of each Regulatory Year are to be determined by the DCC on the basis of the relative proportion of their Charging Group Weighting Factors, such that:

$$\beta_{gt} = \frac{\alpha_{gt}}{\sum_{g=1\ldots3} \alpha_{gt}}$$

Where:

β_{gt} = the CH Charging Group Weighting Factor for applicable to Regulatory Year (t) and each Charging Group (g)

α_{gt} = the Charging Group Weighting Factor applicable to Regulatory Year (t) and each Charging Group (g).

K3.15 For Fixed Alt Han Charges, the "**Alt Han Charging Group Weighting Factors**" to apply to each Alt Han Charging Group in respect of each Regulatory Year are to be determined by the DCC on the basis of an expectation of equal use of Alt Han services per Enrolled Smart Metering system by Import Suppliers and Gas Suppliers, such that:

$\gamma_{gt} = 0.5$ where g =1 or 3

$\gamma_{gt} = 0$ where g =2, 4 or 5

Where:

γ_{gt} = the Alt Han Charging Group Weighting Factor for applicable to Regulatory Year (t) and each Charging Group (g).

Description of Approach to Determining Fixed Charges for Smart Metering Systems for Domestic Premises during and after the UITMR Period

K3.16 In the case of the methodology applying during and after the UITMR Period, the approach to determining the Fixed Charges payable in respect of Smart Metering Systems for Domestic Premises is as set out in Section K5.5 and K6.4 (respectively). The approach to determining the Fixed CH Charges payable in respect of Smart Metering Systems for Domestic Premises is as set out in Section K6A.4. However, to assist Parties in understanding those Sections, the approach is described in generic terms below:

(a) the first part of the equation determines an amount that would be recovered in total in respect of all Smart Metering Systems for Domestic Premises across all Regions and Charging Groups were the charges to be calculated in the same manner as those for Smart Metering Systems for Non-Domestic Premises; and

(b) the second part of the equation is then used to pro-rate this total amount on a non-geographic basis across all persons in each Charging Group. This results in the required uniform charge for each Charging Group in respect of Smart Metering Systems for Domestic Premises, and provides the same aggregate revenue for DCC as would have been derived from the same number of Smart Metering Systems for Non-Domestic Premises at the same locations.

Determining Fixed CH Charges

K3.17 In determining the Fixed CH Charges, the DCC shall calculate its cost-reflective charging under Section K3.7 on the basis of the cost of a Standard Communications Hub.

K3.18 In determining the Fixed CH Charges, the DCC shall have regard to the need, for the purposes of making a prudent estimate in accordance with Condition 36.5 of the DCC Licence, to provide for the availability at all times of a contingency fund in respect of the Communications Hub Finance Charges relating to each Communications Hub Finance Facility that is equal to the DCC's estimate of three months of the Communications Hub Finance Costs relating to that facility.

K3.19 No Explicit Charge applies in the event that a Communications Hub is Withdrawn. Therefore, in order to determine the Fixed CH Charges, the DCC shall calculate a factor to be applied to the charges that would otherwise have applied in order to reflect the costs to the DCC of Communications Hubs being Withdrawn before the costs of those Communications Hubs have been recovered in full. Such factor shall be the "**Non-Domestic Withdrawal Factor**" (which shall be the same for each CH Charging Group and Region).

Description of Approach to Determining Fixed Alt Han Charges for Smart Metering Systems for Domestic Premises and Non-Domestic Premises after the UITMR Period

K3.20 The "**Alt Han Cost Domestic Allocation**" is a factor between zero and one that is determined by the DCC based on information provided by AltHanCo to reflect the proportion of usage of Alt Han Equipment in Domestic Premises expressed as a fraction of the total usage across both Domestic and Non-Domestic Premises and is

represented by μ_t for Regulatory Year (t) such that:

$$\mu_t = \frac{DAHU_t}{DAHU_t + NAHU_t}$$

Where:

$DAHU_t$ is the number of MPANs and MPRNs associated with the use of Alt Han Equipment in Domestic Premises, derived by the DCC from the Alt Han usage data available to it one month prior to the issue of the most recent Charging Statement and the Registration Data prevailing at that time.

$NAHU_t$ is the number of MPANs and MPRNs associated with the use of Alt Han Equipment in Non-Domestic Premises, derived by the DCC from the Alt Han usage data available to it one month prior to the issue of the most recent Charging Statement and the Registration Data prevailing at that time.

K4 DETERMINING FIXED CHARGES BEFORE THE UITMR PERIOD

Introduction

K4.1 The DCC will determine the Fixed Charges for each Regulatory Year occurring prior to the UITMR Period in accordance with this Section K4, using:

(a) the Estimated Fixed Revenue for that Regulatory Year determined in accordance with Section K2;

(b) an estimate, in accordance with this Section K4, of the number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year; and

(c) the Charging Group Weighting Factors described in Section K3.

Estimates

K4.2 In respect of Regulatory Years occurring prior to the UITMR Period:

(a) the DCC must estimate the aggregate number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year;

(b) the DCC must estimate the number of persons in each Charging Group for such Mandated Smart Metering Systems; and

(c) the estimate pursuant to Section K4.2(b) in respect of a Regulatory Year (t) and each Charging Group (g) shall be represented as $EMSMS_{gt}$.

Determining the Fixed Charges

K4.3 The DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person in each Charging Group (g) in respect of each Mandated Smart Metering System (FC_{gt}) as follows:

$$FC_{gt} = \frac{EFR_t}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g} \left(\alpha_{gt} \times EMSMS_{gt} \right)}$$

Where:

α_{gt} = the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t = the number of months (or part months) in Regulatory Year (t)

EFR_t = the Estimated Fixed Revenue (estimated in accordance with Section K2) for Regulatory Year (t)

$EMSMS_{gt}$ = the estimate pursuant to Section K4.2(c) for Regulatory Year (t) and each Charging Group (g).

Calculating number of MSMSs for Fixed Charge Payment

K4.4 Following the end of each month (or part month) occurring during each Regulatory Year prior to the UITMR Period, the DCC will:

(a) determine (insofar as it is able) the actual number of Mandated Smart Metering Systems that existed at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month);

(b) calculate the number of persons in each Charging Group for such Mandated Smart Metering Systems; and

(c) break down these calculations by reference to each Party.

K4.5 The calculation in accordance with Section K4.4(c) for each month (or part month) (m) during Regulatory Year (t) and each Party (p) in each Charging Group (g) shall be represented as $AMSMS_{pgmt}$.

K5 DETERMINING FIXED CHARGES DURING THE UITMR PERIOD

Introduction

K5.1 The DCC will determine the Fixed Charges for each Regulatory Year during the UITMR Period in accordance with this Section K5, using:

(a) the National Fixed Revenue and the Regional Fixed Revenue for that Regulatory Year determined in accordance with Section K3;

(b) an estimate, in accordance with this Section K5, of the number of Smart Metering Systems for Non-Domestic Premises that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year;

(c) an estimate, in accordance with this Section K5, of the number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year; and

(d) the Charging Group Weighting Factors and other relevant matters described in Section K3.

Estimates: Non-Domestic Premises

K5.2 In respect of Regulatory Years occurring during the UITMR Period:

(a) the DCC will estimate the total number of Smart Metering Systems for Non-Domestic Premises that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year;

(b) the DCC must estimate the number of persons in each Charging Group for such Smart Metering Systems;

(c) the DCC must break down its estimate pursuant to Section K5.2(b) by reference to the number of Smart Metering Systems in each Region; and

(d) the estimate pursuant to Section K5.2(c) in respect of a Regulatory Year (t), each Charging Group (g) and each Region (r), shall be represented as $RENSMS_{grt}$.

Estimates: Domestic Premises

K5.3 In respect of Regulatory Years occurring during the UITMR Period:

(a) the DCC must estimate the aggregate number of Mandated Smart Metering Systems that will exist as at the beginning of that Regulatory Year;

(b) the DCC must estimate the number of persons in each Charging Group for such Mandated Smart Metering Systems;

(c) the DCC must break down its estimate pursuant to Section K5.3(b) by reference to the number of Mandated Smart Metering Systems in each Region; and

(d) the estimate pursuant to Section K5.3(c) in respect of a Regulatory Year (t), each Charging Group (g) and each Region (r), shall be represented as $REDSMS_{grt}$.

Determining the Fixed Charges: Non-Domestic Premises

K5.4 For each Regulatory Year (t), the DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Charging Group (g) in respect of each Enrolled Smart Metering System for a Non-Domestic Premises in each Region (r) ($RNFC_{grt}$), as follows:

$$RNFC_{grt} = \frac{NFR_t}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g}\left(\alpha_{gt} \times \sum_{\forall r} RESMS_{grt}\right)} + \frac{RFR_{rt}}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g}\left(\alpha_{gt} \times RESMS_{grt}\right)}$$

Where:

α_{gt} = the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t = the number of months (or part months) in Regulatory Year (t)

NFR_t = the National Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t)

RFR_{rt} = the Regional Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t) and Region (r)

$\forall g \forall r \quad RESMS_{grt} = REDSMS_{grt} + RENSMS_{grt}$

$RENSMS_{grt}$ = the estimate pursuant to Section K5.2(d) for Regulatory Year (t), each Charging Group (g) and each Region (r)

$REDSMS_{grt}$ = the estimate pursuant to Section K5.3(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

Determining the Fixed Charges: Domestic Premises

K5.5 For each Regulatory Year (t), the DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Charging Group (g) in respect of each Mandated Smart Metering System ($RDFC_{gt}$) as follows:

$$RDFC_{gt} = \sum_{\forall g \forall r} \left(RNFC_{grt} \times REDSMS_{grt} \right) \times \frac{\alpha_{gt}}{\sum_{\forall g} \left(\alpha_{gt} \times \sum_{\forall r} REDSMS_{grt} \right)}$$

Where:

α_{gt} = the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

$RNFC_{grt}$ = the Fixed Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in each Charging Group (g) in respect of Enrolled Smart Metering Systems for Non-Domestic Premises in each Region (r), as calculated in accordance with Section K5.4

$REDSMS_{grt}$ = the estimate pursuant to Section K5.3(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

Calculating number of ESMSs for Fixed Charge Payment: Non-Domestic Premises

K5.6 Following the end of each month (or part month) occurring during each Regulatory Year during the UITMR Period, the DCC will:

(a) determine the actual number of Smart Metering Systems for Non-Domestic Premises that have been Enrolled (and not Withdrawn) as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month), whether Enrolled during that month or previously;

(b) calculate the number of persons within each Charging Group for those Enrolled Smart Metering Systems; and

(c) break down these calculations by reference to each Party, and by reference to the Region in which such premises are located.

K5.7 The calculations in accordance with Section K5.6 of the number of Enrolled Smart Metering Systems for Non-Domestic Premises as at the end of each month (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p), and by reference to each Region (r), shall be represented as $ANSMS_{pgrmt.}$

Calculating number of MSMSs for Fixed Charge Payment: Domestic Premises

K5.8 Following the end of each month (or part month) occurring during each Regulatory Year during the UITMR Period, the DCC will:

(a) determine (insofar as it is able) the actual number of Mandated Smart Metering Systems for Domestic Premises as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month);

(b) calculate the number of persons within each Charging Group for those Mandated Smart Metering Systems; and

(c) break down these calculations by reference to each Party.

K5.9 The calculations in accordance with Section K5.8 of the number of Mandated Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p) shall be represented as $ADSMS_{pgmt.}$

K5A DETERMINING FIXED ALT HAN CHARGES DURING THE UITMR PERIOD

Introduction

K5A.1 The DCC will determine the Fixed Alt Han Charges for each Regulatory Year during the UITMR Period in accordance with this Section K5A, using:

(a) the Alt Han Fixed Revenue for that Regulatory Year estimated in accordance with Section K3;

(b) an estimate, in accordance with Section K5, of the number of Smart Metering Systems for Non-Domestic Premises that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year;

(c) an estimate, in accordance with Section K5, of the number of Mandated Smart Metering Systems for Domestic Premises that will exist as at the beginning of that Regulatory Year; and

(d) the Alt Han Charging Group Weighting Factors and other relevant matters described in Section K3.

Determining the Alt Han Fixed Charges

K5A.2 For each Regulatory Year (t), the DCC will determine the Alt Han Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt Han Charging Group (g) in respect of each Mandated Smart Metering System and Enrolled Smart Metering System and Non-Domestic Premises ($RAHFC_{gt}$), as follows:

$$RAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{\gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt} \times \sum_{\forall r} RESMS_{grt}\right)}$$

Where:

γ_{gt} = the Alt Han Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t = the number of months (or part months) in Regulatory Year (t);

$AHFR_t$ = the Alt Han Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t);

$\forall g \forall r \quad RESMS_{grt} = REDSMS_{grt} + RENSMS_{grt}$

$RENSMS_{grt}$ = the estimate pursuant to Section K5.2(d) for Regulatory Year (t), each Charging Group (g) and each Region (r);

$REDSMS_{grt}$ = the estimate pursuant to Section K5.3(d) for Regulatory Year (t), each Charging Group (g) and each Region (r).

K6 DETERMINING FIXED CHARGES AFTER THE UITMR PERIOD (ENDURING)

Introduction

K6.1 The DCC will determine the Fixed Charges for each Regulatory Year following the UITMR Period in accordance with this Section K6, using:

(a) the National Fixed Revenue and the Regional Fixed Revenue for that Regulatory Year determined in accordance with Section K3;

(b) an estimate, in accordance with this Section K6, of the number of Smart Metering Systems that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year; and

(c) the Charging Group Weighting Factors and other relevant matters described in Section K3.

Estimates

K6.2 In respect of Regulatory Years occurring after the UITMR Period, the DCC will estimate the number of Smart Metering Systems that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year. The DCC shall undertake such estimates for Domestic Premises and Non-Domestic Premises separately (being *EDSMS* and *ENSMS* respectively). For each such Regulatory Year (t), the DCC will estimate the average number of persons within each Charging Group (g) for such Smart Metering Systems, and break down such estimates by reference to the Region (r) in which the premises is located, such that:

$$\forall g \forall r \quad ESMS_{grt} = EDSMS_{grt} + ENSMS_{grt}$$

Where:

$EDSMS_{grt}$ = the DCC's estimate of the number of persons within each Charging Group (g) for Smart Metering Systems for Domestic Premises that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year (t), broken down by Region (r); and

$ENSMS_{grt}$ = the DCC's estimate of the number of persons within each Charging Group (g) for Smart Metering Systems for Non-Domestic Premises that will have been Enrolled (and not Withdrawn) as at the beginning of that Regulatory Year (t), broken down by Region (r).

Determining the Fixed Charges: Non-Domestic Fixed Charges

K6.3 For each Regulatory Year (t), the DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Charging Group (g) in respect of each Enrolled Smart Metering System for a Non-Domestic Premises in each Region (r) (NFC_{grt}) as follows:

$$NFC_{grt} = \frac{NFR_t}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g}\left(\alpha_{gt} \times \sum_{\forall r} ESMS_{grt}\right)} + \frac{RFR_{rt}}{NM_t} \times \frac{\alpha_{gt}}{\sum_{\forall g}\left(\alpha_{gt} \times ESMS_{grt}\right)}$$

Where:

α_{gt} = the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t = the number of months (or part months) in Regulatory Year (t)

NFR_t = the National Fixed Revenue (determined in accordance with Section K3) for Regulatory Year (t)

$ESMS_{grt}$ = the estimated number of persons within each Charging Group (g) for Enrolled Smart Metering Systems determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r)

RFR_{rt} = the Regional Fixed Revenue (determined in accordance with Section K3) for Regulatory Year (t) and each Region (r).

Determining the Fixed Charges: Domestic Fixed Charges

K6.4 For each Regulatory Year (t), the DCC will determine the Fixed Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within

each Charging Group (g) in respect of each Enrolled Smart Metering System for a Domestic Premises (DFC_{gt}) as follows:

$$DFC_{gt} = \sum_{\forall g \forall r} \left(NFC_{grt} \times EDSMS_{grt} \right) \times \frac{\alpha_{gt}}{\sum_{\forall g} \left(\alpha_{gt} \times \sum_{\forall r} EDSMS_{grt} \right)}$$

Where:

α_{gt} = the Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NFC_{grt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in each Charging Group (g) in respect of Enrolled Smart Metering Systems for Non-Domestic Premises in each Region (r), as determined in accordance with Section K6.3

$EDSMS_{grt}$ = the estimated average number of persons within each Charging Group (g) for Enrolled Smart Metering Systems for Domestic Premises determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r).

Calculating number of ESMSs for Fixed Charge Payment

K6.5 Following the end of each month (or part month) during each Regulatory Year occurring after the UITMR Period, the DCC will:

(a) determine the actual number of Smart Metering Systems that have been Enrolled (and not Withdrawn) as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month), whether Enrolled during that month or previously, and shall do so for Domestic Premises and for Non-Domestic Premises separately;

(b) calculate the number of persons within each Charging Group for such Enrolled Smart Metering Systems; and

(c) break down these calculations by reference to Parties (p), and (in the case of Smart Metering Systems for Non-Domestic Premises only) by reference to the Region in which such premises are located.

K6.6 The calculations in accordance with Section K6.5 of the number of Enrolled Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p), and (in the case of Non-Domestic Premises only) by reference to each Region (r), shall:

(a) in respect of Domestic Premises, be represented as $ADSMS_{pgmt}$; and

(b) in respect of Non-Domestic Premises, be represented as $ANSMS_{pgrmt}$.

K6A DETERMINING FIXED CH CHARGES

Introduction

K6A.1 The DCC will determine the Fixed CH Charges for each Regulatory Year during or after the UITMR Period in accordance with this Section K6A, using:

(a) the Regional Communications Hub Revenue for that Regulatory Year determined in accordance with Section K3;

(b) an estimate, in accordance with this Section K6A, of the average number of Smart Metering Systems that there will be during that Regulatory Year; and

(c) the CH Charging Group Weighting Factors and other relevant matters described in Section K3.

Estimates

K6A.2 In respect of each Regulatory Year occurring during or after the UITMR Period, the DCC will estimate the average number of Smart Metering Systems that there will be during the Regulatory Year. The DCC shall undertake such estimates for Domestic Premises and Non-Domestic Premises separately (being *EDCH* and *ENCH* respectively). For each such Regulatory Year (t), the DCC will estimate the average number of persons within each CH Charging Group (g) for such Smart Metering Systems, and break down such estimates by reference to the Region (r) in which the premises is located, such that:

$$\forall g \forall r \quad ECH_{grt} = EDCH_{grt} + ENCH_{grt}$$

Where:

$EDCH_{grt}$ = the DCC's estimate of the average number of persons within each CH Charging Group (g) for Smart Metering Systems for Domestic Premises during that Regulatory Year (t), broken down by Region (r); and

$ENCH_{grt}$ = the DCC's estimate of the average number of persons within each CH Charging Group (g) for Smart Metering Systems for Non-Domestic Premises during that Regulatory Year (t), broken down by Region (r).

Determining the Fixed CH Charges: Non-Domestic

K6A.3 For each Regulatory Year (t), the DCC will determine the Fixed CH Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within each CH Charging Group (g) in respect of each Smart Metering System for a Non-Domestic Premises in each Region (r) ($NCHC_{grt}$) as follows:

$$NCHC_{grt} = (1 + \delta_t) \times BNCHC_{grt}$$

Where:

$$BNCHC_{grt} = \frac{RCHR_{rt}}{NM_t} \times \frac{\beta_{gt}}{\sum_{\forall g}(\beta_{gt} \times ECH_{grt})}$$

β_{gt} = the CH Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g)

NM_t = the number of months (or part months) in Regulatory Year (t)

$RCHR_{tr}$ = the Regional Communications Hub Revenue (determined in accordance with Section K3) for Regulatory Year (t) and Region (r)

ECH_{grt} = the estimated number of persons within each Charging Group (g) for Smart Metering Systems determined in accordance with Section K6A.2 for Regulatory Year (t) and each Region (r)

δ_t = the Non-Domestic Withdrawal Factor (determined in accordance with Section K3) for Regulatory Year (t).

Determining the Fixed CH Charges: Domestic

K6A.4 For each Regulatory Year (t), the DCC will determine the Fixed CH Charge payable in respect of each month (or part month) of Regulatory Year (t) by each person within

each Charging Group (g) in respect of each Smart Metering System for a Domestic Premises ($DCHC_{gt}$) as follows:

$$DCHC_{gt} = \sum_{\forall g \forall r} \left(BNCHC_{grt} \times EDCH_{grt} \right) \times \frac{\beta_{gt}}{\sum_{\forall g} \left(\beta_{gt} \times \sum_{\forall r} EDCH_{grt} \right)}$$

Where:

$EDCH_{grt}$ = the estimated average number of persons within each Charging Group (g) for Smart Metering Systems for Domestic Premises determined in accordance with Section K6A.2 for Regulatory Year (t) and each Region (r).

Calculating number of CHs for Fixed CH Charge Payment

K6A.5 Following the end of each month (or part month) during each Regulatory Year occurring during or after the UITMR Period, the DCC will:

(a) determine the actual number of Smart Metering Systems that there are as at the end of the 15th day of that month (or, in the case of a part month that ends on or prior to the 15th day of that month, at the end of that part month), and shall do so for Domestic Premises and for Non-Domestic Premises separately;

(b) calculate the number of persons within each CH Charging Group for such Smart Metering Systems; and

(c) break down these calculations by reference to Parties (p), and (in the case of Smart Metering Systems for Non-Domestic Premises only) by reference to the Region in which such premises are located.

K6A.6 The calculations in accordance with Section K6A.5 of the number of Smart Metering Systems as at the end of each month (or part month) (m) during Regulatory Year (t) within each Charging Group (g) broken down by reference to each Party (p), and (in the case of Non-Domestic Premises only) by reference to each Region (r), shall:

(a) in respect of Domestic Premises, be represented as $ADCH_{pgmt}$; and

(b) in respect of Non-Domestic Premises, be represented as $ANCH_{pgrmt}$.

K6B DETERMINING FIXED ALT HAN CHARGES AFTER THE UITMR PERIOD (ENDURING)

K6B.1 The DCC will determine the Fixed Alt Han Charges for each Regulatory Year after the UITMR Period in accordance with this Section K6B, using:

(a) the Alt Han Fixed Revenue, for that Regulatory Year estimated in accordance with Section K3;

(b) an estimate, in accordance with Section K6, of the number of Smart Metering Systems that there will have been Enrolled (and not Withdrawn) at the beginning of that Regulatory Year; and

(c) the Alt Han Charging Group Weighting Factors and other relevant matters described in Section K3.

Determining the Alt Han Fixed Charges: Domestic

K6B.2 For each Regulatory Year (t) following the UITMR Period, the DCC will determine the Alt Han Fixed Charges payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt Han Charging Group (g) in respect of each Enrolled Smart Metering System for a Domestic Premises ($DAHFC_{gt}$) as follows:

$$DAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{\mu_t \times \gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt} \times \sum_{\forall r} EDSMS_{grt}\right)}$$

Where:

μ_t = the Alt Han Central Cost Domestic Allocation applicable to Regulatory Year (t) (set out in Section K3);

γ_{gt} = the Alt Han Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t = the number of months (or part months) in Regulatory Year (t);

$EDSMS_{grt}$ = the estimated number of persons within each Charging Group (g) for Enrolled Smart Metering Systems for Domestic Premises determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r);

$AHFR_t$ = the Alt Han Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t).

Determining the Alt Han Fixed Charges: Non-Domestic

K6B.3 For each Regulatory Year (t) following the UITMR Period, the DCC will determine the Alt Han Fixed Charges payable in respect of each month (or part month) of Regulatory Year (t) by each person within each Alt Han Charging Group (g) in respect of each Enrolled Smart Metering System for a Non-Domestic Premises ($NAHCFC_{gt}$) as follows:

$$NAHFC_{gt} = \frac{AHFR_t}{NM_t} \times \frac{(1-\mu_t)\times\gamma_{gt}}{\sum_{\forall g}\left(\gamma_{gt}\times\sum_{\forall r} ENSMS_{grt}\right)}$$

Where:

μ_t = the Alt Han Central Cost Domestic Allocation (set out in Section K3);

γ_{gt} = the Alt Han Charging Group Weighting Factor (as set out in Section K3) applicable to Regulatory Year (t) and each Charging Group (g);

NM_t = the number of months (or part months) in Regulatory Year (t);

$ENSMS_{grt}$ = the estimated number of persons within each Alt Han Charging Group (g) for Enrolled Smart Metering Systems for Non-Domestic Premises determined in accordance with Section K6.2 for Regulatory Year (t) and each Region (r);

$AHFR_t$ = the Alt Han Fixed Revenue (estimated in accordance with Section K3) for Regulatory Year (t).

K7 DETERMINING EXPLICIT CHARGES

Introduction

K7.1 The Explicit Charges for each Regulatory Year are payable in respect of the Explicit Charging Metrics for that Regulatory Year.

K7.2 The Explicit Charging Metrics from time to time are as set out in this Section K7.

K7.3 Part of the rationale for Explicit Charging Metrics is to allow the DCC to closely reflect the charges it pays to the DCC Service Providers in respect of certain services, and to AltHANCo in respect of the Alt HAN Costs, so as to minimise the risks for the DCC associated with uncertainty regarding the frequency with which such services are to be provided or such Alt HAN Costs are incurred. The Explicit Charging Metrics may comprise any or all of the Core Communication Services and of the Enabling Services (so they are a sub-set of all Services other than the Elective Communication Services) and of the Alt HAN Costs. The Explicit Charging Metrics represent those Core Communication Services, Enabling Services and Alt HAN Costs that are to be charged for separately from the Fixed Charges, Fixed CH Charges and Fixed Alt HAN Charges.

K7.4 The DCC will determine the Explicit Charges for each Regulatory Year in accordance with this Section K7.

Explicit Charging Metrics

K7.5 The Explicit Charging Metrics for each Party and the Charging Period for each month are as follows:

(a) (*'security assessments'*) an obligation to pay arising during that Charging Period in respect of that Party pursuant to Section G8.48 (Users: Obligation to Pay Charges) in relation to User Security Assessments, Follow-up Security Assessments, User Security Assessment Reports or the activities of the Independent Security Assurance Service Provider;

(b) (*'privacy assessments'*) an obligation to pay arising during that Charging Period in respect of that Party pursuant to Section I2.39 (Users: Obligation to

Pay Charges) in relation to Full Privacy Assessments, Random Sample Privacy Assessments, Privacy Assessment Reports or the activities of the Independent Privacy Auditor;

(c) (*'LV gateway connection'*) an obligation to pay arising during that Charging Period in accordance with an offer for a DCC Gateway LV Connection accepted by that Party pursuant to Section H15 (DCC Gateway Connections), including where the obligation to pay is preserved under Section H15.19(b) (Ongoing Provision of a DCC Gateway Connection);

(d) ('*HV gateway connection*') an obligation to pay arising during that Charging Period in accordance with an offer for a DCC Gateway HV Connection accepted by that Party pursuant to Section H15 (DCC Gateway Connections), including where the obligation to pay is preserved under Section H15.19(b) (Ongoing Provision of a DCC Gateway Connection);

(e) ('*gateway equipment relocation*') an obligation to pay arising during that Charging Period as a result of a request by that Party to relocate DCC Gateway Equipment under Section H15.27 (DCC Gateway Equipment);

(f) (*'elective service evaluations'*) an obligation to pay arising during that Charging Period under the terms and conditions accepted by that Party for a Detailed Evaluation in respect of potential Elective Communication Services pursuant to Section H7.8 (Detailed Evaluations of Elective Communication Services);

(g) ('*P&C support*') an obligation to pay arising during that Charging Period under the terms and conditions accepted by that Party in relation to that Party's use or implementation of the Parse and Correlate Software pursuant to Section H11.12 (Provision of Support & Assistance to Users);

(h) ('*SM WAN for testing'*) an obligation to pay arising during that Charging Period from the acceptance by that Party of the charges offered by the DCC to provide a connection to a simulation of the SM WAN pursuant to Section H14.31 (Device and User System Testing);

(i) (*'additional testing support'*) an obligation to pay arising during that Charging Period from the acceptance by that Party of the charges offered by the DCC to provide additional testing support to that Party pursuant to Section H14.33 (Device and User System Testing);

(j) (*'communication services'*) the number of each of the Services identified in the DCC User Interface Services Schedule which have been provided to that Party during that Charging Period;

(k) (*'CH non-standard delivery'*) an obligation to pay arising during that Charging Period as a result of the request by that Party for non-standard Communications Hub Product delivery requirements pursuant to Section F6.17 (Non-Standard Delivery Options);

(l) (*'CH stock level charge'*) the number (to be measured at the end of that Charging Period) of Communications Hubs that have been delivered to that Party under Section F6 (Delivery and Acceptance of Communications Hubs) and for which none of the following has yet occurred: (i) identification on the Smart Metering Inventory as 'installed not commissioned' or 'commissioned'; (ii) rejection in accordance with Section F6.10 (Confirmation of Delivery); (iii) delivery to the DCC in accordance with Section F8 (Removal and Return of Communications Hubs); or (iv) notification to the DCC in accordance with Section F8 (Removal and Return of Communications Hubs) that the Communications Hub has been lost or destroyed;

(m) (*'CH variant charge'*) the number of each of the Variant Communications Hubs which have been delivered to that Party during that Charging Period under Section F6 (Delivery and Acceptance of Communications Hubs) or F7.4A (Special Installation Mesh Communications Hubs), and which have not been (and are not) returned, or notified as lost or destroyed, for a reason which is a CH Pre-Installation DCC Responsibility;

(n) (*'CH auxiliary equipment'*) the number of each of the types of Communications Hub Auxiliary Equipment which have been delivered to that Party during that Charging Period under Section F6 (Delivery and Acceptance

of Communications Hubs), and which have not been (and are not) rejected in accordance with Section F6.10 (Rejected Communications Hub Products) or (in the case of the Communications Hub Auxiliary Equipment to which Section 7.8 applies (Ownership of and Responsibility for Communications Hub Auxiliary Equipment)) returned, or notified as lost or destroyed, for a reason which is a CH Pre-Installation DCC Responsibility;

(o) ('*CH returned and redeployed*') the number of Communications Hubs which have been returned by that Party during that Charging Period for a reason which is a CH User Responsibility, and which have been (or are intended to be) reconditioned for redeployment pursuant to Section F8 (Removal and Return of Communications Hubs);

(p) ('*CH returned not redeployed*') the number of Communications Hubs which have been returned, or notified as lost or destroyed, by that Party during that Charging Period for a reason which is a CH User Responsibility, and which have not been (and are not intended to be) reconditioned for redeployment pursuant to Section F8 (Removal and Return of Communications Hubs);

(q) (*'CH wrong returns location'*) an obligation to pay arising during that Charging Period as a result of the return by that Party of Communications Hubs to the wrong returns location as referred to in Section F8.9 (Return of Communications Hubs);

(r) ('*test comms hubs*') the number of Test Communications Hubs delivered to that Party during that Charging Period, and which have not been (and are not) returned to the DCC in accordance with Section F10.8 (Ordering, Delivery, Rejection and Returns);

(s) ('*additional CH Order Management System accounts*') the number of additional CH Order Management System accounts made available to that Party during that Charging Period in accordance with Section F5.23 (CH Order Management System Accounts);

(t) ('*shared solution Alt HAN Equipment*') the number (as measured at the end of that Charging Period) of Smart Metering Systems associated with an MPAN at

premises supplied with electricity by that Party, or with an MPRN at premises supplied with gas by that Party, that are using or (except after the UITMR Period where that Party has indicated that it does not wish to use it) capable of using installed Shared Solution Alt HAN Equipment;

(u) ('*point-to-point Alt HAN Equipment*') the number of Smart Metering Systems (as measured at the end of that Charging Period) associated with an MPAN at premises supplied with electricity by that Party, or with an MPRN at premises supplied with gas by that Party, that are using or capable of using installed Point-to-Point Alt HAN Equipment; and

(v) ('*stock level point-to-point Alt HAN Equipment*') the number of items of Point-to-Point Alt HAN Equipment (as measured at the end of that Charging Period) delivered to that Party but not installed.

Explicit Charges

K7.6 The DCC will determine the Explicit Charges for each Explicit Charging Metric and each Regulatory Year:

(a) in the case of the Explicit Charging Metrics referred to in Section K7.5(a) and (b) ('security assessments' and 'privacy assessments'), so as to pass-through to each Party the relevant expenditure incurred by the Panel in respect of the Explicit Charging Metric as notified by the Panel to the DCC for the purpose of establishing such Charges;

(b) (subject to Section K7.6(a)) in a manner consistent with the Charging Objectives referred to in Sections C1.4, C1.5 and C1.6(a), (b), and (c);

(c) (subject to Section K7.6(a) and the Charging Objective referred to in Section C1.4) on a non-discriminatory and cost reflective basis so as to recover the incremental cost to the DCC (including under the DCC Service Provider Contracts) associated with the occurrence of that Explicit Charging Metric (and disregarding any costs and expenses that would be incurred whether or not that Explicit Charging Metric occurred);

(d) in the case of the Explicit Charging Metrics referred to in Section K7.5(c) and (d) ("LV gateway connection' and 'HV gateway connection'), the Explicit Charges may comprise an initial connection charge and an ongoing annual charge (which annual charge may be payable monthly or less frequently);

(e) in the case of the Explicit Charging Metrics referred to in Section K7.5(j) ('communication services'), in accordance with (c) above; save that (where the cost of implementing an Explicit Charge for one or more of the Services referred to in that Section would be disproportionate to the cost-reflective incremental cost) the Explicit Charge for those Services may be set at zero;

(f) in the case of the Explicit Charging Metrics referred to in Section K7.5(l), (m), (n), (o) and (p) ('CH stock level charge', 'CH variant charge', 'CH auxiliary equipment', 'CH returned and redeployed', and 'CH returned not redeployed'), so as to ensure they are uniform across each month of a Regulatory Year and across each Region and do not make any distinction linked to use at Domestic Premises or Non-Domestic Premises;

(g) in the case of the Explicit Charging Metric referred to in Section K7.5(m) ('CH variant charge'), in accordance with (c) above, for which purpose the incremental cost to DCC shall be the cost to the DCC of the Variant Communications Hub as compared to the cost to the DCC of the Standard Communications Hub;

(h) so that the Explicit Charging Metric referred to in Section K7.5(o) ('CH returned and redeployed') is not more than the Explicit Charging Metric referred to in Section K7.5(p) ('CH returned not redeployed');

(i) in the case of the Explicit Charging Metric referred to in Section K7.5(p) ('CH returned not redeployed'), in accordance with (c) above, for which purpose the incremental cost to DCC shall include any early termination fee payable in relation to the Communications Hub, or (if applicable) the net present value of the ongoing costs likely to be incurred by the DCC notwithstanding the fact that the Communications Hub has been removed, lost or destroyed; and

(j) in the case of the Explicit Charging Metrics referred to in Section K7.5(t), (u)

and (v) ('shared solution Alt HAN Equipment', 'point-to-point Alt HAN Equipment' and 'stock level point-to-point Alt HAN Equipment), so as to pass-through to each Party the relevant costs of AltHANCo in respect of the Explicit Charging Metric as notified by AltHANCo to the DCC for the purpose of establishing such Charges.

K7.7 This Section K7.7 applies only in respect of the Explicit Charging Metrics referred to in Sections K7.5(f) and (g) ('elective service evaluation' and 'P&C support'). Where the DCC is simultaneously considering requests for an Explicit Charging Metric from two or more Parties, and where it would be advantageous to all such Parties for the DCC to do so, the DCC shall offer the Explicit Charging Metrics both conditionally on all the Parties taking up the Explicit Charging Metric and without such condition. In respect of the Explicit Charges to apply in respect of the conditional offer, the DCC shall calculate the Explicit Charges for each Party on the assumption that the other Parties accept the offers, and shall accordingly apportion any common costs between the Parties on a non-discriminatory and cost-reflective basis.

Second-Comer Contributions

K7.8 This Section K7.8 applies only in respect of the Explicit Charging Metrics referred to in Sections K7.5(c), (d), (f) and (g) ('LV gateway connection', 'HV gateway connection', 'elective service evaluation' and 'P&C support'). Subject to Section K7.10, where:

(a) the DCC makes an offer in respect of any proposed Explicit Charging Metric to a person (the "**subsequent person**"); and

(b) prior to such offer being made to the subsequent person, another person (the "**initial contributor**") was obliged to pay Explicit Charges designed to recover any costs (the "**relevant costs**") that would otherwise (in accordance with this Charging Methodology) have been recoverable from the subsequent person,

then the DCC shall make an offer to the subsequent person that requires that subsequent person to pay by way of Explicit Charges such a contribution to the relevant costs as may be reasonable in all the circumstances.

K7.9 Subject to Section K7.10, where an offer made by the DCC that includes an element of relevant costs is accepted by the subsequent person, the DCC shall (following payment by the subsequent person) offer such rebate to the initial contributor as may be reasonable in all the circumstances.

K7.10 Sections K7.8 and K7.9 shall not apply:

(a) where the relevant costs are less than £20,000;

(b) where the relevant costs are between £20,000 and £500,000 (inclusive), and the initial contributor's offer for the Explicit Charging Metric was accepted more than 5 years before the offer to the subsequent contributor is made;

(c) where the relevant costs are more than £500,000, and the initial contributor's offer for the Explicit Charging Metric was accepted more than 10 years before the offer to the subsequent contributor is made; and/or

(d) where the initial contributor no longer exists or cannot be contacted by the DCC following reasonable enquiry.

K7.11 All references to an initial contributor in this Section K7 shall, in respect of any subsequent person, be interpreted so as to include any person that was previously a subsequent person in respect of the relevant costs in question and that paid Explicit Charges designed to recover an element of those relevant costs.

K8 DETERMINING ELECTIVE CHARGES

Introduction

K8.1 The Elective Charges for each Regulatory Year are payable in accordance with the relevant Bilateral Agreement.

K8.2 The terms and conditions of each Bilateral Agreement (including those in respect of the Elective Charges payable thereunder) are to be agreed or determined in accordance with Section H7 (Elective Communication Services) and the DCC Licence.

Determining the Elective Charges

K8.3 Where the DCC makes any offer to enter into a Bilateral Agreement in respect of an Elective Communication Service, the DCC shall offer Elective Charges in respect of each such Elective Communication Service determined by the DCC:

(a) in a manner consistent with the Charging Objectives referred to in Sections C1.6(a), (b), and (c);

(b) in a non-discriminatory and cost-reflective manner, so as to recover the total costs to the DCC (including under the DCC Service Provider Contracts) associated with that Bilateral Agreement (including so as to recover a reasonable proportion of any standing costs that would be incurred whether or not that Elective Communication Service was provided); and

(c) so that such proportion of such standing costs is recovered by way of a standing charge that is payable whether or not the service is requested or provided.

K8.4 Where the DCC is simultaneously considering requests for a formal offer to provide Elective Communication Services from two or more Parties, and where it would be advantageous to all such Parties for the DCC to do so, the DCC shall make the offer both conditionally on all the Parties accepting the offer and without such condition. In respect of the Elective Charges to apply in respect of the conditional offer, the DCC shall calculate the Elective Charges for each Party on the assumption that the other

Parties accept the offers, and shall accordingly apportion any common costs between the Parties on a non-discriminatory and cost-reflective basis.

K8.5 Although this Code in no way binds the Authority it is acknowledged that any determination by the Authority of the Elective Charges in respect of a Bilateral Agreement will be undertaken as envisaged by the DCC Licence, including by reference to those matters set out in Sections K8.3 and K8.4.

Second-Comer Contributions

K8.6 Subject to Section K8.8, where:

(a) the DCC makes an offer in respect of any proposed Elective Communications Service to a person (the "**subsequent person**"); and

(b) prior to such offer being made to the subsequent person, another person (the "**initial contributor**") was obliged to pay Elective Charges designed to recover any costs (the "**relevant costs**") that would otherwise (in accordance with this Charging Methodology) have been recoverable from the subsequent person,

then the DCC shall make an offer to the subsequent person that requires that subsequent person to pay by way of Elective Charges such a contribution to the relevant costs as may be reasonable in all the circumstances.

K8.7 Subject to Section K8.8, where an offer made by the DCC that includes an element of relevant costs is accepted by the subsequent person, the DCC shall (following payment by the subsequent person) offer such rebate to the initial contributor as may be reasonable in all the circumstances.

K8.8 Sections K8.6 and K8.7 shall not apply:

(a) where the relevant costs are less than £20,000;

(b) where the relevant costs are between £20,000 and £500,000 (inclusive), and the initial contributor's offer for the Elective Communication Service was accepted more than 5 years before the offer to the subsequent contributor is

made;

(c) where the relevant costs are more than £500,000, and the initial contributor's offer for the Elective Communication Service was accepted more than 10 years before the offer to the subsequent contributor is made; and/or

(d) where the initial contributor no longer exists or cannot be contacted by the DCC following reasonable enquiry.

K8.9 All references to an initial contributor in this Section K8 shall, in respect of any subsequent person, be interpreted so as to include any person that was previously a subsequent person in respect of the relevant costs in question and that paid Elective Charges designed to recover an element of those relevant costs.

K9 WITHIN-YEAR ADJUSTMENTS

Introduction

K9.1 The revenue restriction contained in the DCC Licence allows the DCC to carry forward any under or over recovery in respect of one Regulatory Year to the following Regulatory Year. Therefore, there is no absolute need for the DCC to alter the Charges part way through a Regulatory Year.

K9.2 Nevertheless, subject to compliance with Condition 19 of the DCC Licence, the DCC may alter the Charges part way through a Regulatory Year, including in one of the following two ways:

(a) where this Charging Methodology is amended and the amendment has effect part way through a Regulatory Year; or

(b) where the requirements of this Section K9 are met, by applying within-year adjustments for the matters set out in this Section K9.

Amending this Charging Methodology

K9.3 Where the Authority consents in accordance with Condition 19 of the DCC Licence, the DCC may recalculate the Charges in accordance with this Charging Methodology (including so as to take into account any modification of this Charging Methodology). In such circumstances, the references herein to a Regulatory Year shall be interpreted as meaning the remaining period of such Regulatory Year from the time at which the modified Charges in question are to apply.

Within-Year Adjustment for Bad Debt

K9.4 Where a Party fails to pay to the DCC an amount due by way of Charges such that an Event of Default has occurred, and provided the DCC has complied with its obligations under Section J (Charges) in respect of the same, the DCC may (where it reasonably considers it appropriate to do so, taking into account the matters referred to in Section K9.1) determine the **Unrecovered Bad Debt Payment** ($UBDP_{pemt}$) to be paid by every Compliant Party (p) in respect of that Event of Default (e) in one or more subsequent months (m) of such Regulatory Year (t) as the DCC may determine.

$UBDP_{pemt}$ shall be calculated as follows:

$$UBDP_{pemt} = \frac{UBP_e \times DS_{pe}}{BM_e}$$

Where:

BM_e is the number of months in the balance of the Regulatory Year over which the DCC decides it is to recover the amount owing in respect of the Event of Default

UBP_e is the amount owing in respect of the Event of Default (e) or such smaller amount as DCC decides to recover over the remainder of the Regulatory Year (t)

DS_{pe} is the share of the debt owing in respect of the Event of Default (e) to be paid by each Compliant Party (p), which is to be calculated as follows.

$$DS_{pe} = \frac{TMP_{pe}}{\sum_{\forall p} TMP_{pe}}$$

where TMP_{pe} is the total amount paid or payable by way of Charges by each Compliant Party (p) in respect of the 12 months preceding the month in respect of which the Event of Default (e) occurred

$\sum_{\forall p}$ represents a sum over all Compliant Parties for the Event of Default.

K9.5 Where the DCC:

(a) has levied a charge for an Unrecovered Bad Debt Payment; and

(b) subsequently recovers from the defaulting Party any or all of the unpaid debt to which the Unrecovered Bad Debt Payment related,

then the DCC shall return the money it has recovered from the defaulting Party to the Compliant Parties in proportion to their contributions to $UBDP_{pemt}$. In order to return

such money, the DCC shall include a negative $UBDP_{pemt}$ amount in the Charges for the month following the month in which the DCC received payment (or part payment) from the defaulting Party.

Within-Year Adjustment for Liability Events

K9.6 If a Liability Event arises, the DCC may (where it reasonably considers it appropriate to do so, taking into account the matters referred to in Section K9.1 and having consulted with the Authority and the Panel) determine the **Liability Payment** (LP_{plmt}) to be paid by (or, in the case of negative Liability Sums, paid to) every other Party (p) in respect of that Liability Event (l) in one or more subsequent months (m) of such Regulatory Year (t) as the DCC may determine. LP_{plmt} shall be calculated as follows:

$$LP_{plmt} = \frac{TLP_l \times LS_{pl}}{BM_l}$$

Where:

BM_l is the number of months in the balance of the Regulatory Year over which the DCC decides it is to recover the amount owing in respect of the Liability Event

TLP_l is the Liability Sum arising in respect of the Liability Event (l) or such smaller amount as DCC decides to recover over the remainder of the Regulatory Year (t)

LS_{pl} is the share of the liability owing in respect of the Liability Event (l) to be paid by (or, in the case of negative Liability Sums, paid to) each Party (p), which is to be calculated as follows.

$$LS_{pl} = \frac{TMP_{pl}}{\sum_{\forall p} TMP_{pl}}$$

where TMP_{pl} is the total amount paid or payable by way of Charges by each Party (p) in respect of the 12 months preceding the month in which the

Liability Sum for the Liability Event (l) is payable to or by the DCC Service Providers

$\sum_{\forall p}$ represents a sum over all Parties.

Within-Year Adjustment for Communications Hub Finance Acceleration Events

K9.7 For the purposes of Section K9.6:

(a) a Communications Hub Finance Acceleration Event is a Liability Event;

(b) the amount due and payable by the DCC as a result of a Communications Hub Finance Acceleration Event is a Liability Sum to the extent the DCC estimates that such amount will be recoverable by the DCC as Allowed Revenue;

(c) the reference to "Charges" in the definition of LS_{pl} shall (in the case of a Communications Hub Finance Acceleration Event) be interpreted as a reference to "Communications Hub Charges"; and

(d) the amount payable by each Party in respect of such Liability Event shall (for the purposes of invoicing and payment under Section J (Charges) or Section M11.5(b) (Third Party Rights)) be treated as an amount due by way of Communications Hub Finance Charges relating to the Communications Hub Finance Facility in respect of which the Communications Hub Finance Acceleration Event has occurred.

K10 CALCULATING MONTHLY PAYMENTS

Introduction

K10.1 The monthly payment of Charges payable by each Party shall be calculated in accordance with this Section K10, based on:

(a) the Fixed Charges determined in accordance with Section K4, K5 or K6 (as applicable);

(b) the Fixed Alt HAN Charges determined in accordance with Section K5A or K6B (as applicable);

(c) the Explicit Charges determined in accordance with Section K7;

(d) the Elective Charges determined in accordance with Section K8; and

(e) any within-year adjustments determined in accordance with Section K9.

Calculating Fixed Charges

K10.2 The Fixed Charges and Fixed Alt HAN Charges payable by each person in respect of any month (or part month) during a Regulatory Year shall be calculated following the end of that month based on the calculations in accordance with Section K4, K5, K5A, K6 or K6B (as applicable).

K10.3 The Fixed Charges are payable by the persons in each Charging Group, and the Fixed Alt HAN Charges are payable by the persons in the Alt HAN Charging Groups. The Fixed Charges payable by any Party that is not in a Charging Group shall be zero, and the Fixed Alt HAN Charges payable by any Party that is not in an Alt HAN Charging Group shall be zero.

Calculating Explicit Charges and Elective Charges Payments

K10.4 The Explicit Charges payable by each Party in respect of any month (or part month) during a Regulatory Year shall be calculated following the end of that month based on the Explicit Charging Metrics incurred by that Party during the Charging Period for that month.

K10.5 The Elective Charges payable by each Party in respect of any month (or part month) during a Regulatory Year shall be calculated following the end of that month based on the relevant Bilateral Agreement.

Calculating Monthly Payments

K10.6 For each month (or part month) (m) during a Regulatory Year (t) prior to the UITMR Period, the initial monthly payment (*IMP*) in respect of the Charges payable by each Party (p) shall be calculated as follows:

$$IMP_{pmt} = \sum_{\forall g}\left(FC_{gt} \times AMSMS_{pgmt}\right) + \sum_{\forall g \forall r}\left(NCHC_{grt} \times ANCH_{grt}\right) + \sum_{\forall g}\left(DCHC_{gt} \times ADCH_{gt}\right) + \sum_{i=1}^{i=n}\left(EC_{it} \times ECM_{ipmt}\right) + TEP_{pmt} + \sum_{e \in m} UBDP_{pemt} + \sum_{l \in m} LP_{plmt}$$

Where:

FC_{gt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Mandated Smart Metering Systems, calculated in accordance with Section K4

$AMSMS_{pgmt}$ = the amount described in Section K4.5

$NCHC_{grt}$ = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Smart Metering Systems for Non-Domestic Premises in Region (r)

$ANCH_{grt}$ = the amount described in Section K6A.6

$DCHC_{grt}$ = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Smart Metering Systems for Domestic Premises in Region (r)

$ADCH_{grt}$ = the amount described in Section K6A.6

EC_{it} = the Explicit Charge for an Explicit Charging Metric (i) and a Regulatory Year (t)

ECM_{ipmt} = the Explicit Charging Metrics incurred by a Party (p) during the Charging Period for that month (m) in a Regulatory Year (t)

TEP_{pmt} = the total amount payable by a Party (p) in respect of Elective Charges and a month (m) in a Regulatory Year (t)

$UBDP_{pemt}$ = the Unrecovered Bad Debt Payment in respect of a month (m) in a Regulatory Year (t) and each Event of Default (e), as calculated in accordance with Section K9

LP_{plmt} = the Liability Payment in respect of a month (m) in a Regulatory Year (t) and each Liability Event (l), as calculated in accordance with Section K9.

K10.7 For each month (or part month) (m) during a Regulatory Year (t) during the UITMR Period, the rollout monthly payment (*RMP*) in respect of the Charges payable by each Party (p) shall be calculated as follows:

$$\begin{aligned} RMP_{pmt} = & \sum_{\forall g}\left(RDFC_{gt} \times ADSMS_{pgmt}\right) + \sum_{\forall g}\left(\sum_{\forall r}\left(RNFC_{grt} \times ANSMS_{pgrmt}\right)\right) \\ & + \sum_{\forall g \forall r}\left(NCHC_{grt} \times ANCH_{grt}\right) + \sum_{\forall g}\left(DCHC_{gt} \times ADCH_{gt}\right) \\ & + \sum_{\forall g}\left(RAHFC_{gt} \times ADSMS_{pgmt}\right) + \sum_{\forall g}\left(RAHFC_{gt} \times \sum_{\forall r} ANSMS_{pgrmt}\right) \\ & + \sum_{i=1}^{i=n}\left(EC_{it} \times ECM_{ipmt}\right) + TEP_{pmt} + \sum_{e \in m} UBDP_{pemt} + \sum_{l \in m} LP_{plmt} \end{aligned}$$

Where:

$RDFC_{gt}$ = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of

Mandated Smart Metering Systems, calculated in accordance with Section K5;

$ADSMS_{pgmt}$ = the amount described as such in Section K5.9;

$RNFC_{grt}$ = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Enrolled Smart Metering Systems for Non-Domestic Premises in each Region (r), calculated in accordance with Section K5;

$ANSMS_{pgrmt}$ = the amount described as such in Section K5.7;

$NCHC_{grt}$ = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Smart Metering Systems for Non-Domestic Premises in Region (r);

$ANCH_{grt}$ = the amount described in Section K6A.6;

$DCHC_{grt}$ = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Smart Metering Systems for Domestic Premises in Region (r);

$ADCH_{grt}$ = the amount described in Section K6A.6;

$RAHFC_{gt}$ = the Fixed Alt Han Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises and Smart Metering Systems for Non-Domestic Premises calculated in accordance with Section K5A;

;

EC_{it} = the Explicit Charge for an Explicit Charging Metric (i) and a Regulatory Year (t);

ECM_{ipmt} = the Explicit Charging Metrics incurred by a Party (p) during the Charging Period for that month (m) in a Regulatory Year (t);

TEP_{pmt} = the total amount payable by a Party (p) in respect of Elective Charges and a month (m) in a Regulatory Year (t);

$UBDP_{pemt}$ = the Unrecovered Bad Debt Payment in respect of a month (m) in a Regulatory Year (t) and each Event of Default (e), as calculated in accordance with Section K9;

LP_{plmt} = the Liability Payment in respect of a month (m) in a Regulatory Year (t) and each Liability Event (l), as calculated in accordance with Section K9.

K10.8 For each month (or part month) (m) during a Regulatory Year (t) after the UITMR Period, the monthly payment (*MP*) in respect of the Charges payable by each Party (p) shall be calculated as follows:

$$MP_{pmt} = \sum_{\forall g}\left(DFC_{gt} \times ADSMS_{pgmt}\right) + \sum_{\forall g}\left(\sum_{\forall r}\left(NFC_{grt} \times ANSMS_{pgrmt}\right)\right) + \sum_{\forall g \forall r}\left(NCHC_{grt} \times ANCH_{grt}\right) + \sum_{\forall g}\left(DCHC_{gt} \times ADCH_{gt}\right) + \sum_{\forall g}\left(DAHFC_{gt} \times ADSMS_{pgmt}\right) + \sum_{\forall g}\left(NAHFC_{gt} \times \sum_{\forall r} ANSMS_{pgrmt}\right) + \sum_{i=1}^{i=n}\left(EC_{it} \times ECM_{ipmt}\right) + TEP_{pmt} + \sum_{e \in m} UBDP_{pemt} + \sum_{l \in m} LP_{plmt}$$

Where:

DFC_{gt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Enrolled Smart Metering Systems for Domestic Premises, calculated in accordance with Section K6;

$ADSMS_{pgmt}$ = the amount described as such in Section K6.7;

NFC_{grt} = the Fixed Charges payable in respect of months (or part months) during Regulatory Year (t) by persons in Charging Group (g) in respect of Enrolled Smart Metering Systems for Non-Domestic Premises in each Region (r), calculated in accordance with Section K6;

$ANSMS_{pgrmt}$ = the amount described as such in Section K6.7;

$NCHC_{grt}$ = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Smart Metering Systems for Non-Domestic Premises in Region (r);

$ANCH_{grt}$ = the amount described in Section K6A.6;

$DCHC_{grt}$ = the Fixed CH Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in CH Charging Group (g) in respect of Smart Metering Systems for Domestic Premises in Region (r);

$ADCH_{grt}$ = the amount described in Section K6A.6;

$DAHCFC_{gt}$ = the Domestic Fixed Alt Han Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in Alt HAN Charging Group (g) in respect of Mandated Smart Metering Systems for Domestic Premises calculated in accordance with Section K6B;

$NAHFC_{gt}$ = the Non-Domestic Fixed Alt Han Central Charge payable in respect of months (or part months) during Regulatory Year (t) by persons in Alt HAN Charging Group (g) in respect of Mandated Smart Metering Systems for Non-Domestic Premises calculated in accordance with Section K6B;

EC_{it} = the Explicit Charge for an Explicit Charging Metric (i) and a Regulatory Year (t);

ECM_{ipmt} = the Explicit Charging Metrics incurred by a Party (p) during the Charging Period for that month (m) in a Regulatory Year (t);

TEP_{pmt} = the total amount payable by a Party (p) in respect of Elective Charges and a month (m) in a Regulatory Year (t);

$UBDP_{pemt}$ = the Unrecovered Bad Debt Payment in respect of a month (m) in a Regulatory Year (t) and each Event of Default (e), as calculated in accordance with Section K9;

LP_{plmt} = the Liability Payment in respect of a month (m) in a Regulatory Year (t) and each Liability Event (l), as calculated in accordance with Section K9.

K11 DEFINITIONS

K11.1 In this Charging Methodology, except where the context otherwise requires, the expressions in the left hand column below shall have the meanings given to them in the right hand column below:

Allowed Revenue	has the meaning given to that expression in the revenue restriction conditions of the DCC Licence.
Alt HAN Charging Group	has the meaning given to that expression in Section K3.10.
Alt HAN Charging Group Weighting Factors	has the meaning given to that expression in Section K3.15.
Alt HAN Cost Domestic Allocation	has the meaning given to that expression in Section K3.20.
Alt HAN Costs	has the meaning given to that expression in Section Z6.1.
Alt HAN Fixed Revenue	has the meaning given to that expression in Section K3.7.
AltHANCo	has the meaning given to that expression in Section Z6.1.
Charging Group	has the meaning given to that expression in Section K3.10.
Charging Group Weighting Factor	has the meaning given to that expression in Section K3.13.
Charging Period	means, in respect of each month (the 'current month'),

	the period from the start of the 16th day of the previous month to the end of the 15th day of the current month.
CH Charging Group	has the meaning given to that expression in Section K3.9.
CH Charging Group Weighting Factor	has the meaning given to that expression in Section K3.14.
Compliant Party	means, in respect of any Event of Default giving rise to an Unrecovered Bad Debt Payment, all of the Parties other than: (a) the Defaulting Party in respect of that Event of Default; and (b) the Defaulting Party in respect of any other Event of Default giving rise to an Unrecovered Bad Debt Payment that is calculated under Section K9.4 during the same month as the Unrecovered Bad Debt Payment to which reference is first made in this definition.
Elective Charges	means the Charges payable in respect of Elective Communication Services.
Enrolled Smart Metering System	means a Smart Metering System that has been Enrolled.
Estimated Allowed Revenue	has the meaning given to that expression in Section K2.1.
Estimated Elective Service Revenue	has the meaning given to that expression in Section K2.3.
Estimated Explicit Charges Revenue	has the meaning given to that expression in Section K2.5.

Estimated Fixed Charges Revenue	has the meaning given to that expression in Section K2.6.
Explicit Charges	means the Charges calculated in accordance with Section K7, and payable in respect of the Explicit Charging Metrics.
Explicit Charging Metrics	has the meaning given to that expression in Section K7.
Fixed Alt HAN Charges	means the Charges calculated in accordance with Section K5A or K6B (as applicable).
Fixed CH Charges	means the Charges calculated in accordance with Section K6A.
Fixed Charges	means the Charges calculated in accordance with Section K4, K5 or K6 (as applicable).
Liability Event	means an event as a result of which either: (a) the DCC has a net liability to the DCC Service Providers collectively (excluding in respect of charges arising in the ordinary course of events); or (b) the DCC Service Providers collectively have a net liability to the DCC (excluding in respect of service credits or liquidated damages arising from poor service performance).
Liability Sum	means, in respect of a Liability Event as a result of which: (a) the DCC owes a net liability to the DCC Service

Providers collectively, the amount of such net liability (having taken into account amounts recoverable by the DCC in respect of that Liability Event otherwise than pursuant to this Charging Methodology, including amounts recoverable from other Parties as a result of any breach of this Code by such Parties which caused or contributed to that Liability Event), but only to the extent that the DCC estimates that such net liability will be recoverable by the DCC as Allowed Revenue; or

(b) the DCC Service Providers collectively owe a net liability to the DCC, the net amount actually received by the DCC in respect of such net liability (having taken into account amounts owed by the DCC to other Parties and to third parties in respect of that Liability Event otherwise than pursuant to this Charging Methodology), but only to the extent that the DCC estimates that such net liability will reduce the Allowed Revenue that the DCC could otherwise recover by way of the Charges (which net amount will be expressed as a negative number).

Liability Payment has the meaning given to that expression in Section K9.6 (expressed as a negative number in the case of negative Liability Sums).

Mandated Smart Metering System means, from time to time, each MPAN or MPRN associated with a Domestic Premises (regardless of whether or not a Smart Metering System has been installed or Enrolled), but excluding:

(a) those MPANs and MPRNs associated with premises in respect of which the DCC is exempted from the requirement to Enrol Smart Metering Systems in accordance with the Statement of Service Exemptions; and

(b) those MPANs that do not have the status of "traded" (as identified in the MRA) and those MPRNs that do not have a status that indicates that gas is off-taken at the supply point (as identified in the UNC).

National Fixed Revenue	has the meaning given to that expression in Section K3.7.
Non-Domestic Withdrawal Factor	has the meaning given to that expression in Section K3.18.
Regional Communications Hub Revenue	has the meaning given to that expression in Section K3.9.
Regional Fixed Revenue	has the meaning given to that expression in Section K3.9.
Regulatory Year	means (subject to Section K9.3) a period of twelve months beginning at the start of 1 April in any calendar year and ending at the end of 31 March in the next following calendar year; provided that a Regulatory Year will end and a new one will commence simultaneously with both the commencement and the end of the UITMR Period.
Standard Communications	means, in respect of each Region, Communications Hubs of the HAN Variant which cost the DCC the least

Hubs	to procure in respect of that Region (to be judged in respect of each Regulatory Year at the time at which the DCC is stabling its Charges for that Regulatory Year).
UITMR Period	means the period, covering User integration testing and the mass rollout period, which for these purposes: (a) commences at the start of the month in which the DCC is first obliged to make regular monthly payments to one or more of the DCC Service Providers; and (b) ends at the end of the date referred to in paragraph 1 of Condition 39 of the Energy Supply Licences.
Unrecovered Bad Debt Payment	has the meaning given to that expression in Section K9.4.
Variant Communication Hubs	means, in respect of each Region, all Communications Hubs of the HAN Variant that is not the Standard Communications Hub for that Region.
Weighting Factor	means the Charging Group Weighting Factor, the CH Charging Group Weighting Factor or the Alt HAN Charging Group Weighting Factor.

SECTION L – SMART METERING KEY INFRASTRUCTURE AND DCC KEY INFRASTRUCTURE

L1 SMKI POLICY MANAGEMENT AUTHORITY

Establishment of the SMKI PMA

L1.1 The Panel shall establish a Sub-Committee in accordance with the requirements of this Section L1, to be known as the "**SMKI PMA**".

L1.2 Save as expressly set out in this Section L1, the SMKI PMA shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

Membership of the SMKI PMA

L1.3 The SMKI PMA shall be composed of the following persons (each an "**SMKI PMA Member**"):

(a) the SMKI PMA Chair (as further described in Section L1.5);

(b) three SMKI PMA (Supplier) Members (as further described in Section L1.6);

(c) one SMKI PMA (Network) Member (as further described in Section L1.8); and

(d) one representative of the Security Sub-Committee and one representative of the Technical Architecture and Business Architecture Sub-Committee (in each case as further described in Section L1.10).

L1.4 Each SMKI PMA Member must be an individual (and cannot be a body corporate, association or partnership). No one person can hold more than one office as an SMKI PMA Member at the same time.

L1.5 The "**SMKI PMA Chair**" shall be such person as is (from time to time) appointed to that role by the Panel in accordance with a process designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the SMKI PMA Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(c) the SMKI PMA Chair is remunerated at a reasonable rate;

(d) the SMKI PMA Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members); and

(e) provision is made for the SMKI PMA Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

L1.6 Each of the three "**SMKI PMA (Supplier) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section L1 into this Code):

(a) be appointed in accordance with Section L1.7, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire 2 years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "SMKI PMA (Supplier) Member", references to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", and references to "Panel Members" were to "SMKI PMA Members".

L1.7 Each of the three SMKI PMA (Supplier) Members shall be appointed in accordance with a process:

(a) by which two SMKI PMA (Supplier) Members will be elected by Large Supplier Parties, and one SMKI PMA (Supplier) Member will be elected by Small Supplier Parties;

(b) by which any person (whether or not a Supplier Party) shall be entitled to

nominate candidates to be elected as an SMKI PMA (Supplier) Member; and

(c) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SKMI PMA Chair", references to "Panel Members" were to "SMKI PMA Members", and references to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section L1).

L1.8 The "**SMKI PMA (Network) Member**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section L1 into this Code):

(a) be appointed in accordance with Section L1.9, subject to compliance by the appointed person with Section C6.9 (Member Confirmation);

(b) retire 2 years after his or her appointment (without prejudice to his or her ability to be nominated for a further term of office); and

(c) be capable of being removed from office in accordance with Sections C4.5 and C4.6 (Removal of Elected Members), for which purpose those Sections shall be read as if references to "Elected Member" were to "SMKI PMA (Network) Member", references to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", and references to "Panel Members" were to "SMKI PMA Members".

L1.9 The SMKI PMA (Network) Member shall be appointed in accordance with a process:

(a) by which the SMKI PMA (Network) Member will be elected by the Electricity Network Parties and the Gas Network Parties together (as if they formed a single Party Category, but so that Electricity Network Party Voting Groups and Gas Network Party Voting Groups each have one vote); and

(b) that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "SMKI PMA", to "Panel Chair" were to "PMA Chair", to "Panel Members" were to "SMKI PMA Members", and to provisions of Section C or D were to the

corresponding provisions set out in or applied pursuant to this Section L1).

L1.10 The Security Sub-Committee and the Technical Architecture and Business Architecture Sub-Committee shall each nominate one of their members to be an SMKI PMA Member by notice to the Secretariat from time to time. The Security Sub-Committee or the Technical Architecture and Business Architecture Sub-Committee (as applicable) may each replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation). Until each such Sub-Committee exists, the Panel shall nominate a person to act as a representative of that Sub-Committee (and may from time to time replace such person).

L1.11 Each SMKI PMA Member must ensure that he or she reads the SMKI Document Set when first appointed, and subsequently from time to time, so that he or she is familiar with its content.

Proceedings of the SMKI PMA

L1.12 Each SMKI PMA Member shall be entitled to appoint an Alternate in accordance with Section C5.19 (as it applies pursuant to Section L1.15); provided that:

(a) the SMKI PMA Chair will be deemed to have nominated the SMKI Specialist to act as Alternate for the SMKI PMA Chair;

(b) where the SMKI Specialist is unavailable, the SMKI PMA Chair must nominate another person to act as Alternate for the SMKI PMA Chair (which person may not be another SMKI PMA Member, and which person must be sufficiently independent of any particular Party or class of Parties); and

(c) the person so appointed by each SMKI PMA Member (other than the SMKI PMA Chair) may not be employed by the same organisation as employs that SMKI PMA Member (or by an Affiliate of that SMKI PMA Member's employer).

L1.13 No business shall be transacted at any meeting of the SMKI PMA unless a quorum is present at that meeting. The quorum for each such meeting shall be four of the SMKI PMA Members, at least one of whom must be the SMKI PMA Chair (or his or her

Alternate).

L1.14 Without prejudice to the generality of Section C5.13(c) (Attendance by Other Persons) as it applies pursuant to Section L1.15:

(a) the SMKI Specialist and a representative of the DCC shall be invited to attend each and every SMKI PMA meeting (each of whom shall be entitled to speak at SMKI PMA meetings without the permission of the SMKI PMA Chair); and

(b) other persons who may be invited to attend SMKI PMA meetings may include:

(i) the Independent SMKI Assurance Service Provider;

(ii) one or more representatives of Device Manufacturers; or

(iii) a specialist legal adviser.

L1.15 Subject to Sections L1.12, L1.13 and L1.14, the provisions of Section C5 (Proceedings of the Panel) shall apply to the proceedings of the SMKI PMA, for which purpose that Section shall be read as if references to "Panel" were to "SMKI PMA", references to "Panel Chair" were to "SMKI PMA Chair", and references to "Panel Members" were to "SMKI PMA Members".

L1.16 Notwithstanding Section C3.12 (Protections for Panel Members and Others), that Section shall not apply to the SMKI Specialist when acting as the SMKI PMA Chair's Alternate, and the SMKI Specialist shall have no rights under that Section.

Duties of the SMKI PMA

L1.17 The SMKI PMA shall undertake the following duties:

(a) to approve the Device CPS, Organisation CPS and the IKI CPS, and any changes to those documents, in accordance with Sections L9;

(b) to propose variations to the SMKI SEC Documents, as further described in Section L1.19;

(c) to periodically review (including where directed to do so by the Panel) the effectiveness of the SMKI Document Set (including so as to evaluate whether

the SMKI Document Set remains consistent with the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the SMKI PMA considers appropriate);

(d) as soon as reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (c) above:

(i) the SMKI Compliance Policy;

(ii) the SMKI RAPP;

(iii) the Device Certificate Policy;

(iv) the Organisation Certificate Policy;

(v) the IKI Certificate Policy;

(vi) the SMKI Recovery Procedure,

and (where the SMKI PMA considers it appropriate to do so) submit one or more Modification Proposals in respect of those documents (which Modification Proposals shall, notwithstanding Section X2.3(a), (b) and (c), be subject to Section D (Modification Process) as varied by Section X2.3(d));

(e) to periodically review the effectiveness of the DCCKI Document Set and to:

(i) notify DCC where it considers that changes should be made to the DCCKI Document Set in order to ensure that DCC meets its obligations under Section G (Security) (such notification to include any recommendation for action that the SMKI PMA considers appropriate); and

(ii) copy any such notification to the Security Sub-Committee and, except to the extent that it is appropriate to redact information for security purposes, to other SEC Parties;

(f) as soon as reasonably practicable following the incorporation of each of the

following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (e) above:

(i) the DCCKI RAPP;

(ii) the DCCKI Certificate Policy;

(g) to review the DCCKI CPS, and any amendments proposed to be made to it by the DCC, in accordance with Section L13 (DCC Key Infrastructure);

(h) as part of its review of the SMKI Compliance Policy pursuant to paragraph (d) above, to consider whether SMKI Participants which are subject to assurance assessments pursuant to the SMKI Compliance Policy should be liable to meet the costs (or a proportion of the costs) of undertaking such assessments, and (where the SMKI PMA considers it appropriate to do so) submit one or more Modification Proposals as referred to in paragraph (d) above;

(i) in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, to decide, in accordance with the SMKI Recovery Key Guidance, whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key);

(j) to exercise the functions allocated to it under the SMKI Recovery Procedure, and in particular to exercise any power to nominate Parties for such purposes (and in accordance with such procedures) as may be set out in the SMKI Recovery Procedure;

(k) to provide the Panel, the Change Board and Working Groups with support and advice in respect of Modification Proposals that provide for variations to the SMKI SEC Documents or the DCCKI SEC Documents;

(l) to provide assurance in accordance with Section L2 (SMKI Assurance);

(m) to provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the SMKI Document Set or the DCCKI Document Set;

(n) to provide the Panel and Sub-Committees with general advice and support with respect to the SMKI Services, the SMKI Repository Service, the DCCKI Services and the DCCKI Repository Service;

(o) to exercise such functions as are allocated to it under, and to comply with all the applicable requirements of, the SMKI Document Set in accordance with Section L9.1; and

(p) to perform any other duties expressly ascribed to the SMKI PMA elsewhere in this Code.

L1.18 The SMKI PMA shall establish a process whereby the Code Administrator monitors Modification Proposals with a view to identifying (and bringing to the SMKI PMA's attention) those proposals that are likely to affect the SMKI SEC Documents. The Code Administrator shall comply with such process.

Modification of the SMKI SEC Documents by the SMKI PMA

L1.19 Notwithstanding Section D1.3 (Persons Entitled to Submit Modification Proposals):

(a) the SMKI PMA shall be entitled to submit Modification Proposals in respect of the SMKI SEC Documents where the SMKI PMA considers it appropriate to do so; and

(b) any SMKI PMA Member shall be entitled to submit Modification Proposals in respect of the SMKI SEC Documents where he or she considers it appropriate to do so (where the SMKI PMA has voted not to do so).

L2 SMKI ASSURANCE

SMKI Compliance Policy

L2.1 The SMKI PMA shall exercise the functions allocated to it by the SMKI Compliance Policy.

L2.2 The DCC shall procure all such services as are required for the purposes of complying with its obligations under the SMKI Compliance Policy.

SMKI Participants: Duty to Cooperate in Assessment

L2.3 Each SMKI Participant shall do all such things as may be reasonably requested by the SMKI PMA, or by any person acting on behalf of or at the request of the SMKI PMA (including in particular the Independent SMKI Assurance Service Provider), for the purposes of facilitating an assessment of that SMKI Participant's compliance with any applicable requirements of the SMKI Document Set.

L2.4 For the purposes of Section L2.3, an SMKI Participant shall provide the SMKI PMA (or the relevant person acting on its behalf or at its request) with:

(a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified; and

(b) all such other forms of cooperation as may reasonably be requested, including in particular access at all reasonable times to:

(i) such parts of the premises of that SMKI Participant as are used for; and

(ii) such persons engaged by that SMKI Participant as carry out, or are authorised to carry out,

any activities related to its compliance with the applicable requirements of the SMKI Document Set.

Events of Default

L2.5 In relation to an Event of Default which consists of a material breach by an SMKI Participant of any applicable requirements of the SMKI Document Set, the provisions

of Sections M8.2 (Notification of an Event of Default) to M8.4 (Consequences of an Event of Default) shall apply subject to the provisions of Sections L2.6 to L2.13.

L2.6 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section L2.5, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any applicable requirements of the SMKI Document Set (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

L2.7 Where in accordance with Section M8.2 the Panel receives notification that an SMKI Participant is in material breach of any applicable requirements of the SMKI Document Set, it shall refer the matter to the SMKI PMA. On any such referral, the SMKI PMA may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "SMKI PMA".

L2.8 Where the SMKI PMA has:

(a) carried out an investigation in accordance with Section M8.3; or

(b) received a report from the Independent SMKI Assurance Service Provider, following an assessment by it of the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set, concluding that the SMKI Participant has not complied with those requirements,

the SMKI PMA shall consider the information available to it and shall determine whether any non-compliance with the SMKI Document Set has occurred and, if so, whether that non-compliance constitutes an Event of Default.

L2.9 Where the SMKI PMA determines that an Event of Default has occurred, it shall:

(a) notify the relevant SMKI Participant and any other Party it considers may have been affected by the Event of Default; and

(b) refer the matter to the Panel for the Panel to determine the appropriate steps to take in accordance with Section M8.4.

L2.10 Where the Panel is considering what steps to take in accordance with Section M8.4, it shall request and consider the advice of the SMKI PMA.

L2.11 Where the Panel determines that an SMKI Participant is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the SMKI PMA.

L2.12 Where, in accordance with Section L2.11, the SMKI PMA has approved a remedial action plan in relation to the provision by the DCC of the SMKI Services, the Panel shall ensure that the approved plan (being redacted only in so far as necessary for the purposes of security) is made available to all Parties.

L2.13 Where, in accordance with Section L2.11, the SMKI PMA has approved a remedial action plan in relation to:

(a) the DCC acting in a capacity other than as the provider of the SMKI Services, the Panel may arrange for a version of the approved plan (or parts of that plan) to be made available to all the Parties; or

(b) any other SMKI Participant, the Panel may arrange for an anonymised version of the approved plan (or parts of that plan) to be made available to all the Parties,

but (in each case) only where the Panel considers that such dissemination is necessary for the purposes of security.

Emergency Suspension of SMKI Services

L2.14 Where the SMKI PMA has reason to believe that there is any immediate threat of the DCC Total System, any User Systems, any Smart Metering Systems or any RDP Systems being Compromised to a material extent by the occurrence of an event arising in relation to the SMKI Services, it may instruct the DCC immediately to suspend:

(a) the provision (in whole or in part) of the SMKI Services and/or any other Services which rely on the use of Certificates;

(b) the rights of any SMKI Participant to receive (in whole or in part) the SMKI Services and/or any other Services which rely on the use of Certificates,

and thereafter to retain that suspension in effect until such time as the SMKI PMA

instructs the DCC to reinstate the provision of the relevant Services or the rights of the SMKI Participant (as the case may be).

L2.15 Where the SMKI PMA takes any steps under Section L2.14, it:

(a) shall immediately thereafter notify the Authority;

(b) shall comply with any direction given to it by the Authority in relation to such steps; and

(c) may notify all the Parties of some or all of such steps (without identifying the SMKI Participant), but only where the Panel considers that such notification is necessary for the purposes of security.

L2.16 Any Party which is affected by the SMKI PMA taking any steps under Section L2.14 may appeal the decision to do so to the Authority, and the DCC shall comply with any decision of the Authority in respect of the matter (which shall be final and binding for the purposes of this Code).

L3 THE SMKI SERVICES

The SMKI Services

L3.1 For the purposes of this Section L3, the "**SMKI Services**" means all of the activities undertaken by the DCC in its capacity as:

(a) the Device Certification Authority;

(b) the Organisation Certification Authority; or

(c) the IKI Certification Authority,

in each case in accordance with the applicable requirements of the Code.

Authorised Subscribers

General Provisions

L3.2 For the purposes of this Section L3:

(a) ~~Any~~ any Party which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of any of the Certificate Policies~~,~~; ~~and~~

(b) any RDP which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of the Organisation Certificate Policy~~,~~; and

(c) SECCo in respect of the IKI Certificate Policy,

may apply to become an Authorised Subscriber in accordance with, and by following the relevant procedures set out in, that Certificate Policy and the SMKI RAPP.

~~L3.2~~L3.3 The DCC shall authorise SECCo, any Party or any RDP to submit a Certificate Signing Request, and so to become an Authorised Subscriber, where SECCo, that Party or that RDP has successfully completed the relevant procedures and satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP.

~~L3.3~~L3.4 The DCC shall provide any SMKI Services that may be requested by an

Authorised Subscriber where the request is made by that Authorised Subscriber in accordance with the applicable requirements of the SMKI SEC Documents.

~~L3.4~~L3.5 The DCC shall ensure that in the provision of the SMKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

~~L3.5~~L3.6 Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become an Authorised Subscriber, the Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L.

~~L3.6~~L3.7 Where a Registration Data Provider has been nominated as such by more than one Network Party:

(a) that RDP shall not, by virtue of acting in the capacity of an RDP for different Network Parties, be required to become a Subscriber for different Organisation Certificates;

(b) to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP;

(c) to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP.

Determinations by the Panel

~~L3.7~~L3.8 Where the DCC has notified SECCo, a Party or an RDP that has applied to become an Authorised Subscriber that ~~it~~ the DCC does not consider that ~~the Party or RDP~~it has satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, SECCo, that Party or that RDP (as the case may be) may refer the matter to the Panel for determination.

~~L3.8~~L3.9 Following any reference made to it under Section L3.8, the Panel:

(a) shall determine whether the relevant ~~Party or RDP~~applicant satisfies the criteria set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where the Panel determines that the ~~Party or RDP~~relevant applicant meets those criteria, it shall notify the DCC~~,~~ and the ~~Party or RDP~~applicant shall~~,~~ (subject to any other requirements of the relevant Certificate Policy or the SMKI RAPP)~~,~~ become an Authorised Subscriber.

~~L3.9~~L3.10 Subject to the provisions of Section L3.11, any such determination of the Panel shall be final and binding.

~~L3.10~~L3.11 Nothing in Sections L3.8 to L3.10 shall be taken to prevent SECCo, any Party or any RDP from making a new application to DCC to become an Authorised Subscriber, in accordance with Section L3.2, at any time.

Changes in Circumstance

~~L3.11~~L3.12 Where SECCo, a Party or an RDP which is an Authorised Subscriber becomes aware of a change in circumstance which would be likely, if it were to make a new application to the DCC to become an Authorised Subscriber, to affect whether it would satisfy the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, it shall as soon as is reasonably practicable notify the DCC of that change in circumstance.

~~L3.12~~L3.13 Where the DCC receives a notification from an Authorised Subscriber in accordance with Section L3.12, or otherwise becomes aware of a change in circumstance of the nature referred to in that Section, it shall:

(a) assess whether that ~~Party or RDP~~Authorised Subscriber continues to satisfy the relevant criteria to be an Authorised Subscriber as set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where it determines that the ~~Party or RDP~~Authorised Subscriber does not continue to satisfy the relevant criteria, notify the ~~Party or RDP~~Authorised Subscriber which, subject to Section L3.14, shall cease to be an Authorised

Subscriber in accordance with the Certificate Policy.

~~L3.13~~L3.14 Where the DCC has notified ~~a Party or RDP~~an Authorised Subscriber in accordance with Section L3.13(b):

(a) the provisions of Section L3.8 to L3.11 shall apply as if ~~that Party or RDP~~the person notified had made an unsuccessful application to become an Authorised Subscriber in respect of the relevant Certificate Policy; and

(b) where the relevant Certificate Policy is the Organisation Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, revoke any Organisation Certificates for which that ~~Party or RDP~~person is the Subscriber;

(c) where the relevant Certificate Policy is the IKI Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, take such steps in relation to any IKI Certificates for which that ~~Party or RDP~~person is the Subscriber as may be set out in that Certificate Policy or in the SMKI RAPP.

Eligible Subscribers

~~L3.14~~L3.15 An Authorised Subscriber:

(a) shall be known as an "**Eligible Subscriber**" in respect of a Certificate if it is entitled to become a Subscriber for that Certificate; and

(b) will be entitled to become a Subscriber for a Certificate only if it is identified as an Eligible Subscriber in respect of that Certificate in accordance with the following provisions of this Section L3.

Device Certificates

~~L3.15~~L3.16 A Party which is an Authorised Subscriber in accordance with the Device Certificate Policy will be an Eligible Subscriber in respect of a Device Certificate only where that Subject of that Device Certificate is one that is identified with that Party in the table immediately below.

Party	**Subject**
The DCC	Either: (a) a Communications Hub Function; or (b) a Gas Proxy Function.
An Import Supplier	Either: (a) an Electricity Smart Meter; or (b) a Type 1 Device.
A Gas Supplier	Either: (a) a Gas Smart Meter; (b) a Gas Proxy Function; or (c) a Type 1 Device.
Any other Party	Either: (a) an Electricity Smart Meter (b) a Gas Smart Meter; or (c) a Type 1 Device, but only in so far as the SMI Status of that Device is not set to 'commissioned' or 'installed not commissioned'.

DCA Certificates

L3.17 Where the DCC (acting in its capacity as Root DCA or Issuing DCA) is an Authorised Subscriber in accordance with the Device Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of DCA Certificates;

(b) (save for the purposes of the replacement of the Root DCA Certificate) it will be an Eligible Subscriber only in respect of a single Root DCA Certificate.

Organisation Certificates

L3.18 Where the DCC, a Network Party or another Party which is (or is to become) a User, or any RDP, is an Authorised Subscriber in accordance with the Organisation Certificate Policy, that person will be an Eligible Subscriber in respect of an Organisation Certificate only where:

(a) if the Subject of that Certificate is:

(i) either the DCC (acting pursuant to its powers or duties under the Code) or a DCC Service Provider, that person is the DCC; or

(ii) not the DCC, that person is the Subject of the Certificate; and

(b) if the value of the OrganizationalUnitName field in that Certificate is a Remote Party Role corresponding to that listed in the table immediately below, either:

(i) that person is the DCC, and the Remote Party Role is not one in relation to which a Device may require to undertake processing in accordance with the GB Companion Specification; or

(ii) that person is identified with that Remote Party Role in the second column of that table, and the value of the subjectUniqueID field in the Certificate is a User ID or RDP ID associated with any such User Role or with an RDP as may be identified in the third column of that table.

Remote Party Role	**Party**	**User Role or RDP**
Root	The DCC	[Not applicable]
Recovery	The DCC	[Not applicable]
Transitional CoS	The DCC	[Not applicable]
wanProvider	The DCC	[Not applicable]
Access Control	The DCC	[Not applicable]

Broker		
Issuing Authority	The DCC	[Not applicable]
networkOperator	A Network Party	Either: (a) Electricity Distributor; or (b) Gas Transporter.
supplier	A Supplier Party	Either: (a) Import Supplier; or (b) Gas Supplier.
other	An RDP or any Party other than the DCC	Either: (a) Other User; (b) Registered Supplier Agent; (c) Registration Data Provider; or (d) Export Supplier.

OCA Certificates

L3.19 Where the DCC (acting in its capacity as Root OCA or Issuing OCA) is an Authorised Subscriber in accordance with the Organisation Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of OCA Certificates;

(b) (save for the purposes of the replacement of the Root OCA Certificate) it will be an Eligible Subscriber only in respect of a single Root OCA Certificate.

IKI Certificates

L3.20 Where SECCo or ~~A~~any Party or RDP ~~which~~ is an Authorised Subscriber in accordance with the IKI Certificate Policy, it will be an Eligible Subscriber in respect of an IKI Certificate.

ICA Certificates

L3.21 Where the DCC (acting in its capacity as Root ICA or Issuing ICA) is an Authorised Subscriber in accordance with the IKI Certificate Policy:

(a) it (and only it) will be an Eligible Subscriber in respect of ICA Certificates;

(b) (save for the purposes of the replacement of the Root ICA Certificate) it will be an Eligible Subscriber only in respect of a single Root ICA Certificate.

Certificates for Commissioning of Devices

L3.22 The DCC shall:

(a) prior to the commencement of Interface Testing, or by such later date as may be specified by the Secretary of State, establish and lodge in the SMKI Repository; and

(b) subsequently maintain,

such of its Certificates as are necessary to facilitate the installation at premises of Devices that are capable of being Commissioned.

L3.23 For the purposes of Section L3.22, the DCC shall ensure that the Certificates which are established, lodged in the SMKI Repository and subsequently maintained include at least the following:

(a) the Root OCA Certificate;

(b) the Issuing OCA Certificate;

(c) the Root DCA Certificate;

(d) the Issuing DCA Certificate;

(e) the Recovery Certificate;

(f) the DCC (Access Control Broker) - digitalSignature Certificate;

(g) the DCC (Access Control Broker) – keyAgreement Certificate;

(h) the DCC (wanProvider) Certificate; and

(i) the DCC (transitionalCoS) Certificate.

L3.24 For the purposes of Sections L3.23(e) - (i), the Certificates which are referred to in those paragraphs mean Organisation Certificates in respect of which, in each case:

(a) the value of the KeyUsage field is that identified in relation to the Certificate in the second column of the table immediately below;

(b) the value of the OrganizationalUnitName field corresponds to the Remote Party Role identified in relation to the Certificate in the third column of that table; and

(c) the Certificate is used for the purposes of discharging the obligations of the DCC in the role identified in relation to it in the fourth column of that table.

Certificate	**KeyUsage Value**	**Remote Party Role**	**DCC Role**
Recovery Certificate	digitalSignature	Recovery	The role of the DCC under the SMKI Recovery Procedure.
DCC (Access Control Broker) - digitalSignature Certificate	digitalSignature	AccessControlBroker	AccessControlBroker
DCC (Access Control Broker) – keyAgreement Certificate	KeyAgreement	AccessControlBroker	AccessControlBroker
DCC (wanProvider) Certificate	digitalSignature	wanProvider	wanProvider

DCC (transitionalCoS) Certificate	digitalSignature	Transitional CoS	The role of the DCC as CoS Party.

Definitions

L3.25 For the purposes of this Section L3:

(a) "**KeyUsage**" means the field referred to as such in the Organisation Certificate Policy;

(b) "**OrganizationalUnitName**" and "**subjectUniqueID**" mean those fields which are identified as such in the Organisation Certificate Profile at Annex B of the Organisation Certificate Policy; and

(c) "**AccessControlBroker**" and "**wanProvider**", when used in relation to the roles of the DCC, mean those roles which are identified as such, and have the meanings given to them, in the GB Companion Specification.

L4 THE SMKI SERVICE INTERFACE

DCC: Obligation to Maintain the SMKI Service Interface

L4.1 The DCC shall maintain the SMKI Service Interface in accordance with the SMKI Interface Design Specification and make it available, for sending and receiving communications in accordance with the SMKI Code of Connection, via DCC Gateway Connections, to:

(a) Authorised Subscribers; and

(b) (where applicable) Parties for the purpose of undertaking SMKI Entry Process Testing.

L4.2 The DCC shall ensure that the SMKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing.

The SMKI Service Interface

L4.3 For the purposes of this Section L4, the "**SMKI Service Interface**" means a communications interface designed to allow communications to be sent between an Authorised Subscriber and the DCC for the purposes of the SMKI Services.

SMKI Interface Design Specification

L4.4 For the purposes of this Section L4, the "**SMKI Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) shall specify the technical details of the SMKI Service Interface;

(b) shall include the protocols and technical standards that apply to the SMKI Service Interface;

(c) shall base those technical standards on PKIX/IETF/PKCS open standards, where:

(i) PKIX is the Public Key Infrastructure for X.509 Certificates, being an IETF set of standards for certificate and certificate revocation list profiles as specified in IETF RFC 5280;

(ii) the IETF is the Internet Engineering Task Force; and

(iii) PKCS is the Public Key Cryptography Standard;

(d) may set out the procedure by which an Authorised Subscriber and the DCC may communicate over the SMKI Service Interface, and may in particular specify any requirements on:

(i) an Authorised Subscriber which accesses, or is seeking to access, the SMKI Service Interface;

(ii) the DCC in relation to the provision of means of access to the SMKI Service Interface and/or any steps which must be taken by it in relation to communications made by an Authorised Subscriber and received by it over the SMKI Service Interface; and

(e) may specify limits on the use of the SMKI Service Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent.

SMKI Code of Connection

L4.5 For the purposes of this Section L4, the "**SMKI Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a) sets out the way in which an Authorised Subscriber may access the SMKI Service Interface;

(b) may specify limits on the use of the SMKI Service Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent;

(c) specifies the procedure by which an Authorised Subscriber and the DCC may communicate over the SMKI Service Interface; and

(d) includes a description of the way in which the mutual authentication and protection of communications taking place over the SMKI Service Interface will operate.

SMKI Interface Document Development

L4.6 The DCC shall develop drafts of the SMKI Interface Design Specification and SMKI Code of Connection:

(a) in accordance with the process set out at Section L4.7; and

(b) so that the drafts are available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L4.7 The process set out in this Section L4.7 for the development of drafts of the SMKI Interface Design Specification and SMKI Code of Connection is that:

(a) the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that

have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

L5 THE SMKI REPOSITORY SERVICE

The SMKI Repository

L5.1 For the purposes of this Section L5, the "**SMKI Repository**" means a System for storing and (subject to the provisions of this Section) making available copies of the following:

(a) all Device Certificates;

(b) all DCA Certificates;

(c) all Organisation Certificates;

(d) all OCA Certificates;

(e) the IKI Certificates (to the extent required by the SMKI RAPP);

(f) any other IKI Certificates, and any ICA Certificates, which the DCC may from time to time consider appropriate;

(g) all versions of the Device Certificate Policy;

(h) all versions of the Organisation Certificate Policy;

(i) all versions of the IKI Certificate Policy;

(j) all versions of the SMKI RAPP;

(k) all versions of the SMKI Recovery Procedure;

(l) all versions of the SMKI Compliance Policy;

(m) the latest version of the Organisation CRL;

(n) the latest version of the Organisation ARL;

(o) such other documents or information as may be specified by the SMKI PMA from time to time; and

(p) such other documents or information as the DCC, in its capacity as the

provider of the SMKI Services, may from time to time consider appropriate.

The SMKI Repository Service

L5.2 The DCC shall establish, operate, maintain and make available the SMKI Repository in accordance with the provisions of this Section L5 (the "**SMKI Repository Service**").

L5.3 The DCC shall ensure that the documents and information described in Section L5.1 may be lodged in the SMKI Repository:

(a) by itself, for the purpose of providing the SMKI Services or complying with any other requirements placed on it under the Code; and

(b) (except in the case of Certificates, the CRL and the ARL) by the SMKI PMA, or by the Code Administrator acting on its behalf, for the purpose of fulfilling its functions under the Code.

L5.4 The DCC shall ensure that no person may lodge documents or information in the SMKI Repository other than in accordance with Section L5.3.

L5.5 The DCC shall ensure that the SMKI Repository may be accessed for the purpose of viewing and/or obtaining a copy of any document or information stored on it by:

(a) any Party or RDP which reasonably requires such access in accordance, or for any purpose associated, with the Code;

(b) the Panel (or the Code Administrator acting on its behalf); and

(c) the SMKI PMA (or the Code Administrator acting on its behalf).

L5.6 The DCC shall ensure that no person may access documents or information in the SMKI Repository other than in accordance with Section L5.5.

SMKI PMA: Role in relation to the SMKI Repository

L5.7 The SMKI PMA shall lodge each of the following documents in the SMKI Repository promptly upon the SMKI Repository Service first becoming available or (if later) the incorporation of that document into the Code:

(a) the Device Certificate Policy;

(b) the Organisation Certificate Policy;

(c) the IKI Certificate Policy; and

(d) the SMKI Compliance Policy.

L5.8 The SMKI PMA shall lodge in the SMKI Repository the modified version of each document referred to in Section L5.7 promptly upon any modification being made to that document in accordance with the Code.

L5.9 The SMKI PMA may require the DCC to lodge in the SMKI Repository such other documents or information as it may from time to time direct.

L5.10 Subject to Section L5.3, the SMKI PMA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

Parties: Duties in relation to the SMKI Repository

L5.11 Neither any Party nor RDP, or the SMKI PMA, may access the SMKI Repository for the purpose of viewing and/or obtaining a copy of any document or information stored on it except to the extent that it reasonably requires such access in accordance, or for any purpose associated, with the Code.

L6 THE SMKI REPOSITORY INTERFACE

DCC: Obligation to Maintain the SMKI Repository Interface

L6.1 The DCC shall maintain the SMKI Repository Interface in accordance with the SMKI Repository Interface Design Specification and make it available, via DCC Gateway Connections, to:

(a) the Parties and RDPs;

(b) the Panel (or the Code Administrator on its behalf); and

(c) the SMKI PMA (or the Code Administrator on its behalf),

to send and receive communications in accordance with the SMKI Repository Code of Connection and (where applicable) for the purpose of SMKI Entry Process Testing.

L6.2 The DCC shall ensure that the SMKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing.

The SMKI Repository Interface

L6.3 For the purposes of this Section L6, the "**SMKI Repository Interface**" means a communications interface designed to allow communications to be sent from and received by the SMKI Repository for the purposes of the SMKI Repository Service.

SMKI Repository Interface Design Specification

L6.4 For the purposes of this Section L6, the "**SMKI Repository Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the SMKI Repository Interface; and

(b) includes the protocols and technical standards that apply to the SMKI

Repository Interface.

SMKI Repository Code of Connection

L6.5 For the purposes of this Section L6, the "**SMKI Repository Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a) sets out the way in which the Parties, the RDPs, the Panel and the SMKI PMA may access the SMKI Repository Interface;

(b) may specify limits on the use of the SMKI Repository Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent;

(c) specifies the procedure by which the Parties, the RDPs, the Panel and the SMKI PMA may communicate over the SMKI Repository Interface; and

(d) includes a description of the way in which the authentication and protection of communications taking place over the SMKI Repository Interface will operate.

SMKI Repository Interface Document Development

L6.6 The DCC shall develop drafts of the SMKI Repository Interface Design Specification and SMKI Repository Code of Connection:

(a) in accordance with the process set out at Section L6.7; and

(b) so that the drafts are available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L6.7 The process set out in this Section L6.7 for the development of drafts of the SMKI Repository Interface Design Specification and SMKI Repository Code of Connection is that:

(a) the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to

any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

L7 SMKI AND REPOSITORY ENTRY PROCESS TESTS

Eligibility Generally

L7.1 A Party or RDP shall not be entitled to:

(a) apply to become an Authorised Subscriber for the purposes of any Certificate Policy; or

(b) access the SMKI Repository,

until that Party or RDP has successfully completed the SMKI and Repository Entry Process Tests for the purposes of paragraph (a) or (b) above (as applicable).

L7.2 Only persons that are Parties or RDPs are eligible to complete the SMKI and Repository Entry Process Tests.

SMKI and Repository Entry Guide

L7.3 The DCC shall establish and arrange for the publication on the Website of a guide to the SMKI and Repository Entry Process Tests, which shall identify any information that a Party or RDP is required to provide in support of its application to complete the SMKI and Repository Entry Process Tests (whether for the purposes of Section L7.1(a) or (b) or both).

SMKI and Repository Entry Process Tests

L7.4 A Party or RDP that wishes to complete the SMKI and Repository Entry Process Tests (whether for the purposes of Section L7.1(a) or (b) or both) must apply to the DCC in compliance with any requirements identified in the guide referred to in Section L7.3.

L7.5 On receipt of an application from a Party or RDP pursuant to Section L7.4, the DCC shall process that Party's or RDP's application to complete the SMKI and Repository Entry Process Tests in accordance with this Section L7.

SMKI and Repository Entry Process Test Requirements

L7.6 A Party or RDP wishing to:

(a) become an Authorised Subscriber for the purposes of any Certificate Policy must have successfully completed the SMKI and Repository Entry Process Tests for that purpose; or

(b) access the SMKI Repository must have successfully completed the SMKI and Repository Entry Process Tests for that purpose.

L7.7 A Party or RDP will have successfully completed the SMKI and Repository Entry Process Tests for a particular purpose once that Party or RDP has received confirmation from the DCC that it has met the relevant requirements of Section L7.6.

L7.8 Once a Party or RDP has successfully completed the SMKI and Repository Entry Process Tests for a particular purpose, the DCC shall confirm the same to the Panel.

Network Parties and RDPs

L7.9 Each Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall, when acting in its capacity as the Network Party's RDP to undertake the SMKI and Repository Entry Process Tests, comply with the obligations expressed to be placed on RDPs under Section H14 (Testing Services) and the SMKI and Repository Test Scenarios Document.

L7.10 Where more than one Network Party nominates the same Registration Data Provider, each of those Network Parties shall be jointly and severally liable for any failure by that RDP, when acting in its capacity as the Network Parties' RDP to undertake the SMKI and Repository Entry Process Tests, to comply with any of the obligations expressed to be placed on RDPs under Section H14 (Testing Services) and the SMKI and Repository Test Scenarios Document.

L8 SMKI PERFORMANCE STANDARDS AND DEMAND MANAGEMENT

SMKI Services: Target Response Times

L8.1 The DCC shall undertake the following activities within the following time periods (each such time period being, in respect of each such activity, the "**Target Response Time**" for that activity):

(a) in response to a single Certificate Signing Request, sending to an Eligible Subscriber either an Organisation Certificate or Device Certificate within 30 seconds of receipt of the Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface; and

(b) in response to a Batched Certificate Signing Request, sending to an Eligible Subscriber the number of Device Certificates that were requested:

(i) where the receipt of the Batched Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface occurred between the hours of 08:00 and 20:00 on any day, by no later than 08:00 on the following day; or

(ii) where the receipt of the Batched Certificate Signing Request from that Eligible Supplier over the SMKI Service Interface did not occur between the hours of 08:00 and 20:00, within 24 hours of the time of that receipt.

L8.2 For the purposes of Section L8.1, a "**Batched Certificate Signing Request**" is a single communication containing Certificate Signing Requests for the Issue of more than one but no more than 50,000 Device Certificates.

L8.3 For the purposes of Section L8.1, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Interface Design Specification.

SMKI Repository Service: Target Response Time

L8.4 The DCC shall send to a Party, an RDP, the Panel or the SMKI PMA (as the case may be) a copy of any document or information stored on the SMKI Repository within 3

seconds of receipt of a request for that document from that person or body over the SMKI Repository Interface (and that time period shall be the "**Target Response Time**" for that activity).

L8.5 For the purposes of Section L8.4, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Repository Interface Design Specification.

Code Performance Measures

L8.6 Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period):

No.	Code Performance Measure	Performance Measurement Period	Target Service Level	Minimum Service Level
7	Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.	monthly	99%	96%
8	Percentage of documents stored on the SMKI Repository delivered within the applicable Target Response Time for the SMKI Repository Service.	monthly	99%	96%

SMKI Services: Managing Demand

L8.7 Each Party which is an Authorised Subscriber in accordance with the Device Certificate Policy shall:

(a) as soon as reasonably practicable after becoming an Authorised Subscriber; and

(b) subsequently by the 15th Working Day of the months of March, June, September and December in each year,

provide the DCC with a forecast of the number of Certificate Signing Requests that the Authorised Subscriber will send in each of the 8 months following the end of the month in which such forecast is provided. Such forecast shall contain a breakdown of the total number of Certificate Signing Requests in respect of Device Certificates between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests.

L8.8 The DCC shall monitor and record the aggregate number of Certificate Signing Requests sent by each Authorised Subscriber in total.

L8.9 By no later than the 10th Working Day following the end of each month, the DCC shall provide:

(a) each Authorised Subscriber with a report that sets out the number of Certificate Signing Requests sent by that Authorised Subscriber in respect of Device Certificates during that month (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers sent against the numbers most recently forecast for the applicable month; and

(b) (in so far as there were one or more Parties or RDPs which were Authorised Subscribers during the applicable month) a report to the Panel that sets out:

(i) the aggregate number of Certificate Signing Requests in respect of Device Certificates sent by all Authorised Subscribers collectively during that month (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers for that month sent against the numbers most recently forecast for the applicable month; and

(ii) where the number of Certificate Signing Requests in respect of Device Certificates sent by any Authorised Subscriber during that month is greater than or equal to 110% of the Authorised Subscriber's most recent monthly forecast for the applicable month, the identity of each such Authorised Subscriber and the number of Certificate Signing

Requests in respect of Device Certificates sent by each such Authorised Subscriber (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests)

L8.10 The Panel shall publish each report provided to it pursuant to Section L8.9(b) on the Website, save that the Panel may decide not to publish one or more parts of a report concerning under-forecasting as referred to in Section L8.9(b)(ii) where the Panel considers that the under-forecasting was reasonable in the circumstances (including where it arose as a result of matters beyond the Authorised Subscriber's reasonable control).

L8.11 The DCC shall, as soon as is reasonably practicable, submit a Modification Proposal containing rules that it considers appropriate to enable the prioritisation by the DCC of Certificate Signing Requests in respect of Device Certificates sent over the SMKI Service Interface in circumstances in which the aggregate demand for the Issue of Device Certificates cannot be satisfied within the applicable Target Response Times.

L8.12 The DCC shall not be considered to be in breach of this Code with regard to the obligation to achieve the Target Response Times set out at Section L8.1 if, during the month in question, the aggregate Certificate Signing Requests in respect of Device Certificates sent by all Authorised Subscribers exceeds 110% of the aggregate demand most recently forecast for that month by all Authorised Subscribers pursuant to Section L8.7 (provided that the DCC shall nevertheless in such circumstances take reasonable steps~~use its reasonable endeavours~~ to achieve the Target Response Times).

L9 THE SMKI DOCUMENT SET

Obligations on the SMKI PMA

L9.1 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the SMKI Document Set.

Obligations on SMKI Participants

L9.2 Each SMKI Participant shall (in so far as they apply to it) comply with the requirements of the SMKI SEC Documents.

The SMKI Document Set

L9.3 For the purposes of this Section L, the "**SMKI Document Set**" means:

(a) the SMKI SEC Documents;

(b) the Device CPS;

(c) the Organisation CPS; and

(d) the IKI CPS.

The SMKI SEC Documents

L9.4 For the purposes of this Section L, the "**SMKI SEC Documents**" means the provisions of the Code comprising:

(a) the following SEC Subsidiary Documents:

(i) the Device Certificate Policy;

(ii) the Organisation Certificate Policy;

(iii) the IKI Certificate Policy;

(iv) the SMKI Compliance Policy;

(v) the SMKI RAPP;

(vi) the SMKI Recovery Procedure;

(vii) the SMKI Interface Design Specification;

(viii) the SMKI Code of Connection;

(ix) the SMKI Repository Interface Design Specification;

(x) the SMKI Repository Code of Connection;

(xi) the SMKI and Repository Test Scenarios Document;

(b) the provisions of Sections L1 to L12; and

(c) every other provision of the Code which relates to the provision or the use of the SMKI Services or the SMKI Repository Service or to any matters directly arising from or affecting the provision or the use of those Services.

The Registration Authority Policies and Procedures: Document Development

L9.5 The DCC shall develop a draft of the SMKI RAPP:

(a) to make provision for such matters as are specified in the Certificate Policies as being matters provided for in the SMKI RAPP;

(b) to make provision for such other matters as are necessary or appropriate in relation to the exercise of its functions as the Registration Authority;

(c) to make provision for such matters as are necessary or appropriate in relation to Test Certificates that are being made available to Testing Participants;

(d) to make such provision as the DCC may consider appropriate in relation to the means by which the identity and authorisation of individuals and Parties may be verified for the purposes of the DCCKI Services (in addition to any such provision made in respect of the SMKI Services);

(e) in accordance with the process set out at Section L9.6; and

(f) so that the draft is available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L9.6 The process set out in this Section L9.6 for the development of a draft of the SMKI RAPP is that:

(a) the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of the SMKI RAPP;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the SMKI RAPP, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the SMKI RAPP specified in Section L9.5;

(c) the DCC shall send a draft of the SMKI RAPP to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the SMKI RAPP, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The Device Certification Practice Statement

L9.7 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**Device CPS**".

L9.8 The Device CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the Device Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.9 For the purposes of the approval of the Device CPS by the SMKI PMA in accordance with Section L9.8(d):

(a) the DCC shall submit an initial draft of the Device CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b) the SKMI PMA shall review the initial draft of the Device CPS and shall:

(i) approve the draft, which shall become the Device CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Device CPS that may be directed by the SMKI PMA, and the amended draft shall become the Device CPS.

L9.10 The DCC shall keep the Device CPS under review, and shall in particular carry out a review of the Device CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.11 Following any review of the Device CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.12 Both the DCC and the SMKI PMA shall treat the Device CPS as confidential.

The Organisation Certification Practice Statement

L9.13 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**Organisation CPS**".

L9.14 The Organisation CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the Organisation Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.15 For the purposes of the approval of the Organisation CPS by the SMKI PMA in accordance with Section L9.14(d):

(a) the DCC shall submit an initial draft of the Organisation CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b) the SKMI PMA shall review the initial draft of the Organisation CPS and shall:

(i) approve the draft, which shall become the Organisation CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Organisation CPS that may be directed by the SMKI PMA, and the amended draft shall become the Organisation CPS.

L9.16 The DCC shall keep the Organisation CPS under review, and shall in particular carry out a review of the Organisation CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.17 Following any review of the Organisation CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.18 Both the DCC and the SMKI PMA shall treat the Organisation CPS as confidential.

The IKI Certification Practice Statement

L9.19 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**IKI CPS**".

L9.20 The IKI CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the IKI Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.21 For the purposes of the approval of the IKI CPS by the SMKI PMA in accordance with Section L9.20(d):

(a) the DCC shall submit an initial draft of the IKI CPS to the SMKI PMA by no later than the date which falls one month prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b) the SKMI PMA shall review the initial draft of the IKI CPS and shall:

(i) approve the draft, which shall become the IKI CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft IKI CPS that may be directed by the SMKI PMA, and the amended draft shall become the IKI CPS.

L9.22 The DCC shall keep the IKI CPS under review, and shall in particular carry out a review of the IKI CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.23 Following any review of the IKI CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.24 Both the DCC and the SMKI PMA shall treat the IKI CPS as confidential.

Enquiries in relation to the SMKI Document Set

L9.25 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party or RDP in relation to the SMKI Services, the SMKI Repository Services or the SMKI Document Set, but excluding any request for a copy of any document or information which can be accessed through the SMKI Repository.

L10 THE SMKI RECOVERY PROCEDURE

The SMKI Recovery Procedure

L10.1 For the purposes of this Section L10, the "**SMKI Recovery Procedure**" shall be a SEC Subsidiary Document of that name which sets out, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised:

(a) the mechanism by which Parties and RDPs may notify the DCC and the DCC may notify Parties, RDPs and the SMKI PMA that the Relevant Private Key has been (or is suspected of having been) Compromised;

(b) procedures relating to the use of the Recovery Private Key and Contingency Private Key (including the use of the Symmetric Key) where such use has been required in accordance with a decision of the SMKI PMA;

(c) procedures relating to:

(i) the distribution of new Root OCA Certificates and Organisation Certificates to Devices; and

(ii) the coordination of the submission of Certificate Signing Requests by Eligible Subscribers following the replacement of any OCA Certificate;

(d) steps to be taken by the DCC, the Parties (or any of them, whether individually or by Party Category), RDPs, the SMKI PMA(or any SMKI PMA Members) and the Panel (or any Panel Members), including in particular in respect of:

(i) notification of the Compromise (or suspected Compromise); and

(ii) the process for taking steps to avoid or mitigate the adverse effects of, or to recover from, the (actual or suspected) Compromise, which steps may differ depending on the Relevant Private Key that has been (or is suspected of having been) Compromised and the nature and extent of the (actual or suspected) Compromise and the adverse effects arising from it; and

(e) arrangements to be made preparatory to and for the purpose of ensuring the

effective operation of the matters described in paragraphs (a) to (d), and the associated technical solutions employed by the DCC, including for their periodic testing.

L10.2 The SMKI Recovery Procedure:

(a) shall make provision for the use of the Recovery Private Key and Contingency Private Key (including the use of the Symmetric Key) only where such use has been required in accordance with a decision of the SMKI PMA;

(b) shall make provision for the DCC, if it has reason to believe that the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key) is likely to be required by the SMKI PMA, to take or instruct any Party, any SMKI PMA Member or any Panel Member to take such preparatory steps in respect of that use as it considers appropriate; and

(c) may make provision:

(i) that, in specified circumstances, certain requirements of the SMKI Recovery Procedure, or of decisions made under and in accordance with the provisions of the SMKI Recovery Procedure, may take precedence over the other provisions of the Code;

(ii) for the operation of procedures which, in specified circumstances, require that decisions over whether or not to take certain steps are referred to the SMKI PMA for its determination;

(iii) for the SMKI PMA to require any Party to nominate individuals for the purpose of performing specified tasks.

L10.3 Where the DCC follows any of the procedures specified in the SMKI Recovery Procedure, it shall, as soon as is reasonably practicable, notify the SMKI PMA of the steps that it has taken and provide such additional supporting information as the SMKI PMA reasonably requests.

SMKI Recovery Procedure: Obligations

L10.4 The DCC, each Party, the SMKI PMA (and SMKI PMA Members) and the Panel

(and Panel Members) shall comply, in so far as applicable to it (or them), with any requirements set out in the SMKI Recovery Procedure.

L10.5 Any SMKI PMA Member or Panel Member who is appointed by (respectively) the SMKI PMA or Panel to carry out a specific role in respect of the SMKI Recovery Procedure must take reasonable steps~~use reasonable endeavours~~ to act in accordance with any instructions given to him by the SMKI PMA or Panel (as the case may be) in relation to the way in which that role is to be carried out.

L10.6 The DCC shall reimburse the reasonable costs of any Party which that Party can demonstrate were incurred by it solely and directly in consequence of actions taken by it to support the maintenance of the procedures and arrangements set out in the SMKI Recovery Procedure, and which it would not otherwise have incurred.

SMKI Recovery Procedure: Document Development

L10.7 The DCC shall develop a draft of the SMKI Recovery Procedure:

(a) in accordance with the process set out at Section L10.8; and

(b) so that the draft is available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L10.8 The process set out in this Section L10.8 for the development of a draft of the SMKI Recovery Procedure is that:

(a) the DCC shall, in consultation with the Parties, the SMKI PMA and such other persons as it considers appropriate, produce a draft of the SMKI Recovery Procedure;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the SMKI Recovery Procedure, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the SMKI Recovery Procedure specified in Section L10.1;

(c) the DCC shall send a draft of the SMKI Recovery Procedure to the Secretary of State as soon as is practicable after it is produced, and shall when doing so

provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the SMKI Recovery Procedure, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The SMKI Recovery Key Guidance

L10.9 For the purposes of this Section L10, the "**SMKI Recovery Key Guidance**" shall be a document of that name which makes such provision as is appropriate, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, for any one or more of the following:

(a) any factors which shall be taken into account by the SMKI PMA in deciding whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key);

(b) any other factors which may in particular be taken into account by the SMKI PMA for the purposes of that decision;

(c) any weighting or order of priority which shall, or may, be given by the SMKI PMA to any of the factors referred to in paragraphs (a) and (b); and

(d) any criteria that are to be applied by the SMKI PMA, any approach that is to be followed by it, or any steps that are to be taken by it, prior to making a

decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key).

Recovery Key Guidance: Obligations

L10.10 The SMKI PMA:

(a) shall act in accordance with the SMKI Recovery Key Guidance in making any decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key); and

(b) may request such information and assistance from the DCC, the Security Sub-Committee or any Party as it reasonably considers appropriate for the purposes of making any such decision or ensuring that it will be prepared to make any such decision that may fall to be made by it at a future date.

L10.11 The DCC, each other Party, and the Security Sub-Committee shall promptly provide the SMKI PMA with such information and assistance as may be requested in accordance with Section L10.10.

L10.12 The DCC shall, where requested to do so, reimburse the reasonable costs of any Party associated with the provision of assistance in accordance with Section L10.11.

Recovery Key Guidance: Document Development

L10.13 The SMKI PMA shall:

(a) develop the SMKI Recovery Key Guidance, and for that purpose:

(i) consult with the DCC, the Security Sub-Committee, the Parties, the Secretary of State and the Authority; and

(ii) have regard to the views of each person consulted by it prior to determining the content of the document;

(b) periodically review the SMKI Recovery Key Guidance, and in particular carry out a review whenever (and to the extent to which) it may be required to do so by the Panel or the Authority;

(c) where, following any review, it proposes to amend the SMKI Recovery Key Guidance:

(i) consult the DCC, the Security Sub-Committee, the Parties and the Authority in relation to the proposed amendments; and

(ii) have regard to the views of each person consulted by it prior to making any amendments to the document; and

(d) publish the SMKI Recovery Key Guidance, as initially determined by it and on each amendment made to that document from time to time.

Recovery Events and Recovery Costs

Recovery Events

L10.14 For the purposes of this Section L10, a "**Recovery Event**" is an event that shall be taken to have occurred when the circumstances described in either Section L10.15 or L10.16 exist.

L10.15 The circumstances described in this Section L10.15 are that:

(a) the DCC has notified the SMKI PMA that a Relevant Private Key has been (or is suspected of having been) Compromised; and

(b) in consequence of that (actual or suspected) Compromise, the SMKI PMA has decided to require the use of the Recovery Private Key or Contingency Private Key (including the use of the Symmetric Key) in accordance with the SMKI Recovery Procedure.

L10.16 The circumstances described in this Section L10.16 are that:

(a) the DCC has notified the SMKI PMA that a Relevant Private Key has been (or is suspected of having been) Compromised;

(b) the SMKI PMA has been provided with (or otherwise obtained) evidence that:

(i) attempts have been made, by means of sending appropriate Commands, to replace the Data comprising part of the Device Security Credentials

of Relevant Devices which derive from any Organisation Certificate or OCA Certificate which is (or is suspected of being) Compromised; or

(ii) it was not feasible or appropriate for any such attempt to be made; and

(c) the SMKI PMA has decided not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key).

Recovery Costs

L10.17 For the purposes of this Section L10, the "**Recovery Costs**" shall be such costs as are reasonably incurred in consequence of a Recovery Event (and which would not otherwise have incurred) by any Party:

(a) in respect of the use of the Recovery Private Key or Contingency Private Key (including the use of the Symmetric Key) in accordance with the requirement of the SMKI PMA; and

(b) in taking such action as is necessary, where the Recovery Private Key or Contingency Private Key (including the Symmetric Key) has not been used or has been used unsuccessfully, to replace:

(i) Relevant Devices for which that Party is the Responsible Supplier; or

(ii) the Data comprising part of the Device Security Credentials of such Relevant Devices which derive from any Organisation Certificate or OCA Certificate which is (or is suspected of being) Compromised.

Payment of Recovery Costs by the DCC

L10.18 Where any Party incurs Recovery Costs, it may submit to the DCC a request to be recompensed in respect of those costs.

L10.19 Where any Party wishes to submit a request in accordance with Section L10.18, it shall:

(a) within three months of the Recovery Event, notify the DCC of its intention to do so;

(b) unless, at the same time as notifying the DCC of that intention it also notifies the DCC of the total amount of the costs in respect of which it requests to be recompensed:

(i) provide to the DCC at that time its best estimate of the likely amount of those costs; and

(ii) at least once in every subsequent period of three months, until such time as it notifies the DCC of the total amount of the costs in respect of which it requests to be recompensed, provide to the DCC an updated best estimate of the likely amount of those costs; and

(c) as soon as possible, and in any event within three months of the date on which it ceases to incur Recovery Costs, notify the DCC of the total amount of the costs in respect of which it requests to be recompensed.

L10.20 A Party giving notice to the DCC in accordance with Section L10.19 shall:

(a) subject to paragraph (b), provide to the DCC such evidence in respect of the amount of the Recovery Costs incurred by that Party:

(i) as the DCC may reasonably require;

(ii) by such dates as the DCC may reasonably specify; or

(b) where the Panel considers the matter either of its own motion or on a referral by the Party or the DCC, provide to the DCC such evidence relating to the amount of the costs incurred by that Party:

(i) as the Panel may determine is reasonably required;

(ii) by such dates as the Panel may reasonably specify.

L10.21 The evidence referred to in Section L10.20 may include in particular, if the DCC or the Panel (as the case may be) determines that it is reasonably required, the report of an independent auditor verifying that the amount requested by a Party represents a fair and accurate statement of the Recovery Costs incurred by that Party.

L10.22 On receipt by it of a request from a Party to be recompensed in respect of Recovery

Costs, the DCC shall, where it is satisfied that the amount of the costs requested by that Party is adequately supported by the evidence provided to it in accordance with Section L10.20, pay to the Party that amount.

L10.23 Where the DCC has any question whether the evidence provided to it by a Party is adequate to support the amount of the costs requested:

(a) it shall refer that question to the Panel for its determination; and

(b) the Panel shall determine that question by directing that the DCC shall pay to the Party the full amount requested or only part of that amount (in a sum that is specified by the Panel), or shall make no payment to that Party.

L10.24 Where the amount of the Recovery Costs requested by any Party is (whether alone or taken together with amounts requested by any other Parties in relation to the same Recovery Event) for a sum exceeding that which is determined from time to time by the Panel, following consultation with the Parties and the Authority, for the purposes of this Section L10.24:

(a) the DCC may refer to the Panel, for its determination, the question of the dates on which the payments of the amounts requested shall be made;

(b) the Panel shall determine the dates on which those payments shall be made, and may in particular determine that:

(i) different Parties shall be paid at different times; and

(ii) any amount which is to be paid to a Party shall be paid in instalments at different times; and

(c) the Panel shall consider whether to make any Modification Proposal in relation to the Charging Methodology (taking into account whether it is proposed by the Authority to make any adjustment to the allowable revenues of the DCC, or by the DCC to amend the Charging Statement).

Breach of the Code by the Relevant Subscriber

L10.25 Where a Recovery Event occurs, and where the Relevant Subscriber is the DCC, the

DCC shall be deemed to be in breach of:

(a) where the (actual or suspected) Compromise is to an Organisation Certificate, Section L11.9 (Organisation and IKI Certificates: Protection of Private Keys); or

(b) where the (actual or suspected) Compromise is to an OCA Certificate, Part 6.2.1 of the Organisation Certificate Policy (Cryptographic Module Standards and Controls).

L10.26 Where a Recovery Event occurs, and where the Relevant Subscriber is any Party other than the DCC, that Party shall be deemed to be in breach of Section L11.9 (Organisation and IKI Certificates: Protection of Private Keys), unless the (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event was due to the (actual or suspected) Compromise of an OCA Certificate.

L10.27 Where a Relevant Subscriber is, by virtue of Section L10.25 or L10.26, deemed to be in breach of a provision of this Code, it shall cease to be so deemed (and no such breach shall be treated as having occurred) where:

(a) within three months of the date of the Recovery Event it refers the matter to the Panel;

(b) following that referral it demonstrates to the reasonable satisfaction of the Panel, that the (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event was not due to its breach of Section L11.9 or of Part 6.2.1 of the Organisation Certificate Policy (as the case may be); and

(c) the Panel determines accordingly that no such breach occurred.

L10.28 In all circumstances other than those described in Section L10.27, and subject to the provisions of Section L10.29, where a breach is deemed to have occurred in accordance with Section L10.25 or L10.26, that shall be treated as a final and binding determination of its occurrence for the purposes of this Code.

Appeal to the Authority

L10.29 Any decision made by the Panel in accordance with Section L10.20, L10.23, L10.24 or L10.27 may be appealed to the Authority, whose decision shall be final and binding for the purposes of this Code.

Definitions

L10.30 For the purposes of this Section L10:

(a) a "**Relevant Device**" means a Device:

(i) which has, or had immediately prior to a Recovery Event, an SMI Status of 'commissioned'; and

(ii) the Device Security Credentials of which are populated with, or are reasonably believed immediately prior to a Recovery Event to have been populated with, Data from an Organisation Certificate or OCA Certificate which has been (or is suspected of having been) Compromised as a result of an (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event;

(b) the "**Relevant Subscriber**" means, where a Recovery Event has occurred, the Subscriber for an Organisation Certificate or OCA Certificate which has been (or is suspected of having been) Compromised as the result of an (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event;

(c) a "**Relevant Private Key**" means a Private Key which is used to encrypt the Contingency Key Pair, or a Private Key which is associated with a Public Key contained in:

(i) any Organisation Certificate or OCA Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System; or

(ii) any OCA Certificate that was used as part of the process of Issuing any such Organisation Certificate or OCA Certificate;

(d) a "**Recovery Key Pair**" means a Key Pair established by the DCC for the

purposes of the replacement of Organisation Certificates on Devices after a Relevant Private Key has been Compromised, and:

(i) a "**Recovery Private Key**" means the Private Key which is part of that Key Pair; and

(ii) a "**Recovery Certificate**" means an Organisation Certificate Issued by the OCA and containing the Public Key which is part of that Key Pair; and

(e) a "**Contingency Key Pair**" means a Key Pair established by the DCC for the purposes of the replacement of Root OCA Certificates on Devices after a Relevant Private Key has been Compromised, and comprising:

(i) a "**Contingency Private Key**", being the Private Key which is part of that Key Pair; and

(ii) a "**Contingency Public Key**", being the Public Key which is part of that Key Pair and which is stored in the WrappedApexContingencyKey field of the Root OCA Certificate (being the field identified as such in the Root OCA Certificate Profile at Annex B of the Organisation Certificate Policy).

L11 THE SUBSCRIBER OBLIGATIONS

Certificate Signing Requests

L11.1 Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate.

L11.2 No Eligible Subscriber may make a Certificate Signing Request which contains:

(a) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(b) any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

L11.3 Each Eligible Subscriber shall ensure that any Public Key which is included within a Certificate Signing Request either:

(a) (where appropriate, in the case of a Certificate Signing Request for the Issue of an IKI Certificate) has been generated by software which forms part of a Cryptographic Credential Token that was provided by the DCC to the Eligible Subscriber in accordance with the provisions of this Code; or

~~(c)~~(b) (in the case of any other Certificate Signing Request) is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated.

~~L11.3~~L11.4 No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

(a) a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate;

(b) an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of

the Root OCA Certificate to the extent to which it is expressly permitted in accordance with the Organisation Certificate Policy); or

(c) an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate.

Subscribing for or Rejecting Organisation Certificates

~~L11.4~~L11.5 Where any Organisation Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i) reject that Certificate; and

(ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c) where it does not reject the Certificate, become a Subscriber for that Certificate.

Subscribing for or Rejecting Device Certificates

~~L11.5~~L11.6 Where any Device Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) ~~use its reasonable endeavours~~take reasonable steps to establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i) reject that Certificate; and

(ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c) where it does not reject the Certificate, become a Subscriber for that Certificate.

Subscribing for or Rejecting IKI Certificates

~~L11.6~~L11.7 Where any IKI Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b) if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i) reject that Certificate;

(ii) immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c) where it does not reject the Certificate, become a Subscriber for that Certificate.

Use of Certificates and Key Pairs

~~L11.7~~L11.8 Each Subscriber shall ensure that it does not use any Certificate, Public Key contained within a Certificate, or Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from Devices and the DCC pursuant to the Code.

Organisation and IKI Certificates: Protection of Private Keys

~~L11.8~~L11.9 Each Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) ~~use its reasonable endeavours~~take reasonable steps to ensure that no Compromise occurs to any:

(a) Private Key which is associated with a Public Key contained in an Organisation Certificate or IKI Certificate for which it is the Subscriber; or

(b) Secret Key Material associated with that Private Key.

Organisation Certificates: Expiry of Validity Period

~~L11.9~~L11.10 Each Subscriber shall, prior to the expiry of the Validity Period of an Organisation Certificate or OCA Certificate for which it is the Subscriber:

(a) request a replacement for that Certificate by applying for the Issue of a new Organisation Certificate or OCA Certificate in accordance with the provisions of the Organisation Certificate Policy; and

(b) ensure that any Data from that Certificate which are used to populate the Device Security Credentials of any Device are replaced by Data from the new Certificate Issued to it by the OCA.

L12 RELYING PARTY OBLIGATIONS

Relying Parties

L12.1 For the purposes of this Section L12, a 'Relying Party' in relation to an Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate means any Party or RDP which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from a Device or another Party or RDP pursuant to this Code.

L12.2 For the purposes of Section L12.1, a Relying Party shall be deemed to include:

(a) in the case of a Device which relies on a Certificate, the Responsible Supplier for that Device; and

(b) in the case of a Communications Hub Function or Gas Proxy Function which relies on a Certificate, the DCC.

Duties in relation to Organisation Certificates, OCA Certificates IKI Certificates and ICA Certificates

L12.3 Each Relying Party shall:

(a) before relying on any Organisation Certificate:

(i) check the version of the Organisation CRL on the SMKI Repository, in accordance with the GB Companion Specification; and

(ii) where that Certificate is shown on the Organisation CRL as having been revoked, not rely on the Certificate;

(b) before relying on any OCA Certificate:

(i) check the version of the Organisation ARL on the SMKI Repository, in accordance with the GB Companion Specification; and

(ii) where that Certificate is shown on the Organisation ARL as having been revoked, not rely on the Certificate;

(c) before relying on any IKI Certificate:

(i) check the version of the IKI CRL on the SMKI Repository, in accordance with the GB Companion Specification; and

(ii) where that Certificate is shown on the IKI CRL as having been revoked, not rely on the Certificate; and

(d) before relying on any ICA Certificate:

(i) check the version of the IKI ARL on the SMKI Repository, in accordance with the GB Companion Specification; and

(ii) where that Certificate is shown on the IKI ARL as having been revoked, not rely on the Certificate.

L12.4 No Relying Party may rely on an Organisation Certificate or IKI Certificate where the Validity Period of that Certificate has expired.

L12.5 No Relying Party may rely on an Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate where it suspects that the Certificate has been Compromised.

L12.6 Each Relying Party shall take reasonable steps~~use its reasonable endeavours~~, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate.

L13 DCC KEY INFRASTRUCTURE

The DCCKI Services

The DCCKI Services

L13.1 For the purposes of this Section L13, the "**DCCKI Services**" means all of the activities undertaken by the DCC in its capacity as the DCCKI Certification Authority in accordance with the applicable requirements of the Code.

DCCKI Authorised Subscribers

L13.2 Any Party or RDP may apply to become a DCCKI Authorised Subscriber in accordance with, and by following the relevant procedures set out in, the DCCKI Certificate Policy and the DCCKI RAPP.

L13.3 The DCC shall authorise any Party or RDP to submit a DCCKI Certificate Signing Request, and so to become a DCCKI Authorised Subscriber, where that Party or RDP has successfully completed the relevant procedures and satisfied the criteria set out in the DCCKI Certificate Policy and the DCCKI RAPP.

L13.4 The DCC shall provide any DCCKI Services that may be requested by a DCCKI Authorised Subscriber where the request is made by that DCCKI Authorised Subscriber in accordance with the applicable requirements of the DCCKI SEC Documents.

L13.5 The DCC shall ensure that in the provision of DCCKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

L13.6 Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become a DCCKI Authorised Subscriber, the Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L13.

L13.7 Where a Registration Data Provider has been nominated as such by more than one

Network Party:

(a) to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L13.6 in respect of the actions of the RDP;

(b) to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L13.6 in respect of the actions of the RDP.

DCCKI Eligible Subscribers

L13.8 A DCCKI Authorised Subscriber:

(a) shall be known as a "**DCCKI Eligible Subscriber**" in respect of a DCCKI Certificate if it is entitled to become a DCCKI Subscriber for that DCCKI Certificate; and

(b) will be entitled to become a DCCKI Subscriber for a DCCKI Certificate only if it is identified as a DCCKI Eligible Subscriber in respect of that DCCKI Certificate in accordance with the provisions of the DCCKI Certificate Policy and the DCCKI RAPP.

DCCKI Subscribers

L13.9 A Party or RDP shall be entitled to become a DCCKI Subscriber in accordance with, and by following the relevant procedures set out in, the DCCKI Certificate Policy and the DCCKI RAPP.

The DCCKI Service Interface

DCC: Obligation to Maintain the DCCKI Service Interface

L13.10 The DCC shall maintain the DCCKI Service Interface in accordance with the DCCKI Interface Design Specification and make it available, to DCCKI Authorised Subscribers, for sending and receiving communications in accordance with the DCCKI Code of Connection.

L13.11 The DCC shall ensure that the DCCKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing.

The DCCKI Service Interface

L13.12 For the purposes of this Section L13, the "**DCCKI Service Interface**" means a communications interface designed to allow communications to be sent between a DCCKI Authorised Subscriber and the DCC for the purposes of the DCCKI Services.

DCCKI Interface Design Specification

L13.13 For the purposes of this Section L13, the "**DCCKI Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the DCCKI Service Interface;

(b) includes the protocols and technical standards that apply to the DCCKI Service Interface; and

(c) bases those technical standards on PKIX/IETF/PKCS open standards, where:

(i) PKIX is the Public Key Infrastructure for X.509 Certificates, being an IETF set of standards for certificate and certificate revocation list profiles as specified in IETF RFC 5280;

(ii) the IETF is the Internet Engineering Task Force; and

(iii) PKCS is the Public Key Cryptography Standard.

DCCKI Code of Connection

L13.14 For the purposes of this Section L13, the "**DCCKI Code of Connection**" shall be a

SEC Subsidiary Document of that name which:

(a) sets out the way in which DCCKI Authorised Subscribers may access the DCCKI Service Interface;

(b) specifies the procedure by which DCCKI Authorised Subscribers and the DCC may communicate over the DCCKI Service Interface; and

(c) includes a description of the way in which the mutual authentication and protection of communications taking place over the DCCKI Service Interface will operate.

DCCKI Interface Document Development

L13.15 The DCC shall develop drafts of the DCCKI Interface Design Specification and DCCKI Code of Connection:

(a) in accordance with the process set out at Section L13.16; and

(b) so that the drafts are available by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.16 The process set out in this Section L13.16 for the development of drafts of the DCCKI Interface Design Specification and DCCKI Code of Connection is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document

to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Repository Service

The DCCKI Repository

L13.17 For the purposes of this Section L13, the "**DCCKI Repository**" means a System for storing and (subject to the provisions of this Section) making available copies of the following:

(a) all DCCKI Infrastructure Certificates;

(b) the Root DCCKICA Certificate and the EII DCCKICA Certificate;

(c) all versions of the DCCKI Certificate Policy;

(d) the latest version of the DCCKI RAPP;

(e) the latest version of the EII DCCKICA CRL;

(f) the latest version of the DCCKI ARL; and

(g) such other documents or information as the DCC, in its capacity as the provider of the DCCKI Services, may from time to time consider appropriate.

The DCCKI Repository Service

L13.18 The DCC shall establish, operate, maintain and make available the DCCKI Repository in accordance with the provisions of this Section L13 (the "**DCCKI Repository Service**").

L13.19 The DCC shall ensure that the documents and information described in Section L13.17 may be lodged in the DCCKI Repository by itself for the purpose of providing the DCCKI Services or complying with any other requirements placed on it under the Code.

L13.20 The DCC shall ensure that no person may lodge documents or information in the DCCKI Repository other than in accordance with Section L13.19.

L13.21 The DCC shall ensure that the DCCKI Repository may be accessed for the purpose of viewing and/or obtaining a copy of any document or information stored on it by any Party or RDP which reasonably requires such access in accordance, or for any purpose associated, with the Code.

L13.22 The DCC shall make available a copy of any document stored on the DCCKI Repository to the Panel or the SMKI PMA (or the Code Administrator acting on their behalf) following receipt of a reasonable request to do so.

Parties: Duties in relation to the DCCKI Repository

L13.23 No Party or RDP may access the DCCKI Repository for the purpose of viewing and/or obtaining a copy of any document or information stored on it except to the extent that it reasonably requires such access in accordance, or for any purpose associated, with the Code.

The DCCKI Repository Interface

DCC: Obligation to Maintain the DCCKI Repository Interface

L13.24 The DCC shall maintain the DCCKI Repository Interface in accordance with the DCCKI Repository Interface Design Specification and make it available to the Parties and to RDPs to send and receive communications in accordance with the DCCKI Repository Code of Connection and (where applicable) for the purpose of Entry Process Testing.

L13.25 The DCC shall ensure that the DCCKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing.

The DCCKI Repository Interface

L13.26 For the purposes of this Section L13, the "**DCCKI Repository Interface**" means a communications interface designed to allow communications to be sent from and received by the DCCKI Repository for the purposes of the DCCKI Repository Service.

DCCKI Repository Interface Design Specification

L13.27 For the purposes of this Section L13, the "**DCCKI Repository Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the DCCKI Repository Interface; and

(b) includes the protocols and technical standards that apply to the DCCKI Repository Interface.

DCCKI Repository Code of Connection

L13.28 For the purposes of this Section L13, the "**DCCKI Repository Code of Connection**" shall be a SEC Subsidiary Document of that name which sets out the way in which the Parties and RDPs may access the DCCKI Repository Interface.

DCCKI Repository Interface Document Development

L13.29 The DCC shall develop drafts of the DCCKI Repository Interface Design Specification and DCCKI Repository Code of Connection:

(a) in accordance with the process set out at Section L13.30; and

(b) so that the drafts are available by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.30 The process set out in this Section L13.30 for the development of drafts of the DCCKI Repository Interface Design Specification and DCCKI Repository Code of Connection is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Document Set

Obligations on the SMKI PMA

L13.31 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the DCCKI Document Set.

Obligations on DCCKI Participants

L13.32 Each DCCKI Participant shall (in so far as they apply to it) comply with the requirements of the DCCKI SEC Documents.

The DCCKI Document Set

L13.33 For the purposes of this Section L13, the "**DCCKI Document Set**" means:

(a) the DCCKI SEC Documents; and

(b) the DCCKI CPS.

The DCCKI SEC Documents

L13.34 For the purposes of this Section L13, the "**DCCKI SEC Documents**" means the provisions of the Code comprising:

(a) the following SEC Subsidiary Documents:

(i) the DCCKI Certificate Policy;

(ii) the DCCKI RAPP;

(iii) the DCCKI Interface Design Specification;

(iv) the DCCKI Code of Connection;

(v) the DCCKI Repository Interface Design Specification;

(vi) the DCCKI Repository Code of Connection;

(b) the provisions of this Section L13; and

(c) every other provision of the Code which relates to the provision or the use of the DCCKI Services or the DCCKI Repository Service or to any matters

directly arising from or affecting the provision or the use of those Services.

The DCCKI Registration Authority Policies and Procedures: Document Development

L13.35 The DCC shall develop a draft of the DCCKI RAPP:

(a) to make provision for such matters as are specified in the DCCKI Certificate Policy as being matters provided for in the DCCKI RAPP;

(b) to make provision for such other matters as are necessary or appropriate in relation to the exercise of its functions as the DCCKI Registration Authority;

(c) in accordance with the process set out at Section L13.36; and

(d) so that the draft is available by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.36 The process set out in this Section L13.36 for the development of a draft of the DCCKI RAPP is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of the DCCKI RAPP;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the DCCKI RAPP, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the DCCKI RAPP specified in Section L13.35;

(c) the DCC shall send a draft of the DCCKI RAPP to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the DCCKI RAPP, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Certification Practice Statement

L13.37 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**DCCKI CPS**".

L13.38 The DCCKI CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the DCCKI Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code;

(d) is reviewed by the SMKI PMA to assess whether it is appropriate for these purposes; and

(e) is approved by the individual(s) carrying out the DCCKI PMA Functions as being appropriate for these purposes.

L13.39 For the purposes of the review of the DCCKI CPS by the SMKI PMA in accordance with Section L13.38(d), the DCC shall submit an initial draft of the DCCKI CPS to the SMKI PMA by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be agreed by the SMKI PMA.

L13.40 The DCC shall keep the DCCKI CPS under review, and shall in particular carry out a review of the DCCKI CPS:

(a) whenever (and to the extent to which) it may be required to so by the SMKI PMA or the individual(s) carrying out the DCCKI PMA Functions; and

(b) following receipt of a notification from the SMKI PMA in accordance with Section L1.17(e) (Duties of the SMKI PMA).

L13.41 Following:

(a) any review of the DCCKI CPS, the DCC may propose amendments to it, which it shall submit to:

(i) the SMKI PMA for its review; and

(ii) the individual(s) carrying out the DCCKI PMA Functions for his (or their) approval;

(b) a review carried out in accordance with Section L13.40(b), the DCC shall report to the SMKI PMA any remedial steps taken or proposed to be taken in order for it to continue to meet its obligations under Section G (Security).

Enquiries in relation to the DCCKI Document Set

L13.42 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party or RDP in relation to the DCCKI Services, the DCCKI Repository Service or the DCCKI Document Set, but excluding any request for a copy of any document or information which can be accessed through the DCCKI Repository.

The DCCKI Subscriber Obligations

DCCKI Certificate Signing Requests

L13.43 Each DCCKI Eligible Subscriber shall ensure that all of the information contained in each DCCKI Certificate Signing Request made by it is true and accurate.

L13.44 No DCCKI Eligible Subscriber may make a DCCKI Certificate Signing Request

which contains:

(a) any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(b) any confidential information which would be contained in a DCCKI Certificate Issued in response to that DCCKI Certificate Signing Request.

Subscribing for or Rejecting DCCKI Certificates

L13.45 Where any DCCKI Certificate is Issued to a DCCKI Eligible Subscriber in response to a DCCKI Certificate Signing Request, that DCCKI Eligible Subscriber shall:

(a) establish whether the information contained in that DCCKI Certificate is consistent with information that was contained in the DCCKI Certificate Signing Request;

(b) if it identifies that the DCCKI Certificate contains any information which is untrue or inaccurate immediately inform the DCC that it rejects the DCCKI Certificate and give to the DCC its reasons for doing so;

(c) in the absence of any such rejection, become a DCCKI Subscriber for that DCCKI Certificate.

Use of DCCKI Certificates

L13.46 Each DCCKI Subscriber shall ensure that it does not use any DCCKI Certificate held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from the DCC pursuant to the Code.

DCCKI Certificates: Protection of Private Keys

L13.47 Each DCCKI Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) take reasonable steps ~~use its reasonable endeavours~~ to ensure that no Compromise occurs to any:

(a) Private Key which is associated with a Public Key contained in a DCCKI Certificate for which it is the DCCKI Subscriber; or

(b) Secret Key Material associated with that Private Key.

The DCCKI Relying Party Obligations

DCCKI Relying Parties

L13.48 For the purposes of this Section L13, a "DCCKI Relying Party" in relation to a DCCKI Certificate or DCCKICA Certificate, means any Party or RDP which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from the DCC or another Party or RDP pursuant to this Code.

Duties in relation to DCCKI Certificates and DCCKICA Certificates

L13.49 Each DCCKI Relying Party shall:

(a) before relying on any DCCKI Certificate:

(i) check the version of the DCCKI CRL on the DCCKI Repository, in accordance with IETF RFC 5280; and

(ii) where that DCCKI Certificate is shown on the DCCKI CRL as having been revoked, not rely on the DCCKI Certificate; and

(b) before relying on any DCCKICA Certificate:

(i) check the version of the DCCKI ARL on the DCCKI Repository, in accordance with IETF RFC 5280; and

(ii) where that DCCKICA Certificate is shown on the DCCKI ARL as having been revoked, not rely on the DCCKICA Certificate.

L13.50 No DCCKI Relying Party may rely on a DCCKI Certificate where the Validity Period of that DCCKI Certificate has expired.

L13.51 No DCCKI Relying Party may rely on a DCCKI Certificate or DCCKICA Certificate where it suspects that the DCCKI Certificate has been Compromised.

L13.52 Each DCCKI Relying Party shall ~~use its reasonable endeavours~~take reasonable

steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any DCCKI Certificate or DCCKICA Certificate.

The DCCKI PMA Functions

Performance of the DCCKI Functions

L13.53 The DCC shall make arrangements which shall ensure that:

(a) a senior member of DCC Personnel;

(b) a senior member of the personnel of a DCC Service Provider; or

(c) a number of individuals, each of whom falls within either paragraph (a) or (b), acting together,

shall carry out the DCCKI PMA Functions.

The DCCKI PMA Functions

L13.54 For the purpose of this Section L13, the "**DCCKI PMA Functions**" shall mean the activities of:

(a) approving the DCCKI CPS, and any amendments to it;

(b) periodically:

(i) reviewing the effectiveness of the DCCKI Document Set (including so as to evaluate whether the DCCKI Document Set remains consistent with the SEC Objectives); and

(ii) identifying any changes that should be made to the DCCKI Document Set in order to ensure that the DCC meets its obligations under Section G (Security);

(c) as soon as is reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in

accordance with section 88 of the Energy Act 2008, carrying out in relation to it the activities specified in paragraph (a) above:

(i) the DCCKI Certificate Policy;

(ii) the DCCKI RAPP;

(d) on receipt by the DCC of a notification from the SMKI PMA in accordance with Section L1.17(e) (Duties of the SMKI PMA), carrying out in relation to the DCCKI Document Set the activities specified in paragraph (a) above, having regard in particular to any recommendation for action made by the SMKI PMA; and

(e) performing any other duties expressly described as DCCKI PMA Functions elsewhere in this Code.

The Duties of the DCC

L13.55 Where the individual(s) carrying out the DCCKI PMA Functions notifies the DCC of any matter, or makes any recommendation with regard to the compliance by the DCC with its obligations under Section G (Security) (including in particular any recommendation for the modification of the DCCKI Document Set for the purpose of ensuring such compliance), the DCC shall:

(a) consider and take into account the matter notified, or recommendation made, to it; and

(b) where, having done so, it considers that it would be appropriate to make a change to the:

(i) DCCKI SEC Documents, submit a Modification Proposal for that purpose; and

(ii) DCCKI CPS, propose amendments to it in accordance with Section L13.42.

L13.56 The DCC shall ensure that the SMKI PMA and Security Sub-Committee shall each be provided with such of the following information as it may request:

(a) any notification or recommendation made to the DCC by the individual(s) carrying out the DCCKI PMA Functions; and

(b) copies of all agenda and supporting papers available at any meeting between individuals acting together to carry out the DCCKI PMA Functions, insofar as those agenda and papers are reasonably relevant to the functions of the SMKI PMA or Security Sub-Committee (as the case may be).

L13.57 The DCC shall ensure that, where it receives any report with regard to its ISO 27001 certification and part of that report relates to any matters concerned with the DCCKI Services, it will as soon as reasonably practicable provide those parts of that report to the SMKI PMA.

SECTION M: GENERAL

M1 COMMENCEMENT AND DURATION

Commencement

M1.1 This Code shall take effect from the effective date designated by the Secretary of State pursuant to Condition 22 of the DCC Licence.

Duration

M1.2 Once this Code comes into effect, it shall remain in effect:

(a) in respect of the DCC, until the DCC ceases to be a Party in accordance with Section M9 (Transfer of the DCC Licence); and

(b) in respect of each Party other than the DCC, until (subject to Section M8.14) such Party ceases to be a Party in accordance with Section M8 (Suspension, Expulsion and Withdrawal).

M2 LIMITATIONS OF LIABILITY

Unlimited Liabilities

M2.1 Nothing in this Code or any Bilateral Agreement shall exclude or limit a Party's Liability:

(a) for death or personal injury resulting from the negligence of that Party;

(b) for fraud or fraudulent misrepresentation;

(c) to pay the Charges and any interest accruing in respect of the Charges in accordance with this Code; or

(d) for any other type of Liability which cannot by law be excluded or limited.

Exclusion of Indirect Loss

M2.2 No Party shall in any circumstances be liable to another Party for loss arising as a result of a breach of this Code and/or any Bilateral Agreement that does not directly result from such breach and that was not reasonably foreseeable as likely to occur in the ordinary course of events.

Confidentiality and Intellectual Property Rights

M2.3 Each Party's Liability for breaches of Section M4 (Confidentiality) shall be:

(a) in the case of any breach of Section M4.20 (Confidentiality of DCC Data) relating to Data that has been clearly marked by the DCC as 'confidential', unlimited (save as provided in Section M2.2); and

(b) in the case of any other breach of Section M4, limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents, save as provided in Section M2.3A.

M2.3A The Liability of the DCC for a breach of Section M4.1 (Prohibition on disclosure and use by DCC) shall, where the amount of that Liability is recoverable by the DCC from a DCC Service Provider in accordance with the terms of a DCC Service Provider

Contract, be:

(a) unlimited if the amount of the Liability that is recoverable from the DCC Service Provider is unlimited; or

(b) limited to any amount in which the Liability that is recoverable from the DCC Service Provider is limited, or to £1,000,000 (one million pounds) in respect of each incident or series of related incidents, whichever is the greater,

but, for the purposes of this Section, no regard shall be had to any limitation in a DCC Service Provider Contract which is expressed to be set by reference to any amount specified in or calculated under this Code.

M2.4 Each Party's Liability for any breach of Section M5 (Intellectual Property Rights) shall be unlimited (save as provided in Section M2.2).

Damage to Physical Property

M2.5 Subject to Section M2.1, each Party's Liability for loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data) arising as a result of a breach by that Party of this Code and/or any Bilateral Agreement shall be limited as follows:

(a) the Liability of the DCC shall be limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents; and

(b) the Liability of each Party other than the DCC shall be limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents,

for which purposes:

(c) where a defect in the design, manufacture, materials or workmanship of two (or more) Devices causes loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data), the defect in each such Device shall constitute a separate unrelated incident; and

(d) where a Party's Liability exceeds £1,000,000 (one million pounds) and is

limited under this Section M2.5 and that Liability is in respect of loss or damage suffered by more than one other Party, each such other Party shall be entitled to recover a proportion of the £1,000,000 (one million pounds) calculated by reference to the amount of any loss and damage suffered by it expressed as a fraction of the total amount of loss and damage suffered by such other Parties collectively.

Recovery of Loss which is Expressly Permitted

M2.6 It is expressly agreed that a Party may recover the following losses arising as a result of a breach of this Code (and without intending to limit recovery of any other Liability that may arise as a result of such breach):

(a) (subject to Sections F9.25 (Exclusive Remedies for Site Visits) and M2.5) where such breach causes the loss of, or damage to, a Smart Metering System (or any part of it), the Import Supplier, Export Supplier and/or Gas Supplier (as applicable) for that Smart Metering System shall be entitled to recover the reasonable costs and expenses (including reasonable labour costs) incurred in attending the relevant premises for the purpose of repairing or replacing that Smart Metering System (or the relevant part of it);

(b) in the case of breaches of Section F6 (Delivery and Acceptance of Communications Hubs) and/or the CH Handover Support Materials, the DCC shall be entitled to recover the reasonable costs and expenses referred to in Section F6.18 (Failure to Accept Delivery);

(c) where such breach causes an Organisation Certificate to be Compromised or issued otherwise than in accordance with the relevant Certificate Policy (and, in either case, the Subscriber wishes it to be replaced), the reasonable costs and expenses (including reasonable labour costs) incurred in replacing any or all such Compromised Certificates held on Devices (but not the costs and expenses of replacing Device Certificates), limited to £1,000,000 (one million pounds) in respect of each incident or series of related incidents; and

(d) where such breach (including a breach which is deemed to occur in accordance

with Section L10.26 (Breach of the Code by the Relevant Subscriber)) gives rise to a Recovery Event such that the DCC incurs (or is required to make payments in respect of) Recovery Costs under Section L10 (the SMKI Recovery Procedure), the DCC shall be entitled to recover the Recovery Costs that it has incurred (or been required so to pay), limited to £1,000,000 (one million pounds) in respect of each Recovery Event.

Exclusion of Loss of Profit etc.

M2.7 Subject to Sections M2.1 and M2.6 and save in the case of a breach referred to in Section M2.3(b) or M2.4, no Party shall in any circumstances be liable to another Party for any of the following losses arising as a result of a breach of this Code and/or any Bilateral Agreement:

(a) loss of profit;

(b) loss of revenue;

(c) loss of use;

(d) loss of contract;

(e) loss of goodwill; or

(f) loss resulting from the liability of such other Party to a third party for any of the matters referred to in paragraphs (a) to (e) above.

Exclusion of Other Liabilities

M2.8 Subject to Sections M2.1 and M2.6 and save in the case of a breach of those provisions referred to in Section M2.3 or M2.4, no Party shall be liable to any other Party for loss arising from any breach of this Code and/or any Bilateral Agreement other than for losses that are subject to Section M2.5. This Section M2.8 is without prejudice to the operation of the Charging Methodology, and the payments required under Section F9.22 (Payment of Type Fault and Batch Fault Compensation) or F9.23 (Compensation for Product Recall or Technology Refresh).

M2.9 The rights and remedies provided by this Code and/or any Bilateral Agreement are exclusive and not cumulative, and exclude and are in place of all substantive (but not procedural) rights or remedies provided by common law or statute in respect of the subject matter of this Code and/or any Bilateral Agreement, including any rights that any Party may possess in tort (or delict).

M2.10 Subject to Section M2.1, each of the Parties hereby waives to the fullest extent possible all such rights and remedies provided by common law or statute (and releases the other Parties to the same extent from all Liabilities or obligations provided by common law or statute in respect of the subject matter of this Code and/or any Bilateral Agreement).

Statutory Rights

M2.11 For the avoidance of doubt, nothing in this Section M2 shall exclude or restrict or otherwise prejudice or affect any of:

(a) the rights, powers, duties and obligations of any Party which are conferred or created by the Relevant Instruments; or

(b) the rights, powers and duties of the Authority or the Secretary of State.

Other Matters

M2.12 Each of the sub-clauses of this Section M2 shall be construed as a separate and severable contract term, and if one or more of such sub-clauses is held to be invalid, unlawful or otherwise unenforceable, then the other or others of such sub-clauses shall remain in full force and effect and shall continue to bind the Parties.

M2.13 In respect of all substantive (but not procedural) rights or remedies provided by common law or statute (including in tort or delict, but without prejudice to contractual rights or remedies) in respect of loss of or damage to physical property (including loss of or damage to Systems, and loss or corruption of Data) arising in relation to the subject matter of this Code and/or any Bilateral Agreement, it is agreed that:

(a) each Party hereby waives and releases (to the fullest extent possible at law) such rights and remedies in respect of such loss or damage as such Party may otherwise have against the contractors, employees and agents of each other

Party (including the DCC Service Providers) in their capacity as such;

(b) the DCC shall ensure that each DCC Service Provider (when acting in its capacity as such) waives and releases (to the fullest extent possible at law) such rights and remedies in respect of such loss or damage as such DCC Service Provider may otherwise have against the Parties other than DCC in their capacity as such (and/or against the contractors, employees and agents of such Parties in their capacity as such);

(c) the waiver and release referred to in Section M2.13(a) is to be enforceable by the persons stated therein to have the benefit thereof in accordance with Section M11.5 (Third Party Rights); and

(d) the DCC shall ensure that the waiver and release referred to in Section M2.13(b) is enforceable by the persons stated therein to have the benefit thereof under the Contracts (Rights of Third Parties) Act 1999.

M2.14 Each Party shall be under a duty to mitigate its loss.

M2.15 Each Party hereby acknowledges and agrees that the provisions of this Section M2 are fair and reasonable having regard to the circumstances.

Conduct of Indemnity Claims

M2.16 Where this Code provides that one Party (the "**Indemnifier**") is to indemnify another Party (the "**Indemnified Party**") against third party claims, the Indemnified Party shall:

(a) promptly notify the Indemnifier of any such claim, and provide it with details in relation to the same and all relevant documentation excluding that which attracts legal privilege;

(b) consult with the Indemnifier with respect to the subject matter of the claim and the manner in which the Indemnified Party intends to deal with the same, keep the Indemnifier promptly advised of developments concerning the same, and have due regard to the Indemnifier's views in relation to the same;

(c) not settle, compromise or make any admission of liability concerning any such claim, without the prior written consent of the Indemnifier (such consent not to be unreasonably withheld or delayed); and

(d) where the Indemnifier so requests, allow the Indemnifier (or such person as the Indemnifier may nominate) to conduct all negotiations and proceedings regarding the claim (at the Indemnifier's cost), in which case the Indemnifier shall ensure that the claim is diligently defended in accordance with any reasonable instructions of the Indemnified Party and not settled or compromised without the Indemnified Party's consent (such consent not to be unreasonably withheld or delayed).

SECCo

M2.17 The provisions of this Section M2 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party, but shall not limit SECCo's liability under Section C3.12 (Protections for Panel Members and Others).

M2.18 Nothing in this Section M2 shall limit the DCC's liability to reimburse SECCo in respect of Recoverable Costs.

M3 SERVICES FM AND FORCE MAJEURE

Force Majeure affecting the Services - Services FM

M3.1 The concept of Services FM applies in respect of the obligations of the DCC to provide the Services pursuant to this Code (including pursuant to any Bilateral Agreement).

M3.2 The DCC may claim relief from Liability for non-performance of its obligations in respect of the Services to the extent this is due to Services FM. To the extent that performance of the DCC's obligations is unaffected by the Services FM, the provisions of this Code and any Bilateral Agreement will continue to apply.

M3.3 The DCC cannot claim Services FM has occurred:

(a) in relation to any wilful act, neglect or failure to take reasonable precautions against the relevant Services FM event by the DCC or its servants, agents, employees or contractors (including the DCC Service Providers);

(b) in relation to any circumstances resulting from a failure or delay by any other person in the performance of that other person's obligations under a contract with the DCC (unless that other person is itself prevented from or delayed in complying with its obligations as a result of Services FM); and/or

(c) as a result of any shortage of labour, material or other resources unless caused by circumstances which are themselves Services FM,

and in any event, the DCC shall not be entitled to relief if and to the extent that it is required to comply with the BCDR Procedure in accordance with Sections H10.9 and H10.10 (the Business Continuity and Disaster Recovery Procedure) but has failed to do so (unless this failure is also due to Services FM affecting the operation of the BCDR Procedure).

M3.4 The DCC shall, as soon as reasonably practicable (and in any event within five (5) days of the occurrence of the Services FM), give to the Users that were due to receive the affected Services and to the Panel full details of the Services FM and any relief the DCC wishes to claim in connection with the Services FM.

M3.5 The DCC shall be entitled to relief in respect of Services FM to the extent that the Panel agrees (or it is subsequently determined by arbitration) that the requirements of Sections M3.2 and M3.3 are met, and that:

(a) the DCC could not have avoided the occurrence of the Services FM (or its consequences or likely consequences) by taking steps which the DCC was required to take (or procure) under this Code and any Bilateral Agreement or might reasonably be expected to have taken;

(b) the Services FM directly caused the non-performance of the Services for which relief is claimed;

(c) the time lost and/or relief from the obligations under this Code and any Bilateral Agreement claimed by the DCC could not reasonably be expected to be mitigated or recovered by the DCC acting in accordance with Good Industry Practice; and

(d) the DCC is taking all steps in accordance with Good Industry Practice to overcome or minimise the consequences of the Services FM on the performance of the Services.

M3.6 If the DCC is entitled to relief in respect of Services FM in accordance with Section M3.5, then:

(a) the DCC shall be relieved of Liability under this Code and any Bilateral Agreement in respect of the Services to the extent to which that Liability would otherwise have arisen solely as a result of the Services FM; and

(b) for the avoidance of doubt, the Charges (but not, for the avoidance of doubt, the Fixed Charges) payable by a User shall be reduced to the extent that the DCC does not provide the Services to that User as a result of the Services FM (and shall be calculated on the basis of the Services that are actually provided).

M3.7 The DCC shall notify the affected Users and the Panel as soon as reasonably practicable after the Services FM ceases or no longer causes the DCC to be unable to comply with its obligations under this Code and/or any Bilateral Agreement in respect

of the Services. Following such notification, the Services shall continue to be performed in accordance with the terms and conditions existing immediately before the occurrence of the Services FM.

M3.8 The DCC hereby irrevocably and unconditionally waives all and any rights to claim any extension or allowance of time or other relief from performance of its obligations in respect of the Services other than to the extent caused by Services FM. Each User hereby irrevocably and unconditionally waives all and any rights to claim compensation (including for breach of contract or in tort) for failure by the DCC to provide the Services to the extent caused by Services FM.

Force Majeure

M3.9 The concept of Force Majeure applies in respect of:

(a) all obligations of the DCC pursuant to this Code and any Bilateral Agreement other than the obligations of the DCC to provide the Services; and

(b) all obligations of the other Parties pursuant to this Code and any Bilateral Agreement,

all such obligations together being in this Section M3 the "**Relevant Obligations**".

M3.10 Subject to Section M3.11, the Affected Party will not be in breach of this Code and/or any Bilateral Agreement or otherwise liable for any failure or delay in performance of any Relevant Obligations to the extent such failure or delay is caused by Force Majeure.

M3.11 An Affected Party may only rely upon Section M3.10 in respect of a failure or delay in performance of any Relevant Obligations to the extent that the Affected Party and the Party or Parties to whom the Affected Party owes the Relevant Obligations agree (or it is determined by arbitration) that the Affected Party:

(a) notified the Party or Parties to whom the Affected Party owes those Relevant Obligations of the matters constituting Force Majeure as soon as reasonably practicable following their occurrence;

(b) kept such Party or Parties fully informed as to the matters relating to the Force Majeure; and

(c) took all reasonable steps in accordance with Good Industry Practice to overcome the Force Majeure and/or minimise the consequences of the Force Majeure on the performance of the Relevant Obligations.

M3.12 The Affected Party shall notify the Party or Parties to whom the Affected Party owes the Relevant Obligations as soon as reasonably practicable after the Force Majeure ceases or no longer causes the Affected Party to be unable to comply with the Relevant Obligations.

M3.13 Each Party hereby irrevocably and unconditionally waives all and any rights to claim any extension or allowance of time or other relief from performance of the Relevant Obligations other than to the extent caused by Force Majeure. Each Party hereby irrevocably and unconditionally waives all and any rights to claim compensation (including for breach of contract or in tort) for, or to seek to expel the Affected Party from this Code for, any failure by the Affected Party to comply with the Relevant Obligations to the extent caused by Force Majeure.

SECCo

M3.14 The provisions of this Section M3 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

M4 CONFIDENTIALITY

Prohibition on disclosure and use by DCC

M4.1 Subject to Sections M4.3 and M4.4, the DCC shall not disclose another Party's Confidential Information to, or authorise access to another Party's Confidential Information by, any person.

M4.2 Subject to Section M4.3, the DCC shall not use a Party's Confidential Information for any purpose other than the purpose for which it was provided (or otherwise made available) to the DCC, and in any event for any purpose other than the purposes of this Code.

Circumstances in which disclosure or use by the DCC are permitted

M4.3 The restrictions on disclosure and authorisation of access in Section M4.1 and on use in Section M4.2 shall not apply to the disclosure or use of, or authorisation of access to, a Party's Confidential Information to the extent:

(a) expressly permitted or required by the DCC Licence;

(b) necessary for the exercise by the DCC of any of its obligations under the Electricity Act, the Gas Act, the DCC Licence, or this Code;

(c) made or given in accordance with the Authority's prior written consent;

(d) such Confidential Information is already available in the public domain other than as a result of a breach by the DCC of this Section M4 and/or the DCC Licence; or

(e) such Confidential Information is already lawfully in the possession of the DCC otherwise than as a result (whether directly or indirectly) of a breach of this Code and/or the DCC Licence (but without prejudice to any obligations to which the DCC is subject in respect of the use or disclosure of such Confidential Information under the arrangements relating to such lawful possession).

M4.4 The restrictions on disclosure and authorisation of access in Section M4.1 shall not apply to the disclosure of, or authorisation of access to, a Party's Confidential Information to the extent:

(a) made or given in order to comply with the DCC's duties under Laws and Directives or the rules of any recognised stock exchange; provided that, in so far as is reasonably practicable in accordance with such Laws and Directives or rules, the DCC shall provide that Party with prior notice of such proposed disclosure or authorisation of access; or

(b) made or given to the employees, other agents, contractors or advisers of the DCC to the extent such persons require such Confidential Information for the purpose of performing their roles as such; provided that such persons are subject to restrictions on the disclosure or use of, or authorisation of access to, such Confidential Information equivalent to those under this Section M4, and provided that the DCC shall be liable for any disclosure, authorisation or use by such persons otherwise than in accordance with this Section M4. This Section M4.4(b) is without prejudice to Section M4.5.

Restriction of disclosure to DCC employees who are leaving

M4.5 The DCC shall not (having regard to the nature and effective life of the Confidential Information in question) continue to disclose Confidential Information to (or authorise access to Confidential Information by) an employee or other agent of the DCC who has notified DCC of his or her intention to become engaged as an employee or agent of:

(a) any other Party; or

(b) a broker or consultant who is known to provide services in relation to the Supply of Energy and/or Commercial Activities,

save where the DCC could not, in all the circumstances, reasonably be expected to refrain from divulging to such employee or other agent Confidential Information which is required for the proper performance of his or her duties.

DCC Practices, Systems and Procedures

M4.6 The DCC shall put in place and at all times maintain managerial and operational practices, systems, and procedures designed to ensure that it complies with this Section M4.

Provision of Information to the Panel

M4.7 Each Party agrees, subject to any confidentiality provision binding on it, to provide to the Panel (or its Sub-Committees and/or Working Groups, including via the Code Administrator, the Secretariat or SECCo) all Data reasonably requested by the Panel (or its Sub-Committees and/or Working Groups, including via the Code Administrator, the Secretariat or SECCo) in order that they may properly carry out their duties and functions under this Code.

Confidentiality and the Panel

M4.8 Where a Party wishes its Party Data to remain confidential, it shall:

(a) in the case of the DCC (in so far as it acts in accordance with Sections M4.22 to M4.24) clearly mark such Party Data as either 'confidential' or 'controlled' ; and

(b) in the case of any other Party, clearly mark such Party Data as 'confidential'.

M4.9 Where a Party does not clearly mark its Party Data as 'confidential', or (in the case of the DCC only) 'controlled', the Panel (or its Sub-Committees or Working Groups, the Code Administrator, the Secretariat or SECCo, as applicable) may treat such Party Data as not being confidential (and shall have no confidentiality obligation in respect of the same).

M4.10 Subject to Section M4.11, the Panel shall not (and shall also ensure that its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo shall not) disclose, or authorise access to, any Party Data provided (or otherwise made available) to them by a Party where that Party has clearly marked such Party Data as 'confidential', or (in the case of the DCC only) 'controlled', in accordance with Section M4.8.

M4.11 The restrictions in Section M4.10 on disclosures of, or authorisation of access to, Party Data shall not apply to the extent:

(a) made or given in accordance with duties under Laws and Directives or instructions of the Authority;

(b) such Party Data is already available in the public domain other than as a result of a breach by the Panel (or its Sub-Committees or Working Groups, the Code Administrator, the Secretariat or SECCo); or

(c) such Party Data is already lawfully in the possession of the Panel (or its Sub-Committees or Working Groups, the Code Administrator, the Secretariat or SECCo) otherwise than as a result (whether directly or indirectly) of this Code and/or the DCC Licence (but without prejudice to any obligations in respect of the use or disclosure of such Party Data under the arrangements relating to such lawful possession).

M4.12 The Parties acknowledge that, in order for the Panel (and its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo) to properly carry out their duties and functions under this Code, the Panel may decide (or be obliged) to keep Data as confidential, and not disclose that Data to the Parties. The Panel shall ~~use its reasonable endeavours~~take reasonable steps to keep such instances to a minimum.

Panel Information Policy

M4.13 The Panel shall establish and maintain a policy for classifying, labelling, handling and storing Party Data received by it (and its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo) pursuant to the provisions of Section G (Security), Section I (Data Privacy), and Section L (Smart Metering Key Infrastructure) and its related SEC Subsidiary Documents.

M4.14 The Panel (and its Sub-Committees and Working Groups, the Code Administrator, the Secretariat and SECCo) shall act in accordance with the policy established and maintained in accordance with Section M4.13.

Confidentiality of DCC Data

M4.15 Where Data belonging to the DCC, or relating to the DCC or the Services, is disclosed (or otherwise becomes available) to another Party under or in relation to this Code, and where the DCC wishes such Data to remain confidential, the DCC shall (in so far as it acts in accordance with Sections M4.22 to M4.24) clearly mark such Data as either 'confidential' or 'controlled', and where the DCC does not do so the other Parties may treat such Data as not being confidential (and shall have no confidentiality obligation in respect of the same).

M4.16 Where a Party wishes to dispute whether or not Data which the DCC has marked as 'controlled' may be given that designation in accordance with Section M4.23, that Party may refer the matter to arbitration in accordance with Section M7 (Dispute Resolution).

M4.17 Where a Party wishes to be able to receive from the DCC Data which the DCC marks as 'confidential', that Party shall:

(a) provide to the DCC a list containing the names and contact details of one or more individuals who are authorised by it to receive such Data;and

(b) where it wishes to change the names and/or contact details of the individuals on the list, provide an updated version of the list to the DCC a reasonable time in advance of the update taking effect.

M4.18 Where a Party has provided to the DCC in accordance with Section M4.17 the names and contact details of one or more individuals who are authorised by it to receive Data marked by the DCC as 'confidential', the DCC shall not disclose such Data to that Party except by sending it or making it available to all of those named individuals.

M4.19 Where a Party has not provided to the DCC the names and contact details of one or more individuals who are authorised by it to receive Data marked by the DCC as 'confidential':

(a) the DCC shall be under no obligation to, and shall not, disclose any such Data to that Party; and

(b) paragraph (a) shall be deemed to take precedence over any contrary provision of this Code, and any such provision shall be read as if it incorporated no requirement to disclose any Data marked by the DCC as 'confidential'.

M4.20 Each Party other than the DCC shall not disclose, or authorise access to, Data that is clearly marked by the DCC as either 'confidential' or 'controlled', in accordance with Section M4.15, provided that such restrictions on disclosure and access shall not apply to the extent that:

(a) the disclosure is made or given in accordance with duties under Laws and Directives or instructions of the Authority;

(b) such Data is already available in the public domain other than as a result of a breach of this Code by a Party;

(c) such Data is already lawfully in the possession of the Party otherwise than as a result (whether directly or indirectly) of this Code and/or the DCC Licence (but without prejudice to any obligations in respect of the use or disclosure of such Data under the arrangements relating to such lawful possession); or

(d) such Data is clearly marked by the DCC as 'confidential', but the DCC has disclosed it to the Party by sending or making it available to an individual not named in a list provided by the Party under Section M4.17, or by using contact details different to those specified in that list, and:

(i) the disclosure or access occurs as a direct consequence of that breach by the DCC of Section M4.18; and

(ii) if the Party was made or otherwise became aware of that breach by the DCC, it had taken all reasonable steps to avoid the disclosure or access.

Use of DCC Data

M4.21 The Parties other than the DCC may only use the Data belonging to the DCC, or relating to the DCC or the Services, which is disclosed (or otherwise becomes available) to them under or in relation to this Code for the purpose of performing their obligations or exercising their rights under this Code (or for any other use that is

expressly authorised by the DCC in writing).

DCC Classification of Data

M4.22 For the purposes of Sections M4.8 and M4.15, the DCC may only mark Data as 'confidential' where:

(a) that Data relates to a DCC Service Provider providing services pursuant to a DCC Service Provider Contract which was referred to in paragraph 1.5 of schedule 1 to the DCC Licence on its grant;

(b) the DCC is subject to an existing obligation under the DCC Service Provider Contract referred to in paragraph (a) to ensure that that Data remains confidential;

(c) the DCC's Liability for breaching the obligation referred to in paragraph (b) is unlimited; and

(d) the DCC is not prohibited from marking that Data as 'confidential' under Section M4.24.

M4.23 For the purposes of Sections M4.8 and M4.15, the DCC may only mark Data as 'controlled' where:

(a) the uncontrolled disclosure of, or uncontrolled authorised access to, that Data could reasonably be considered to be prejudicial to the DCC (or any DCC Service Provider); and

(b) the DCC is not prohibited from marking that Data as 'controlled' under Section M4.24.

M4.24 The DCC shall not mark Data as either 'confidential' or 'controlled' where or to the extent that:

(a) the DCC is expressly required to place that Data in the public domain in order to comply with its duties under Laws and Directives;

(b) it is necessary for the exercise by the DCC of any of its obligations under the

Electricity Act, the Gas Act, the DCC Licence, or this Code to place that Data in the public domain; or

(c) that Data is already in the public domain other than as a result of a breach by the Parties or the Panel of this Section M4 and/or the DCC Licence.

Onward Supply of Supplier Party Data

M4.25 Where the DCC is obliged under a condition of the DCC Licence to disclose to a third party for a specified purpose information relating to a Supplier Party, that Supplier Party shall, where requested to do so, consent to the further disclosure of that information by that third party to the extent such further disclosure is necessary to fulfil that specified purpose.

Injunctive Relief

M4.26 The Parties agree that damages may not be an adequate remedy in the event of breach of this Section M4, and that a Party may seek injunctive relief in respect of any breach or potential breach of this Section M4.

M5 INTELLECTUAL PROPERTY RIGHTS

SEC Materials

M5.1 Section M5.2 applies in respect of this Code and any and all documents, materials, reports, charts and tables, diagrams and specifications, and any and all other works, inventions, ideas, designs or proposals (in whatever form, and including Modification Proposals) arising out of or in connection with the central administration, operation and development of this Code, including any and all associated drafts and working papers (collectively, the "**SEC Materials**"); provided that the SEC Materials shall not include the Consumer Data or the Services IPR.

M5.2 The Parties agree that, as between the Parties, any and all Intellectual Property Rights subsisting in the SEC Materials and the whole of the title to the SEC Materials will:

(a) be owned by SECCo; and

(b) automatically and immediately vest in SECCo upon their creation or acquisition.

M5.3 Where a Party other than SECCo acquires (by operation of Laws and Directives or otherwise) any Intellectual Property Rights in the SEC Materials, then that Party:

(a) (as far as is permitted by law) hereby assigns such Intellectual Property Rights to SECCo with full title guarantee, by way of present assignment of future Intellectual Property Rights; and

(b) (to the extent such assignment is not permitted) shall (and shall procure that any of its employees, agents or contractors shall) do all acts and things and execute all documents that may be reasonably necessary to transfer such Intellectual Property Rights to SECCo with full title guarantee (and pending such assignment shall hold such rights on trust for SECCo).

M5.4 SECCo hereby grants to each of the other Parties (for so long as they remain a Party) a royalty-free, non-exclusive, non-transferable licence to use the SEC Materials for the sole purpose of participating as a Party (including exercising its rights and performing its obligations as a Party). Each licence granted to a Party under this Section M5.4

includes the right of that Party to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of that Party's participation as a Party (and the SEC Materials are used for no other purpose).

M5.5 SECCo hereby grants to each of the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat (for so long as they each remain such) a royalty-free, non-exclusive, non-transferable licence to use the SEC Materials for the sole purpose of performing their roles as such. Each licence granted to a person under this Section M5.5 includes the right of that person to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of that person's performance of the role for which the licence was granted (and the SEC Materials are used for no other purpose).

Consumer Data

M5.6 Section M5.7 applies in respect of the Data that is obtained by the DCC (or its employees, other agents or contractors) as a result of providing Services to that User, including the Data contained in requests for Services and that is obtained as a result of communicating with Smart Metering Systems pursuant to this Code on behalf of a User (such Data being the "**Consumer Data**" of that User).

M5.7 As between the DCC and each User, any and all Intellectual Property Rights subsisting in the Consumer Data of that User shall be owned by that User (and the DCC shall make no claims in respect of such Intellectual Property Rights).

M5.8 Each User, in respect of its Consumer Data, hereby grants to the DCC a royalty-free, non-exclusive, non-transferable licence to use that Consumer Data for the sole purpose of DCC exercising its rights and performing its obligations under the Electricity Act, the Gas Act, the DCC Licence and this Code. Each licence granted to the DCC under this Section M5.8 includes the right of the DCC to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of the DCC's rights and obligations under the Electricity Act, the Gas Act, the DCC Licence and this Code (and the Consumer Data is used for no other purpose).

M5.9 Each User, in respect of its Consumer Data, shall ensure that the DCC (and its agents,

contractors and advisers) can use that Consumer Data in the manner envisaged by Section M5.8, and shall indemnify the DCC in respect of any Liabilities suffered or incurred by the DCC (or its agents, contractors or advisers) as a result of claims brought by persons alleging that the use of that Consumer Data in the manner envisaged by Section M5.8 has infringed any Intellectual Property Rights.

Party Data

M5.10 Section M5.11 applies in respect of the Data (other than SEC Materials and Consumer Data) that is provided (or otherwise made available) pursuant to this Code to the Panel (or its Sub-Committees and/or Working Groups, including via the Code Administrator, the Secretariat or SECCo) by or on behalf of a Party (such Data being the "**Party Data**" of that Party).

M5.11 As between the Panel (including its Sub-Committees and/or Working Groups, the Code Administrator, the Secretariat and SECCo) and each Party, any and all Intellectual Property Rights subsisting in the Party Data of that Party shall be owned by that Party (and none of the Panel, its Sub-Committees, its Working Groups, the Code Administrator, the Secretariat or SECCo shall make any claims in respect of such Intellectual Property Rights).

M5.12 Without prejudice to Section M4.10 (Confidentiality and the Panel), each Party, in respect of its Party Data, hereby grants to SECCo, the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat a royalty-free, non-exclusive, non-transferable licence to use that Party Data for the sole purpose of performing their roles as such. Each licence granted to a person under this Section M5.12 includes the right of that person to grant sub-licences to its agents, contractors and advisers provided that they are granted solely in respect of that person's performance of the role for which the licence was granted (and the Party Data is used for no other purpose).

M5.13 Without prejudice to Section M4.10, each Party, in respect of its Party Data, shall ensure that SECCo, the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat (and their agents, contractors and advisers) can use that Party Data in the manner envisaged by Section M5.12, and

shall indemnify the SECCo, the Panel Members, any Sub-Committee or Working Group members, the Code Administrator and the Secretariat in respect of any Liabilities suffered or incurred by them (or their agents, contractors or advisers) as a result of claims brought by persons alleging that the use of that Party Data in the manner envisaged by Section M5.12 has infringed any Intellectual Property Rights.

Services IPR

M5.14 Section M5.15 applies in respect of the Intellectual Property Rights created by, arising from or that are associated with:

(a) the activities undertaken by the DCC for the purposes of carrying on its Authorised Business (as defined in the DCC Licence) in accordance with the DCC Licence; or

(b) the operation of a DCC Service Provider Contract in accordance with its provisions,

such Intellectual Property Rights being the "**Services IPR**".

M5.15 As between the DCC and each User, the Services IPR shall be owned by the DCC (and no User shall make any claims in respect of the Services IPR).

M5.16 The DCC hereby grants to each User a royalty-free, non-exclusive, non-transferable licence to use the Services IPR for the sole purpose of receiving (and to the extent necessary to receive) the Services. Each licence granted by the DCC under this Section M5.16 includes the right of the User to grant sub-licences to its agents, and contractors provided that they are granted solely for the purpose of the User receiving (and to the extent necessary for the User to receive) the Services (and that the Services IPR is used for no other purpose).

M5.17 The DCC shall ensure that each User (and its agents and contractors) can use the Services IPR in the manner envisaged by Section M5.16, and shall indemnify each User in respect of any Liabilities suffered or incurred by that User (or its agents or contractors) as a result of claims brought by persons alleging that the use of that Services IPR in the manner envisaged by Section M5.16 has infringed any Intellectual

Property Rights.

General

M5.18 For the avoidance of doubt, the use by a Party of Intellectual Property Rights licensed to it under this Section M5 otherwise than in accordance with such licence shall constitute a breach of this Code.

M5.19 The Parties agree that damages may not be an adequate remedy in the event of breach of this Section M5, and that a Party may seek injunctive relief in respect of any breach or potential breach of this Section M5.

SECCo

M5.20 The provisions of this Section M5 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

M6 PARTY DETAILS

Provision of the Party Details

M6.1 Each Party's original Party Details shall be provided as part of its Framework Agreement counterpart or its Accession Agreement (as applicable).

Amendments to Party Details

M6.2 Each Party may amend its Party Details by notice to the Secretariat from time to time, and each Party shall ensure that its Party Details remain up-to-date.

Publication

M6.3 The Secretariat shall maintain a record of each Party's Party Details, and shall publish that record on the Website (other than those elements of the Party Details that are identified in Schedule 5 as being confidential).

M6.4 As soon as reasonably practicable after each person becomes a Party, or following notification of an amendment to a Party's Party Details in accordance with Section M6.2, the Secretariat shall update the record referred to in Section M6.3.

M6.5 The Secretariat shall take reasonable steps~~use its reasonable endeavours~~ to identify any errors or omissions in each Party's Party Details, and shall notify the relevant Party of any such errors or omissions.

M7 DISPUTE RESOLUTION

Duty to Seek to Resolve

M7.1 Where a Dispute arises between two or more Parties, each such Party shall seek to resolve the Dispute amicably within a reasonable timescale through negotiation in good faith.

Reference to the Authority

M7.2 Any Dispute of a nature that is expressly stated in this Code or in the Electricity Act or the Gas Act or in the Energy Licences to be subject to determination by the Authority shall be subject to determination by the Authority (which shall be final and binding for the purposes of this Code). For the purposes of Condition 20.3(c) of the DCC Licence, disputes of the nature referred to in Condition 20 of the DCC Licence in respect of the following Other Enabling Services shall be subject to determination by the Authority pursuant to that condition:

(a) requests by TCH Participants for Test Communications Hubs pursuant to Section F10 Test Communications Hubs);

(b) requests by Parties for Detailed Evaluations pursuant to Section H7.7 (Detailed Evaluations of Elective Communication Services);

(c) requests by Parties for the provision of further assistance in respect of the Parse and Correlate Software pursuant to Section H11.12 (Provision of Support and Assistance to Users);

(d) requests by Testing Participants for the provision of a connection to a simulation of the SM WAN for the purposes of testing pursuant to Section H14.31 (Device and User System Tests);

(e) requests by Testing Participants for the provision of additional testing support pursuant to Section H14.33 (Device and User System Tests); and

(f) requests by Parties for DCC Gateway Connections pursuant to Section H15 (DCC Gateway Connections).

Reference to the Panel or its Sub-Committees

M7.3 Any Dispute of a nature that is expressly stated in this Code or a Bilateral Agreement to be subject to determination by the Panel (or one of its Sub-Committees) shall be subject to determination by the Panel (or that Sub-Committee). The Panel shall ensure that any such Dispute is determined within a reasonable period of time after its referral to the Panel (or its Sub-Committee).

M7.4 Unless such determination by the Panel (or one of its Sub-Committees) is expressly stated in this Code or a Bilateral Agreement to be final and binding, such disputes shall (following the Panel's or Sub-Committee's determination) be subject to final determination by the Authority (where this is expressly stated to be the case) or as referred to in Section M7.5.

Arbitration

M7.5 Subject to Sections M7.2, M7.3 and M7.4, any Dispute shall be subject to determination by arbitration in accordance with Section M7.6 (subject to Section M7.13).

M7.6 Where this Section M7.6 applies:

(a) the Party seeking to initiate the arbitration shall give a written notice to the other Party or Parties involved in the Dispute, stating that the matter is to be referred to arbitration and setting out a brief summary of the Dispute;

(b) the Party seeking to initiate the arbitration shall send a copy of that notice to the Panel;

(c) to the extent consistent with this Section M7.6, the arbitration shall be subject to the Arbitration Act 1996 and the rules of the London Court of International Arbitration (the **LCIA**);

(d) the arbitrator shall be a person appointed by agreement between the Parties involved in the Dispute, or (in the absence of agreement within 10 Working Days following the notice under Section M7.6(a)) appointed by the LCIA;

(e) (unless otherwise agreed by the Parties involved in the Dispute) the arbitration proceedings shall take place in London and in the English language;

(f) the Parties involved in the Dispute agree to keep the arbitration process (and the decision or anything said, done or produced in or in relation to the arbitration process) confidential, except as may be required by Laws and Directives and provided that representatives of the Panel may attend the arbitration and receive a copy of the decision;

(g) the Panel shall treat the decision and all other information relating to the arbitration as confidential, and Section M4.10 (Confidentiality and the Panel) shall apply to the decision and such information;

(h) the arbitrator shall have the power to make provisional awards as provided for in Section 39 of the Arbitration Act 1996; and

(i) subject to any contrary award by the arbitrator, each Party involved in the Dispute shall bear its own costs in relation to the arbitration and an equal share of the fees and expenses of the arbitrator.

M7.7 The decision of the arbitrator pursuant to a reference in accordance with Section M7.6 shall be final and binding on each of the Parties to the arbitration, except where there is a serious irregularity (as defined in section 68(2) of the Arbitration Act 1996) or a Party successfully appeals the arbitral award on a point of law in accordance with section 69 of the Arbitration Act 1996. Each Party shall comply with such decision provided that (for the avoidance of doubt) the arbitrator shall not have the power to modify this Code.

DCC Service Provider Disputes

M7.8 If any Dispute that is subject to determination by arbitration involves the DCC, and the DCC considers that the Dispute relates to a dispute it has under or in relation to one or more of the DCC Service Provider Contracts, then the DCC may join the relevant DCC Service Provider or DCC Service Providers to the arbitration, so that the arbitrator hears and determines the disputes under or in relation to the DCC Service Provider Contracts simultaneously with the Dispute. The Parties other than the DCC hereby

consent to such joining of disputes.

M7.9 Where the DCC is aware of any dispute arising under or in relation to one or more DCC Service Provider Contracts that may reasonably relate to a Dispute or potential Dispute that would be subject to arbitration, then the DCC may give notice of that dispute to the Panel and to any or all of the other Parties.

M7.10 Where the DCC gives notice to a Party under Section M7.9, such notice shall only be valid if the DCC gives reasonable detail of such dispute and expressly refers to the waiver that may potentially be given by that Party under Section M7.12.

M7.11 Within 30 Working Days after the DCC has given a valid notification to a Party under Section M7.9 in respect of a dispute under or in relation to a DCC Service Provider Contract, that Party should give notice to the DCC of any Dispute that that Party wishes to bring in relation to that dispute. Where that Dispute is to be resolved by arbitration, the DCC may then exercise its rights under Section M7.8.

M7.12 Where the DCC gives notice to a Party in accordance with Section M7.9, and where that Party does not give notice to the DCC in accordance with Section M7.11, then that Party shall be deemed to have waived any right it may have to bring a claim against the DCC in respect of the subject matter of the dispute in question (and shall, notwithstanding Section M2 (Limitations of Liability), indemnify the DCC in full against any Liabilities incurred by the DCC as a consequence of that Party bringing any such claim).

Claims by Third Parties

M7.13 Subject to Section M7.14, if any person who is not a Party to this Code brings any legal proceedings in any court against any Party and that Party considers such legal proceedings to raise or involve issues that are or would be the subject matter of a Dispute or potential Dispute that would (but for this Section M7.13) be subject to arbitration, then (in lieu of arbitration) the court in which the legal proceedings have been commenced shall hear and determine the legal proceedings and the Dispute between such person and the Parties.

M7.14 If any person who is not a Party to this Code brings any legal proceedings in any court

against any Party and that Party considers such legal proceedings to raise or involve issues that are the subject matter of a Dispute that is already subject to an ongoing arbitration, then Section M7.13 shall only apply where the arbitrator in that arbitration determines that such legal proceedings raise or involve issues that are the subject matter of the Dispute.

Injunctive Relief

M7.15 Nothing in this Section M7 shall prevent a Party seeking interim or interlocutory remedies in any court in relation to any breach of this Code.

SECCo

M7.16 The provisions of this Section M7 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

M8 SUSPENSION, EXPULSION AND WITHDRAWAL

Events of Default

M8.1 An "**Event of Default**" shall have occurred in respect of any Party other than the DCC (the "**Defaulting Party**") if one or more of the following occurs in respect of the Defaulting Party:

(a) the Defaulting Party does not hold an Energy Licence and has not, during any period of six consecutive months, done any or all of the following: (i) taken one or more Services; and/or (ii) made a request for a formal offer for a proposed Elective Communication Service;

(b) the Defaulting Party has committed a material breach of Section I1.2 (User Obligations);

(c) the Defaulting Party has failed in a material respect to comply with an enforcement notice served by the Information Commissioner pursuant to section 40 of the Data Protection Act, whether such failure has been notified to the Panel by the Information Commissioner or the Panel has otherwise become aware of such failure;

(d) the DCC has served a notice on the Defaulting Party in accordance with Section J2.1 (Notification of Payment Failure) in respect of Charges payable by the Defaulting Party, and such Charges have not been paid within three (3) Working Days following that notice;

(e) the DCC has issued a notice to the Defaulting Party in accordance with Section J3.14 (Breach of Credit Cover Obligations) in respect of Credit Support required to be procured by the Defaulting Party, and such Credit Support has not been provided within three (3) Working Days following that notice;

(f) the Defaulting Party has not paid any amount other than in respect of the Charges (failures in respect of which are subject to Section M8.1(d)) which the Defaulting Party is due to have paid under this Code, and does not remedy such failure within five (5) Working Days after a notice requiring it to do so (which

notice must refer to this Section M8);

(g) the Defaulting Party has made a material misrepresentation in its Application Form;

(h) the Defaulting Party is in material breach of any of its material obligations under this Code and/or any Bilateral Agreement (other than those that are subject to another paragraph of this Section M8.1) and the Defaulting Party has failed to remedy the breach (or to desist from the breach and mitigate its effects insofar as it is reasonably practicable to do so) within 20 Working Days after a notice requiring it to do so (which notice must describe the breach in reasonable detail and refer to this Section M8); and/or

(i) the Defaulting Party suffers an Insolvency Type Event.

Notification of an Event of Default

M8.2 Where the DCC or the Code Administrator or the Secretariat becomes aware that an Event of Default has occurred in respect of a Party, then the DCC or the Code Administrator or the Secretariat (as applicable) shall notify the Panel of such occurrence. Where any Party other than the DCC becomes aware that an Event of Default has occurred in respect of another Party, the Party that has become so aware may notify the Panel of such occurrence.

Investigation of an Event of Default

M8.3 Where the Panel has reason to believe that an Event of Default may have occurred in respect of a Party, then the Panel may investigate the circumstances relating to such potential Event of Default. Each Party shall provide all reasonable Data and cooperation as the Panel may reasonably request in respect of any such investigation.

Consequences of an Event of Default

M8.4 Where an Event of Default occurs in respect of a Defaulting Party and while that Event of Default is continuing, the Panel may take one or more of the following steps (in each case to the extent and at such time as the Panel sees fit, having regard to all the circumstances of the Event of Default and any representations made by any Competent

Authority or any Party, provided that the Panel must always take the steps referred to in Section M8.4(a) and (b)):

(a) notify the Authority that such Event of Default has occurred in respect of the Defaulting Party;

(b) notify the Defaulting Party that such Event of Default has occurred in respect of it;

(c) notify each other Party that such Event of Default has occurred in respect of the Defaulting Party;

(d) require the Defaulting Party to give effect to a reasonable remedial action plan designed to remedy and/or mitigate the effects of the Event of Default within a reasonable timescale (a material breach of which plan shall in itself constitute an Event of Default);

(e) suspend one or more of the Defaulting Party's rights referred to in Section M8.5 (following such prior consultation with the Defaulting Party as the Panel considers appropriate);

(f) instruct the DCC to suspend (in which case the DCC shall, within one Working Day thereafter, suspend) one or more of the Defaulting Party's rights referred to in Section M8.6 (following such prior consultation with the Defaulting Party as the Panel considers appropriate); and/or

(g) expel the Defaulting Party from this Code subject to and in accordance with Section M8.10.

Suspension of Rights

M8.5 The rights referred to in Section M8.4(e) are:

(a) the right of the Defaulting Party (and each other member of its Voting Group) to vote in Panel Member elections under Section C4 (Panel Elections);

(b) the right of the Defaulting Party to raise new Modification Proposals under

Section D (Modifications); and

(c) the right of the Defaulting Party to influence the appointment of a Change Board Member, so that:

(i) in the case of a Supplier Party, the Change Board Member appointed by the Voting Group of which that Supplier Party forms part shall be suspended; or

(ii) in the case of any Party other than a Supplier Party, the Secretariat shall ignore the views of that Party when considering any request to appoint or remove a Change Board Member appointed by the Party Category of which that Party forms part.

M8.6 The rights referred to in Section M8.4(f) are:

(a) the right of the Defaulting Party to receive Core Communication Services or Local Command Services in the 'Other User' User Role;

(b) (subject to the Authority's approval) the right of the Defaulting Party to receive Core Communication Services or Local Command Services in any User Role other than the 'Other User' User Role;

(c) (subject to the Authority's approval) the right of the Defaulting Party to receive any or all Elective Communication Services;

(d) (subject to the Authority's approval) the right of the Defaulting Party to initiate Enrolment of Smart Metering Systems; and

(e) (subject to the Authority's approval) the right of the Defaulting Party to request or receive any or all Services other than those referred to elsewhere in this Section M8.6.

M8.7 The suspension of any or all of the Defaulting Party's rights referred to in Section M8.5 or M8.6 shall be without prejudice to the Defaulting Party's obligations and Liabilities under and in relation to this Code (whether accruing prior to, during, or after such suspension). Without prejudice to the generality of the foregoing, the Defaulting

Party shall continue to be liable for all Charges that it is or becomes liable to pay under this Code.

M8.8 Where the Panel has, pursuant to Section M8.4(e) and/or (f), suspended a Party's rights, then the Panel may at any time thereafter end such suspension (provided that, in the case of rights that the Panel cannot suspend without the Authority's approval, the Panel may not end such suspension without the Authority's approval).

Ceasing to be a Party

M8.9 A Party that holds an Energy Licence that requires that Party to be a party to this Code:

(a) cannot be expelled from this Code by the Panel unless the Authority has approved such expulsion (and, in the case of any such approval, Section M8.10(a) shall apply as if the Party did not hold an Energy Licence that requires it to be a party to this Code); and

(b) cannot voluntarily cease to be a Party while that Energy Licence remains in force.

M8.10 A Party that does not hold an Energy Licence that requires that Party to be a party to this Code:

(a) may (while an Event of Default is continuing in respect of that Party) be expelled from this Code with effect from such time on such date as the Panel may resolve (where the Panel considers it reasonable to do so in the circumstances); and

(b) may give notice to the Panel of that Party's intention to voluntarily cease to be a Party and of the time on the date from which it wishes to cease to be a Party. The Panel shall, following receipt of such a notice, resolve that that Party shall cease to be a Party with effect from the time on the date notified.

M8.11 The Panel shall notify the Authority and each remaining Party in the event that any person is expelled from this Code or voluntarily ceases to be a Party.

Appeal to the Authority

M8.12 Where the Panel resolves to suspend the rights of a Party and/or to expel a Party pursuant to this Section M, then that Party may at any subsequent time apply to the Authority to have such suspension lifted or to be reinstated as a Party. The Parties and the Panel shall give effect to any decision of the Authority pursuant to such application, which shall be final and binding for the purposes of this Code.

Consequences of Ceasing to be a Party

M8.13 Where the Panel makes a resolution in respect of a Party in accordance with Section M8.10, then with effect from the time on the date at which such resolutions are effective:

(a) that Party's accession to this Code shall be terminated, and it shall cease to be a Party; and

(b) subject to Section M8.14, that Party shall cease to have any rights or obligations under this Code or any Bilateral Agreement.

M8.14 The termination of a Party's accession to this Code shall be without prejudice to:

(a) those rights and obligations under this Code and/or any Bilateral Agreement that may have accrued prior to such termination; or

(b) those provisions of this Code or any Bilateral Agreement that are expressly or by implication intended to survive such termination, including Sections A (Definitions and Interpretation), J (Charges), M2 (Limitations of Liability), M5 (Intellectual Property Rights), M7 (Dispute Resolution), M10 (Notices), and M11 (Miscellaneous).

M9 TRANSFER OF DCC LICENCE

Introduction

M9.1 This Section M9 is included in accordance with Condition 22 of the DCC Licence, and provides for the transfer of (amongst other things) the DCC's interest in this Code to a Successor Licensee.

Application and Interpretation of this Section M9

M9.2 This Section M9 shall only apply where two persons hold a DCC Licence at the same time. In such circumstances:

(a) "**Transfer Date**" has the meaning given to that expression in Condition 43 of the earlier of the two DCC Licences;

(b) until the Transfer Date, the holder of the earlier DCC Licence shall be "**the DCC**" for the purposes of this Code, and the holder of the later DCC Licence shall be "**the Successor Licensee**"; and

(c) from the Transfer Date, all references in this Code to "**the DCC**" shall be references to the holder of the later DCC Licence.

Novation Agreement

M9.3 Where this Section M9 applies, the DCC and the Successor Licensee shall each enter into a novation agreement in a form approved by the Authority.

M9.4 Such novation agreement will, with effect from the Transfer Date, novate to the Successor Licensee all rights and obligations of the DCC under the agreements referred to in Section M9.5 (including all rights obligations and liabilities of the DCC that may have accrued in respect of the period prior to the Transfer Date).

M9.5 Such novation agreement shall be in respect of the following agreements:

(a) the Framework Agreement;

(b) all Accession Agreements; and

(c) all Bilateral Agreements.

M9.6 The DCC shall enter into such novation agreement in (to the extent applicable) its own right, and also (to the extent applicable) on behalf of the Parties (which shall include SECCo) that are counterparties to the agreements referred to in Section M9.5.

DCC Authority to enter into Accession Agreements

M9.7 Each Party (which shall include SECCo) hereby irrevocably and unconditionally authorises the DCC to execute and deliver, on behalf of such Party, a novation agreement as envisaged by this Section M9.

Co-operation

M9.8 Each Party shall do all such things as the Panel may reasonably request in relation to the novation of the agreements referred to in Section M9.5 from the DCC to the Successor DCC.

M10 NOTICES

Communication via Specified Interfaces

M10.1 This Code requires certain communications to be sent via certain specified means, including as described in:

(a) Section E2 (Provision of Registration Data);

(b) Section H3 (DCC User Interface);

(c) Section H8 (Service Management, Self-Service Interface and Service Desk); and

(d) Section L4 (The SMKI Service Interface) and L5 (The SMKI Repository Interface).

Other Notices

M10.2 Save as referred to in Section M10.1, any notice or other communication to be made by one Party to another Party under or in connection with this Code or any Bilateral Agreement shall be in writing and shall be:

(a) delivered personally or by courier;

(b) sent by first class prepaid post; or

(c) sent by fax or email.

M10.3 All notices and communications as described in Section M10.2 shall be sent to the physical address, fax number or email address specified for such purpose in the relevant Party's Party Details. Where no fax or email address is specified for a particular type of notice or communication, notice may not be given in that manner.

M10.4 Subject to Section M10.5, all notices and communications as described in Section M10.2 shall be deemed to be received by the recipient:

(a) if delivered personally or by courier, when left at the address set out for such purpose in the relevant Party's Party Details;

(b) if sent by first class prepaid post, two Working Days after the date of posting;

(c) if sent by fax, upon production by the sender's equipment of a transmission report indicating that the fax was sent to the fax number of the recipient in full without error; and

(d) if sent by email, one hour after being sent, unless an error message is received by the sender in respect of that email before that hour has elapsed.

M10.5 Any notice that would otherwise be deemed to be received on a day that is not a Working Day, or after 17.30 hours on a Working Day, shall be deemed to have been received at 9.00 hours on the next following Working Day.

The Panel, Code Administrator, Secretariat and SECCo

M10.6 Notices between a Party and any of the Panel, the Code Administrator, the Secretariat or SECCo shall also be subject to this Section M. Notices to any of the Panel, the Code Administrator, the Secretariat or SECCo shall be sent to the relevant address given for such purpose, from time to time, on the Website (or, in the absence of any such address, to SECCo's registered office).

Process Agent

M10.7 Any Party (being a natural person) who is not resident in Great Britain or (not being a natural person) which is not incorporated in Great Britain shall, as part of its Party Details, provide an address in Great Britain for service of process on its behalf in any proceedings under or in relation to this Code and/or any Bilateral Agreement. Where any such Party fails at any time to provide such address, such Party shall be deemed to have appointed SECCo as its agent to accept such service of process on its behalf.

M11 MISCELLANEOUS

Entire Code

M11.1 This Code and any document referred to herein represents the entirety of the contractual arrangements between the Parties in relation to the subject matter of this Code. This Code and any document referred to herein supersedes any previous contract between any of the Parties with respect to the subject matter of this Code.

M11.2 Each Party confirms that, except as provided in this Code and without prejudice to any claim for fraudulent misrepresentation, it has not relied on any representation, warranty or undertaking which is not contained in this Code or any document referred to herein.

Severability

M11.3 If any provision of this Code shall be held to be invalid or unenforceable by a judgement or decision of any Competent Authority, that provision shall be deemed severable and the remainder of this Code shall remain valid and enforceable to the fullest extent permitted by law.

Waivers

M11.4 The failure by any Party to exercise, or the delay by any Party in exercising, any right, power, privilege or remedy provided under this Code or by law shall not constitute a waiver thereof nor of any other right, power, privilege or remedy. No single or partial exercise of any such right, power, privilege or remedy shall preclude any future exercise thereof or the exercise of any other right, power, privilege or remedy.

Third Party Rights

M11.5 The following persons shall be entitled to enforce the following rights in accordance with the Contracts (Rights of Third Parties) Act 1999:

(a) the person referred to in Sections C3.12 (Protections for Panel Members and Others) and M2.13(a) (Other Matters) shall be entitled to enforce the respective rights referred to in those Sections; and

(b) the Approved Finance Party for each Communications Hub Finance Facility shall be entitled to exercise and/or enforce the following rights of the DCC in respect of the Communications Hub Finance Charges relating to that facility where a Communications Hub Finance Acceleration Event has occurred in respect of that Communications Hub Finance Facility and the Authority has determined that the DCC is unwilling or unable to do so:

(i) the right to calculate the amount of the Communications Hub Finance Charges arising as a result of that event (provided in such circumstances that the Approved Finance Party must demonstrate to the satisfaction of the Authority that the amount of the charges so calculated will in aggregate be no more than the amount contractually due and payable (but unpaid) by the DCC to the Approved Finance Party in respect of that event);

(ii) the right to invoice the Users in respect of the Communications Hub Finance Charges arising as a result of the Communications Hub Finance Acceleration Event (whether in the amount calculated by the DCC in accordance with this Code, or in the amount calculated by the Approved Finance Party and approved by the Authority under Section M11.5(b)); and/or

(iii) the right to enforce payment by the Users in accordance with this Code of the amount of Communications Hub Finance Charges invoiced in accordance with this Code,

and the payment of any amount by a User to an Approved Finance Party pursuant to this Section M11.5(b) shall satisfy that User's obligation to pay that amount to the DCC.

M11.6 Subject to Section M11.5, the Parties do not intend that any of the terms or conditions of this Code will be enforceable by a third party (whether by virtue of the Contracts (Rights of Third Parties) Act 1999 or otherwise).

M11.7 Notwithstanding that a person who is not a Party has the right to exercise and/or

enforce particular rights in accordance with Section M11.5, the Parties may vary or terminate this Code in accordance with its terms without requiring the consent of any such person.

Assignment and Sub-contracting

M11.8 Without prejudice to a Party's right to appoint agents to exercise that Party's rights, no Party may assign any of its rights under this Code without the prior written consent of the other Parties.

M11.9 Any Party may sub-contract or delegate the performance of any or all of its obligations under this Code to any appropriately qualified and experienced third party, but such Party shall at all times remain liable for the performance of such obligations (and for the acts and omissions of such third party, as if they were the Party's own). It is expressly acknowledged that the DCC has sub-contracted a number of its obligations under this Code to the DCC Service Providers.

Agency

M11.10 Nothing in this Code shall create, or be deemed to create, a partnership or joint venture or relationship of employer and employee or principal and agent between the Parties and no employee of one Party shall be deemed to be or have become an employee of another Party.

M11.11 No Party shall:

(a) pledge the credit of another Party;

(b) represent itself as being another Party, or an agent, partner, employee or representative of another Party; or

(c) hold itself out as having any power or authority to incur any obligation of any nature, express or implied, on behalf of another Party.

Derogations

M11.12 A Party that holds an Energy Licence shall not be obliged to comply with its

obligations under this Code to the extent to which such Party has the benefit of a derogation from the obligation to do so granted by the Authority under such Energy Licence.

Law and Jurisdiction

M11.13 This Code and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the laws of England and Wales.

M11.14 In relation to any dispute or claim arising out of or in connection with this Code (including in respect of non-contractual claims), each Party (subject to Section M7 (Dispute Resolution)) irrevocably agrees to submit to the exclusive jurisdiction of the courts of England and Wales and of Scotland. For the avoidance of doubt, the foregoing shall not limit a Party's right to enforce a judgment or order in any other jurisdiction.

SECCo

M11.15 The provisions of this Section M11 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

SECTION N: SMETS1 METERS

N1 DEFINITIONS FOR THIS SECTION N

N1.1 In this Section N, unless the context otherwise requires, the expressions in the left-hand column below shall have the meanings given to them in the right-hand column below:

Adoption	means, in respect of a Communications Contract, to novate (with or without amendment) some or all of the Supplier Party's rights and obligations under the contract (to the extent arising after the date of novation) to the DCC; and "**Adopt**", "**Adopting**" and "**Adopted**" shall be interpreted accordingly.
Adoption Criteria	means the non-exhaustive criteria (including those set out in Section N3.7) against which the DCC will analyse and report upon the feasibility and cost of Adopting a Communications Contract in order to facilitate the provision by the DCC of the Minimum SMETS1 Services in respect of the Eligible Meters that are the subject of that contract.
Communications Contract	means, in respect of an Energy Meter, the contract or contracts (or the relevant parts thereof) pursuant to which the Supplier Party has (or, will following installation, have) the right to receive communication services in respect of that Energy Meter.
Eligible Meter	means, in respect of each Supplier Party, an Energy Meter which is: (a) either a SMETS1 Meter or subject to an upgrade plan which will result in it being a

SMETS1 Meter prior to its Enrolment; and

(b) installed at premises (or planned to be installed at premises) for which that Supplier Party is an energy supplier.

Enrolment	means, in respect of a SMETS1 Meter, the establishment by the DCC of communications with the SMETS1 Meter such that the DCC can (on an ongoing basis) provide the SMETS1 Services in respect of the SMETS1 Meter (and the words "**Enrol**" and "**Enrolled**" will be interpreted accordingly).
Initial Enrolment	means the Enrolment of some or all of the Eligible Meters included within the scope of the Initial Enrolment Project Feasibility Report.
Initial Enrolment Code Amendments	has the meaning given to that expression in Section N3.1 (Overview of Initial Enrolment).
Initial Enrolment Project Feasibility Report	has the meaning given to that expression in Section N3.1 (Overview of Initial Enrolment).
Minimum SMETS1 Services	means those communication services described in Appendix F (Minimum Communication Services for SMETS1 Meters).
SMETS1 Eligible Products List	has the meaning given to that expression in Section N2.14 (SMETS1 Eligible Products List).
SMETS1 Meter	means an Energy Meter that has (as a minimum) the functional capability specified by and complies with the other requirements of the SMETS that was designated on 18 December 2012 and amended and restated on 31 March 2014 (but not any subsequent

	version of the SME Technical Specification).
SMETS1 Services	means those communication services described in Section N2.2 (SMETS1 Services).

N1.2 To the extent that Section A1.1 (Definitions) contains the same defined expressions as are set out in Section N1.1, the defined expressions in Section A1.1 shall not apply to this Section N.

N1.3 The expressions used in this Section N that are to have the meanings given in Section A1.1 (Definitions) and which have a meaning which relates directly or indirectly to the provision of Services in connection with Smart Metering Systems shall be interpreted by reference to the purposes of this Section N (including the purpose of establishing the feasibility, cost and means of providing the SMETS1 Services in connection with the SMETS1 Meters).

N2 SMETS1 ENROLMENT PROJECTS GENERALLY

Overview

N2.1 This Section N2 sets out certain matters which will apply to all projects to Enrol SMETS1 Meters, regardless of whether this is pursuant to the Initial Enrolment Project Feasibility Report or any subsequent Modification Proposal.

SMETS1 Services

N2.2 Upon Enrolment of any SMETS1 Meter, the communication services (the "**SMETS1 Services**") that the DCC provides in relation to those meters must include (as a minimum) the ability, for those Users identified as eligible to do so, to send Service Requests to those meters requesting the Minimum SMETS1 Services.

N2.3 The detail of the SMETS1 Services will be established in the amendments to this Code produced pursuant to the Initial Enrolment Project Feasibility Report or any subsequent Modification Proposal.

SMETS1 Compliance

N2.4 In respect of each Energy Meter that is to be Enrolled as a SMETS1 Meter, the Supplier Party that is Registered for the MPAN or MPRN to which the Energy Meter relates shall:

(a) ensure that such Energy Meter is a SMETS1 Meter at the time of its Enrolment; and

(b) ensure that testing has been undertaken which confirms that the Energy Meter is a SMETS1 Meter (and the Supplier Party shall make evidence of such testing available to the Authority or the Panel on request).

N2.5 Before seeking to have an Energy Meter Enrolled as a SMETS1 Meter, the Supplier Party seeking Enrolment must have provided the following confirmation to the DCC in respect of the relevant Device Model:

"[*Full legal name of Supplier Party*] hereby declares that [*device model*]:

(a) consists of an Electricity Meter or a Gas Meter and any associated or ancillary devices identified in;

(b) has the functional capability specified by; and

(c) complies with the minimum technical requirements of,

the SMETS that was designated by the Secretary of State on 18 December 2012 and amended and restated on 31 March 2014. Testing has been undertaken to confirm compliance and evidence of this will be made available to the Panel and the Authority on request.

signed by [*name and title*]

for and on behalf of [*Full legal name of Supplier Party]"*

N2.6 The DCC shall not Enrol an Energy Meter that is (or is purported to be) a SMETS1 Meter until the DCC has received the confirmation referred to in Section N2.5 in respect of that Energy Meter's Device Model from the Supplier Party requesting Enrolment.

N2.7 A Party which considers that an Energy Meter purported to be a SMETS1 Meter is not a SMETS1 Meter shall be entitled to raise a dispute under Section F3 (Panel Dispute Resolution Role). The DCC shall comply with any direction by the Panel to the DCC not to Enrol an Energy Meter which is the subject of such a dispute until such dispute is resolved or the Panel otherwise directs.

Testing

N2.8 Before Enrolling one or more SMETS1 Meters of a particular type, the DCC shall ensure that it has tested the DCC Systems and its processes to demonstrate that it is capable of discharging its obligations and exercising its rights under this Code (as amended pursuant to the Initial Enrolment Project Feasibility Report or any subsequent Modification Proposal) in respect of that type of SMETS1 Meter.

N2.9 In discharging its obligations under Section N2.8, the DCC must prepare and follow an approach to testing that is (to the extent that it is appropriate to do so given the

purpose for which the testing is being undertaken) consistent with the approach to testing set out in Section T (Testing During Transition). Where Section T has ceased to apply, this Section N2.9 shall be taken to refer to the provisions of Section T that applied immediately before it ceased to apply.

Security

N2.10 In producing the Initial Enrolment Project Feasibility Report or analysing and reporting on any subsequent Modification Proposal relating to the Enrolment of SMETS1 Meters, the DCC shall:

(a) prepare a risk assessment detailing the security risks associated with operating and using the SMETS1 Services;

(b) detail the measures (including Systems) proposed in order to ensure that the level of security risk to the DCC Total System, Enrolled Smart Metering Systems and/or User Systems will not be materially increased as a consequence of the provision of the SMETS1 Services; and

(c) prepare a risk treatment plan outlining the residual risks which exist once the measures referred to above have been taken.

N2.11 For the purposes of Section N2.10, the expressions Enrolled Smart Metering Systems, DCC Total System, and User Systems shall, when assessing the security risks that will apply as a consequence of the provision of the SMETS1 Services in respect of SMETS1 Meters, be interpreted so as to also include (respectively) those SMETS1 Meters and all additional Systems of the DCC and Users that would be used in relation to those SMETS1 Services.

N2.12 In discharging its obligations under Section N2.10, the DCC shall consult with the Security Sub-Committee, and shall document the extent to which the views of the Security Sub-Committee have been taken into account.

Data Privacy

N2.13 Any amendment to the Code to facilitate Enrolment of SMETS1 Meters, whether pursuant to the Initial Enrolment Project Feasibility Report or any subsequent

Modification Proposal, shall include provisions such that Section I (Data Privacy), is (where necessary) amended to provide for an equivalent privacy treatment of Data and Service Requests as is provided for in respect of Smart Metering Systems.

SMETS1 Eligible Products List

N2.14 The DCC shall establish, maintain and publish on the DCC Website a list (the "**SMETS1 Eligible Products List**") which lists the Device Models of SMETS1 Meters which Supplier Parties are entitled to Enrol (as a result of the amendments made to this Code pursuant to the Initial Enrolment Project Feasibility Report or any subsequent Modification Proposal). The DCC shall not be obliged to publish such a list until any such Device Models exist.

N2.15 The SMETS1 Eligible Products list must identify the following for each Device Model of SMETS1 Meter:

(a) manufacturer, model and hardware version;

(b) firmware version (number or ID); and

(c) the effective date of the amendment to this Code which enabled SMETS1 Meters of that Device Model to be Enrolled.

N2.16 The DCC shall notify the Panel and each other Party on making any amendment to the SMETS1 Eligible Products List.

N3 INITIAL ENROLMENT

Overview of Initial Enrolment

N3.1 This Section N3 together with Sections N4 and N5 sets out the process by which the DCC will:

(a) analyse, evaluate and report (the "**Initial Enrolment Project Feasibility Report**") to the Secretary of State regarding the feasibility and cost of the options for Initial Enrolment; and

(b) prepare one or more sets of proposed amendments to this Code (the "**Initial Enrolment Code Amendments**") designed to deliver Initial Enrolment.

N3.2 The DCC shall comply with the Secretary of State's directions from time to time regarding:

(a) the scope of the Initial Enrolment Project Feasibility Report;

(b) the scope and number of the Initial Enrolment Code Amendments to be prepared; and

(c) the timing and process to be followed by the DCC in relation to the production of the Initial Enrolment Project Feasibility Report and the Initial Enrolment Code Amendments.

DCC's Invitation

N3.3 Where, and by such date as, the Secretary of State may direct for the purposes of this Section N3.3, the DCC shall send an invitation to each Supplier Party seeking details of the Energy Meters of that Supplier Party which the Supplier Party wishes to be included within the scope of the Initial Enrolment Project Feasibility Report.

N3.4 Each Supplier Party undertakes that it shall not propose Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report unless those Energy Meters are Eligible Meters, and shall confirm to the DCC that the Energy Meters that it proposes are Eligible Meters. The DCC shall not be obliged to determine whether the Energy Meters proposed by each Supplier Party are Eligible

Meters, and shall rely upon the confirmation provided by each Supplier Party.

N3.5 The DCC shall provide a copy of its invitation pursuant to Section N3.3 to the Secretary of State, the Authority and the Panel, and shall arrange for its publication on the DCC Website.

N3.6 The DCC's invitation pursuant to Section N3.3 shall specify:

(a) the reasonable date by which Supplier Parties must respond in order for their Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report;

(b) the reasonable format in which Supplier Parties must respond in order for their Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report;

(c) any reasonable information which Supplier Parties must provide in order for their Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report (which will include such details as the DCC shall specify regarding the Communications Contracts relating to those Energy Meters); and

(d) the Adoption Criteria.

N3.7 The Adoption Criteria specified by the DCC must include reference to Communications Contract provisions relating to the following concepts:

(a) novation;

(b) termination;

(c) liability;

(d) exclusivity and restrictions on competing activities;

(e) data ownership and security;

(f) confidentiality; and

(g) disaster recovery, business continuity and incident management.

N3.8 The DCC must respond in a timely manner to reasonable clarification requests from Supplier Parties regarding the DCC's invitation pursuant to Section N3.3, and any further information requests made by the DCC pursuant to this Section N3.

Suppliers' Response

N3.9 No Supplier Party is obliged to propose Energy Meters to be included within the scope of the Initial Enrolment Project Feasibility Report.

N3.10 Each Supplier Party that wishes to propose any or all of its Energy Meters for inclusion within the scope of the Initial Enrolment Project Feasibility Report must provide the DCC with the information in respect of those Energy Meters required by the DCC pursuant to this Section N3 by the date and in the format required by the DCC pursuant to this Section N3.

N3.11 Following receipt of each response from a Supplier Party pursuant to this Section N3, the DCC shall review the response to establish whether it complies with the requirements of this Section N3. Where a response is incomplete or the DCC reasonably requires supplementary information in respect of a response, the DCC may request that further information is provided within a reasonable period. The DCC must request further or supplementary information where it considers that the initial information provided by a Supplier Party is not sufficient to enable the DCC to include the Supplier Party's Energy Meters within the scope of the Initial Enrolment Project Feasibility Report.

Inclusion of Meters in Scope of Project

N3.12 The Energy Meters of a Supplier Party shall only be included within the scope of the Initial Enrolment Project Feasibility Report where the Supplier Party has provided all of the information in respect of those Energy Meters required by the DCC pursuant to this Section N3 by the date and in the format required by the DCC in accordance with this Section N3.

N3.13 In respect of each Energy Meter put forward by a Supplier Party, the DCC shall notify

that Supplier Party whether the DCC considers that Energy Meter to be within (or outside) the scope of the Initial Enrolment Project Feasibility Report (determined as described in Section N3.12).

Disputes

N3.14 Without prejudice to Section N2.7 (SMETS1 Compliance), where:

(a) the DCC requests information from a Supplier Party pursuant to this Section N3, and the Supplier Party disputes whether that information has been requested in accordance with this Section N3; or

(b) a Supplier Party disagrees with the DCC's notification that some or all of the Supplier Party's Energy Meters are outside the scope of the Initial Enrolment Project Feasibility Report,

then the Supplier Party may refer the matter to the Secretary of State (whose decision shall be final and binding for the purposes of this Code).

N4 INITIAL ENROLMENT PROJECT FEASIBILITY REPORT

Analysis

N4.1 The DCC shall analyse the information received from Supplier Parties pursuant to Section N3, evaluate the options for Initial Enrolment that the DCC considers are reasonable, and report to the Secretary of State in the Initial Enrolment Project Feasibility Report on the feasibility and estimated cost of each option and the manner in which it would be delivered.

Timetable

N4.2 As soon as reasonably practicable following receipt of the relevant information from Supplier Parties pursuant to Section N3, the DCC shall publish on the DCC Website its proposed timetable for undertaking the steps required under this Section N4.

Report

N4.3 The DCC shall include within the Initial Enrolment Project Feasibility Report the DCC's analysis regarding the options for the Enrolment of all the Eligible Meters which were included within the scope of the Initial Enrolment Project Feasibility Report. Where the Enrolment of one or more subsets of such Eligible Meters would differ materially from the Enrolment of all of such Eligible Meters (in terms of risk, timescales and/or cost), then the DCC shall include its analysis for that subset (as well as for all of them).

N4.4 The DCC shall include within the Initial Enrolment Project Feasibility Report the DCC's analysis regarding the following matters in respect of the Enrolment of all (and, where applicable in accordance with Section N4.3, each subset referred to in that Section) of the Eligible Meters which were included within the scope of the Initial Enrolment Project Feasibility Report:

(a) the timeframe and process for the Enrolment of the Eligible Meters;

(b) its assessment of the Communications Contracts against the Adoption Criteria, and of whether some or all of the Communications Contracts should be Adopted, and of whether those that are to be Adopted should be amended or

consolidated following their Adoption;

(c) any amendments that would be required to existing DCC Service Provider Contracts in order to deliver Initial Enrolment;

(d) the establishment of any new contracts which the DCC would require in order to deliver Initial Enrolment;

(e) the means by which the DCC will provide SMETS1 Services in respect of the Eligible Meters such that (insofar as reasonably practicable) Users may send Service Requests and receive Service Responses in respect of those communication services via the DCC User Interface (such that the format of communications over the DCC User Interface in relation to each SMETS1 Service is the same as that for existing equivalent DCC User Interface Services);

(f) where it better facilitates achievement of the SEC Objectives, the provision by the DCC to Users of the SMETS1 Services in respect of the Eligible Meters by another means than that referred to in (e) above;

(g) to the extent that they can be offered without a material increase in cost, risk or timescale, any rights for Parties also to Enrol SMETS1 Meters which were not included within the scope of the Initial Enrolment Project Feasibility Report;

(h) options for amendment of the Minimum SMETS1 Services such that DCC can provide additional Services to Parties which are equivalent to the DCC User Interface Services;

(i) options for provision by DCC to Users of a service for Eligible Meters to be commissioned first in the DCC (in addition to Enrolment post-commissioning);

(j) any Enabling Services that the DCC considers necessary to support Enrolment (including the equivalent of Testing Services);

(k) the development and testing of the Systems via which the Enrolment of Eligible Meters and provision of SMETS1 Services will be delivered, in

compliance with the requirements of Section N2.8 (Testing);

(l) the measures proposed in order to ensure that the SMETS1 Services are delivered in a manner that will not materially increase the security risk, in compliance with the requirements of Section N2.10 (Security);

(m) an assessment of which Supplier Parties are (in accordance with the Charging Objectives) likely to pay a premium and its reasonable estimate of the amount of those premiums in respect of Enrolled SMETS1 Meters (over and above the Charges for Smart Metering Systems); and

(n) other matters required to be considered in compliance with the requirements of Section N2 (SMETS1 Enrolment Projects Generally).

Consultation

N4.5 Before submitting the Initial Enrolment Project Feasibility Report to the Secretary of State, the DCC shall produce a draft report and consult with the Panel, the Parties and other interested persons concerning the content of such draft. The DCC shall ensure that a reasonable period of time is allowed for consultation responses to be made, which period may not be less than two months.

N4.6 On submitting the Initial Enrolment Project Feasibility Report to the Secretary of State, the DCC shall also provide the Secretary of State with:

(a) copies of all consultation responses received;

(b) a commentary identifying where and the extent to which the DCC has amended its report to take into account any comments, representations or objections raised as part of such consultation responses; and

(c) where the DCC has not amended the report to address any comments or representations of objections raised as part of such consultation responses, the DCC's reasons for not doing so.

Inclusion or Exclusion of Meters from Scope of Report

N4.7 Before submitting the Initial Enrolment Project Feasibility Report to the Secretary of

State, the DCC shall (subject to Section N4.11) publish a final draft of the report in the form it intends to submit to the Secretary of State (subject only to Section N4.9).

N4.8 On publishing the draft report pursuant to Section N4.7, the DCC shall notify the Supplier Parties that they each have two weeks to notify the DCC if they wish to include additional Energy Meters, or exclude some or all of their Energy Meters, from some or all of the options within the scope of the Initial Enrolment Project Feasibility Report. If no response is received from a Supplier Party within that period, the DCC shall assume that all of the Energy Meters previously included within the scope of the report remain within scope.

N4.9 The DCC shall include or exclude (as applicable) from the scope of the Initial Enrolment Project Feasibility Report those Energy Meters notified in accordance with Section N4.8, and:

(a) where the DCC considers that the inclusion or exclusion of those Energy Meters has a material impact on the Initial Enrolment Project Feasibility Report, then the DCC shall produce a further draft of the report, and undertake a further consultation in accordance with Section N4.5 (but without repeating the steps at Section N4.7 and N4.8); or

(b) where the DCC considers that the inclusion or exclusion of those Energy Meters does not have a material impact on the Initial Enrolment Project Feasibility Report, then the DCC shall amend the report only insofar as necessary to include or exclude those Energy Meters from the scope of the report and submit the report to the Secretary of State.

Redaction for Reasons of Security

N4.10 Before consulting on or publishing the draft report pursuant to Section N4.5 or N4.7, the DCC shall provide to the Panel and (on request) the Secretary of State:

(a) a copy of the draft report; and

(b) where relevant, a list of sections of the report which the DCC considers should be redacted prior to publication in order to avoid a risk of Compromise to the

DCC Total System and/or User Systems .

N4.11 The DCC shall only consult on or publish its draft report pursuant to Section N4.5 or N4.7 after it has redacted those sections of the report which it is directed to redact by the Panel where the Panel considers that those sections contain information which may pose a risk of Compromise to the DCC Total System and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction).

N5 INITIAL ENROLMENT CODE AMENDMENTS

Amendments

N5.1 Where directed to do so by the Secretary of State, the DCC shall prepare Initial Enrolment Code Amendments in respect of one or more options for Initial Enrolment in respect of some or all of the Eligible Meters included within the scope of the Initial Enrolment Project Feasibility Report (as directed by the Secretary of State).

N5.2 Such amendments shall include those necessary to enable the Enrolment of the relevant SMETS1 Meters, the request and receipt of SMETS1 Services in respect of those SMETS1 Meters, and the calculation of the Charges for the same in accordance with the Charging Objectives.

N5.3 Such amendments shall be prepared in a format capable of being laid before Parliament by the Secretary of State pursuant to section 88 of the Energy Act 2008.

Consultation

N5.4 Before submitting the Initial Enrolment Code Amendments to the Secretary of State pursuant to Section N5.1, the DCC shall produce draft amendments and consult with the Authority, the Panel, the Parties and other interested persons concerning such draft. The DCC shall ensure that a reasonable period of time is allowed for consultation responses to be made, which period may not be less than two months.

N5.5 On submitting the Initial Enrolment Code Amendments to the Secretary of State, the DCC shall also provide the Secretary of State with:

(a) copies of all consultation responses received;

(b) a commentary identifying where and the extent to which the DCC has amended its draft to take into account any comments, representations or objections raised as part of such consultation responses; and

(c) where the DCC has not amended its draft to address any comments or representations of objections raised as part of such consultation responses, the DCC's reasons for not doing so.

SECTION T – TESTING DURING TRANSITION

T1 DEVICE SELECTION METHODOLOGY

Overview

T1.1 The Device Selection Methodology is the methodology for determining the Devices that are to be used by the DCC for the purposes of Systems Integration Testing, Interface Testing and User Entry Process Tests.

Use of Devices

T1.2 Systems Integration Testing, Interface Testing and User Entry Process Tests are to be undertaken using (to the extent reasonably practicable) actual Devices (rather than Test Stubs or other alternative arrangements).

Device Selection Methodology

T1.3 The DCC shall develop, publish (including on the DCC Website) and comply with a methodology (the "**Device Selection Methodology**") concerning the selection and de-selection of Devices for the purposes of Systems Integration Testing, Interface Testing and User Entry Process Tests. The DCC shall consult with the other Parties and Manufacturers prior to finalising the Device Selection Methodology. The Device Selection Methodology shall include provision for the DCC to:

(a) (save for Communications Hubs) select as many different Device Models as the DCC considers appropriate in order to demonstrate that the Testing Objectives have been achieved; provided that, when the DCC first selects Device Models, the DCC shall select at least the first two Gas Meter Device Models and at least the first two Electricity Meter Device Models offered in accordance with the Device Selection Methodology that meet the criteria set out in Sections T1.4 and T1.6 (as varied by Section T1.5);

(b) (save for Communications Hubs) select the Device Models in accordance with the selection criteria described in Sections T1.4 and T1.6 (as varied by Section T1.5);

(c) (save for Communications Hubs) publish an invitation to submit Device Models

for selection (such publication to be in a manner likely to bring it to the attention of Parties and Manufacturers, including publication on the DCC Website), such invitation to require Devices to be offered for use on reasonable terms specified by the DCC and from a certain date;

(d) de-select a Device Model (for the purposes of the then current phase of testing and any future phases of testing pursuant to this Section T) if that Device Model is subsequently found to not comply with the criteria set out in Section T1.4(a), with respect to which the methodology shall describe the process to be followed by the DCC in such circumstances and provide for an appeal by a Party or a Manufacturer to the Panel. The Panel's decision on such matter may then be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) for final determination of disputes regarding whether or not a Device Model does comply with the requirements of Section T1.4(a); and

(e) select Communications Hubs comprising Devices of the Device Models that the DCC first proposes to make available to Supplier Parties pursuant to the Communications Hub Services (which Device Models need not, at the start of Systems Integration Testing, have CPA Certificates or (where the Secretary of State so directs) a ZigBee Alliance Assurance Certificate).

T1.4 In selecting Devices (other than those comprising Communications Hubs), the DCC shall apply the following selection criteria:

(a) that the Device Models selected are SMETS compliant, provided that they need not (where the Secretary of State so directs) have a ZigBee Alliance Assurance Certificate or a DLMS Certificate and need not have a CPA Certificate until CPA Certificates are generally available for the relevant Physical Device Type (and the DCC need only switch to a Device Model with those Assurance Certificates where it is reasonably practicable for it to do so, having regard to the timely achievement of the Testing Objectives);

(b) that Gas Meter Device Models and Electricity Meter Device Models are selected so that, in respect of each Communications Hub Device Model that the DCC first proposes to make available pursuant to the Communications Hub

Services, there are at least two Gas Meter Device Models and at least two Electricity Meter Device Models of a Manufacturer which is not the Manufacturer (or an Affiliate of the Manufacturer) of that Communications Hub Device Model; and

(c) that there will be sufficient Devices available for Systems Integration Testing, Interface Testing and User Entry Process Tests.

T1.5 Where the DCC is not able to select Devices that meet all the criteria set out in Section T1.4, it may relax the requirements in accordance with the Device Selection Methodology.

T1.6 The Device Selection Methodology must also include:

(a) in addition to the selection criteria set out in Section T1.4, any other reasonable criteria that the DCC considers appropriate and that are consistent with those set out in Section T1.4;

(b) an explanation of the level of assurance the DCC needs regarding the achievement of the Testing Objectives and of how the Device Selection Methodology will ensure that level of assurance; and

(c) any amendments to the process referred to in Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) for resolving Testing Issues which are to be applied by the DCC in respect of Testing Issues concerning Devices that arise during activities undertaken pursuant to this Section T.

Appeal of Methodology

T1.7 Within the 14 days after publication of the Device Selection Methodology under Section T1.3, any person that is a Party and/or a Manufacturer may refer the methodology to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the methodology meets the requirements of this Section T1 (which determination shall be final and binding for the purposes of this Code).

T1.8 Following a referral in accordance with Section T1.7, the DCC shall comply with any directions of the person making the determination thereunder to reconsider and/or

amend the Device Selection Methodology. The DCC shall republish (including on the DCC Website) the methodology as so amended and the provisions of Section T1.7 and this Section T1.8 shall apply to any such amended methodology.

Compliance with Methodology

T1.9 Following its decision on which Device Models (or alternative arrangements) to select pursuant to the Device Selection Methodology, the DCC shall publish its decision on the DCC Website. The DCC shall not publish details of the Device Models (if any) which were proposed for selection but not selected. The DCC shall notify the Secretary of State, the Authority and the person which proposed any Device Models which were not selected of the DCC's decision (together with its reasons for selecting the Device Models (or other arrangements) that were selected, and for not selecting that person's proposed Device Models).

T1.10 Where any Party and/or Manufacturer believes that the DCC has not complied with the Device Selection Methodology as published from time to time in accordance with this Section T1, then such person may refer the matter to be determined by the Panel. The Panel's decision on such matter may be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code.

T2 SYSTEMS INTEGRATION TESTING

Overview

T2.1 Systems Integration Testing tests the capability of the DCC and the component parts of the DCC Systems together with the Communications Hubs selected pursuant to Section T1 to interoperate with each other and with the RDP Systems.

SIT Objective

T2.2 The objective of Systems Integration Testing (the "**SIT Objective**") is to demonstrate that the DCC and the component parts of the DCC Systems together with the Communications Hubs selected pursuant to Section T1 interoperate with each other and with the RDP Systems to the extent necessary in order that:

(a) the DCC is capable of complying with its obligations under Sections E (Registration Data), G (Security) and H (DCC Services); and

(b) the Registration Data Providers are capable of complying with the obligations under Section E (Registration Data) with which the Network Parties are obliged to procure that the Registration Data Providers comply,

in each case at levels of activity commensurate with the relevant Volume Scenarios.

T2.3 For the purposes of Section T2.2, the Sections referred to in that Section shall be construed by reference to:

(a) the decision or consultation document concerning the intended future content of those Sections most recently published by the Secretary of State prior to [DATE~~14 December 2015~~][1] (regardless of whether the content of those documents has yet been incorporated into this Code~~,~~ or whether those Sections ~~are stated to not~~ yet have effect~~apply under Section X (Transition)~~, but taking into account any variations to this Code pursuant to Section X (Transition) that apply (or are due to apply on the Section or a relevant Subsidiary Document coming into effect) and that will continue to apply on Communication Services first becoming available); and

[1] This date is to reflect the date on which the modification to this section is laid before Parliament.

(b) to the extent not inconsistent with any document referred to in (a), any document regarding technical or procedural requirements which support those Sections which is published from time to time by the Secretary of State for the purposes of this Section T2.3.

T2.4 Systems Integration Testing is to be undertaken on a Region-by-Region basis and an RDP-System-by-RDP-System basis; such that the SIT Objective is to be achieved in respect of each Region and each RDP System separately.

SIT Approach Document

T2.5 The DCC shall develop a document (the "**SIT Approach Document**") which sets out:

(a) the reasonable entry criteria to be satisfied with respect to each Registration Data Provider prior to commencement of Systems Integration Testing in respect of that Registration Data Provider;

(b) the manner in which Systems Integration Testing is to be undertaken, including the respective obligations of the DCC, and each Registration Data Provider and the Volume Scenarios to be used;

(c) a reasonable timetable for undertaking and completing Systems Integration Testing;

(d) the frequency and content of progress reports concerning Systems Integration Testing to be provided by the DCC to the Panel (which the Panel shall make available to the Secretary of State, the Authority and Testing Participants), which reports must include details of Testing Issues identified and resolved and of any problems and solutions encountered with respect to Devices (the details of such Testing Issues to be anonymised and redacted as required in accordance with Section H14.44 (General: Testing Issue Resolution Process));

(e) (to the extent it is not reasonably practicable to use actual Devices) details of the alternative arrangements (which may include Test Stubs) to be used in their place (together with an explanation of how such arrangements will provide sufficient assurance that the SIT Objective has been met), in which case there must also be a process describing whether and how to switch to the use of actual

Devices as they become available;

(f) where a Device Model is de-selected pursuant to the Device Selection Methodology, the process for switching to an alternate Device Model where practicable, or otherwise to Tests Stubs or an alternative arrangement;

(g) a Good Industry Practice methodology for determining whether the SIT Objective has been achieved in respect of each Region and each RDP System, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria; provided that one such exit criteria for each Region must include the successful use in that Region of each Communications Hub Device Model that the DCC first proposes to make available in that Region (save that such Communications Hub Device Models need not have CPA Certificates and need not (where the Secretary of State so directs) have a ZigBee Alliance Assurance Certificate);

(h) that the DCC will produce a report where the DCC considers that the exit criteria referred to in (g) above have been achieved for a Region or an RDP System (providing evidence of such achievement in such report), having consulted with each Registration Data Provider in relation to the exit criteria applicable to that Registration Data Provider; and

(i) how an auditor (that is sufficiently independent of the DCC, the DCC Service Providers and the Registration Data Providers) will be selected, and how such auditor will monitor the matters being tested pursuant to Systems Integration Testing, and confirm that the exit criteria referred to in (g) above have been achieved for a Region or an RDP System (such independent auditor to be appointed by the DCC on terms consistent with Good Industry Practice).

Approval of SIT Approach Document

T2.6 The DCC shall submit the SIT Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T2.

T2.7 The DCC shall not submit the SIT Approach Document to the Panel under Section T2.6 until after the DCC has first published the Device Selection Methodology.

T2.8 Before submitting the SIT Approach Document to the Panel, the DCC shall consult with the Registration Data Providers regarding the SIT Approach Document. When submitting the SIT Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the Registration Data Providers. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T2.9 Where the Panel decides not to approve the SIT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the Registration Data Providers giving the reasons why it considers that it is not fit for the purposes envisaged in this Section T2. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the Registration Data Providers; and

(c) re-submit the document to the Panel for approval and comply with Section T2.8 (following which this Section T2.9 or Section T2.10 shall apply).

T2.10 Where the Panel decides to approve the SIT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the Registration Data Providers. In such circumstances, the DCC and each Registration Data Provider shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the SIT Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T2;

(b) is not fit for the purposes envisaged by this Section T2, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T2 and should be revised and re-submitted by the DCC in accordance with Section T2.9,

(and any such determination shall be final and binding for the purposes of this Code).

Commencement of Systems Integration Testing

T2.11 Subject to Section T2.12, once the SIT Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T2.10(b)), the DCC shall publish the approved document on the DCC Website and give at least 3 months' (or such shorter period as the Secretary of State may direct) notice to the Registration Data Providers of the date on which Systems Integration Testing is to commence. Where directed to do so by the Secretary of State, the DCC shall determine a revised commencement date for Systems Integration Testing (provided that the DCC shall first consult on such date with such persons as the Secretary of State may specify in such direction), and shall (where specified by the Secretary of State in such direction) make consequential revisions to the SIT Approach Document (which date (and, where relevant, revisions) must be published at least 3 months (or such shorter period as the Secretary of State may direct) in advance of the revised date on which Systems Integration Testing is to commence).

T2.12 The DCC shall not publish the SIT Approach Document and give notice under Section T2.11 where the Panel's decision has been appealed under Section T2.10 (pending approval of the document thereunder or revision in accordance with a determination made under Section T2.10(b)), save that where:

(a) the Panel's approval of the SIT Approach Document is appealed by one or more Registration Data Providers, the DCC shall nevertheless publish the document and give notice under Section T2.11 insofar as the document relates to the other Registration Data Providers; and/or

(b) the Panel's approval of the SIT Approach Document is appealed by one or more Registration Data Providers or the DCC, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay notice under Section T2.11, in which case the DCC shall publish the document and give notice under Section T2.11 (noting the appeal).

T2.13 Prior to the commencement of Systems Integration Testing, the DCC shall assess whether or not each Registration Data Provider meets the entry criteria referred to in Section T2.5(a), and report to the Registration Data Provider and the Panel on the same. Each Network Party shall ensure that its Registration Data Provider:

(a) cooperates with the DCC in its assessment of whether the Registration Data Provider meets the entry criteria referred to in Section T2.5(a);

(b) takes all reasonable steps to meet those entry criteria by the date required in accordance with the SIT Approach Document; and

(c) notifies the Panel and the DCC as soon as reasonably practicable if the Registration Data Provider considers that it will not meet those criteria by that date.

T2.14 Systems Integration Testing in respect of each Registration Data Provider shall only commence once the Registration Data Provider meets the entry criteria referred to in Section T2.5(a). Any disagreement between the DCC and a Registration Data Provider as to whether the Registration Data Provider has met such entry criteria shall be determined by the Panel, provided that such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to the Registration Data Provider. The Panel's decision on such matter may (within 14 days after the Panel's decision) be appealed by the DCC or the affected Registration Data Provider to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code.

Systems Integration Testing

T2.15 The DCC shall comply with its obligations under the approved SIT Approach Document. The DCC shall take reasonable steps~~use its reasonable endeavours~~ to ensure that Systems Integration Testing is completed as soon as it is reasonably practicable to do so.

T2.16 Each Network Party shall ensure that its Registration Data Provider complies with its obligations under the approved SIT Approach Document.

T2.17 Where requested by the DCC and/or a Registration Data Provider, each Party shall take all reasonable steps to do all such things as are within its power and necessary or expedient in order to facilitate achievement of the SIT Objective.

T2.18 Where the DCC wishes to make amendments to the SIT Approach Document (other

than consequential revisions in accordance with Section T2.11), the DCC shall consult with the Registration Data Providers regarding those amendments and submit those amendments to the Panel (in accordance with Section T2.8) for approval (following which Sections T2.9 to T2.12 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Sections T2.11 and T2.12 to giving notice were not included).

Completion of Systems Integration Testing

T2.19 Subject to Section T2.20, Systems Integration Testing shall end in respect of each Region or RDP System on the date notified as the end of Systems Integration Testing for that Region or RDP System by the DCC to the Secretary of State, the Authority, the Panel, the Parties and the Registration Data Providers.

T2.20 The DCC shall not notify the end of Systems Integration Testing in respect of each Region or RDP System before the following reports have been produced in respect of that Region or RDP System:

(a) the DCC's report in accordance with the SIT Approach Document demonstrating that the exit criteria have been met in respect of that Region or RDP System (as envisaged by Section T2.5(h)); and

(b) the independent auditor's report to the DCC in accordance with the SIT Approach Document confirming that the exit criteria have been met in respect of that Region or RDP System (as envisaged by Section T2.5(i)).

T2.21 On notifying the end of Systems Integration Testing for one or more Regions or RDP Systems, the DCC shall provide to the Authority and the Panel and (on request) to the Secretary of State:

(a) copies of the reports referred to in Section T2.20; and

(b) where relevant, a list of sections of the report or reports which the DCC considers should be redacted prior to circulation of the reports to the Parties, Registration Data Providers or Testing Participants where the DCC considers that those sections contain information which may pose a risk of Compromise to the DCC Total System or RDP Systems.

T2.22 Once directed to do so by the Panel, the DCC shall make copies of the reports referred to in Section T2.20 available to the Parties, the Registration Data Providers and the Testing Participants. Prior to making such copies available, the DCC shall redact those sections of the reports which it is directed to redact by the Panel where the Panel considers that those sections contain information which may pose a risk of Compromise to the DCC Total System or RDP Systems (which sections may or may not include those sections which the DCC proposed for redaction).

Testing Issues

T2.23 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of Systems Integration Testing. Each Registration Data Provider shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of Systems Integration Testing.

T2.24 During Systems Integration Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

Additional Systems Integration Testing

T2.25 On each occasion that the Secretary of State so directs for the purpose of this Section T2.25, the DCC shall undertake testing against the SIT Objective in respect of such Services that have not previously been the subject of testing under this Section T2 as the Secretary of State may direct (each such round of testing being "**Additional SIT**").

T2.26 The purpose of each round of Additional SIT shall be to demonstrate the SIT Objective as described in Sections T2.2 and T2.3, but subject to the following variations (the SIT Objective as so varied being the "**Additional SIT Objective**"):

(a) the only variations pursuant to Section X (Transition) that will be taken into account in interpreting the relevant Sections are those that will continue to apply following commencement of the provision of the Services that are the subject of that round of Additional SIT; and

(b) the Additional SIT Objective shall not apply by reference to the document

published from time to time by the Secretary of State for the purpose of Section T2.3(b), but instead by reference to the document published from time to time by the Secretary of State for the purposes of that Additional SIT.

T2.27 The provisions of this Section T2 shall apply to each round of Additional SIT, subject to the following:

(a) all references in this Section T2 to "Systems Integration Testing" shall be read as references to "the relevant round of Additional SIT";

(b) Sections T2.25 and T2.26 shall apply in place of Sections T2.2 and T2.3; for which purpose it is acknowledged that some of the capability and interoperability to be demonstrated via Additional SIT will already have been demonstrated via previous testing undertaken pursuant to this Section T (and further testing of such capability or interoperability shall not be required to the extent that it has already been sufficiently proven for the purposes of the Additional SIT Objective as part of such earlier testing);

(c) the Additional SIT shall be undertaken only in respect of the Region or Regions and the RDP System or RDP Systems directed by the Secretary of State;

(d) the SIT Approach Document shall apply to the Additional SIT (without prejudice to the DCC's ability to make changes to the SIT Approach Document in accordance with this Section T2);

(e) (unless otherwise directed by the Secretary of State) the Registration Data Providers shall not be obliged to participate in the Additional SIT and the entry and exit criteria relating to RDP Systems shall not apply (and, accordingly, Registration Data Providers need not be consulted regarding, and shall have no appeal right in respect of, changes to the SIT Approach Document that relate only to Additional SIT in which the Registration Data Providers are not participating);

(f) no period of notice need be given by the DCC in advance of commencement of Additional SIT (unless otherwise directed by the Secretary of State);

(g) the Device Models to be used for Additional SIT are those selected pursuant to

the previous phase of testing pursuant to this Section T.

T3 INTERFACE TESTING

Overview

T3.1 Interface Testing tests the capability of the DCC and the DCC Systems together with the Communications Hubs selected pursuant to Section T1 to interoperate with User Systems.

Interface Testing Objective

T3.2 The objective of Interface Testing (the "**Interface Testing Objective**") is to demonstrate that the DCC and the DCC Systems together with the Communications Hubs selected pursuant to Section T1 interoperate with User Systems to the extent necessary in order that the DCC is capable of complying with its obligations under Sections E (Registration Data), G (Security) and H (DCC Services) (in each case) at levels of activity commensurate with the relevant Volume Scenarios.

T3.3 For the purposes of Section T3.2, the Sections referred to in that Section shall be construed by reference to:

(a) the decision or consultation document concerning the intended future content of those Sections most recently published by the Secretary of State prior to [DATE~~14 December 2015~~][2] (regardless of whether the content of those documents has yet been incorporated into this Code~~,~~ or whether those Sections ~~are stated to not~~ yet have effect~~apply under Section X (Transition)~~, but taking into account any variations to this Code pursuant to Section X (Transition) that apply (or are due to apply on the Section or a relevant Subsidiary Document coming into effect) and that will continue to apply on Communication Services first becoming available); and

(b) to the extent not inconsistent with any document referred to in (a), any document regarding technical or procedural requirements which support those Sections which is published from time to time by the Secretary of State for the purposes of this Section T3.3.

[2] This date is to reflect the date on which the modification to this section is laid before Parliament.

T3.4 Interface Testing is to be undertaken on a Region-by-Region basis; such that the Interface Testing Objective is to be demonstrated in respect of each Region separately. Interface Testing for a Region cannot be completed until Systems Integration Testing has been completed for that Region. For the avoidance of doubt, Interface Testing cannot be completed until Systems Integration Testing has been completed for each and every Region and RDP System.

T3.5 During Interface Testing, Parties who wish to do so, and who are ready to do so in accordance with the entry criteria for the User Entry Process Tests, shall be able to undertake the User Entry Process Tests (pursuant to Section H14 (Testing Services)).

Overlapping Provision of Systems Integration Testing and Interface Testing

T3.6 Prior to the start of Interface Testing, the DCC may propose to the Secretary of State, having regard to the overriding objective of completing Interface Testing in a timely manner, that Interface Testing should be commenced from some point during Systems Integration Testing for any or all Regions. The DCC's proposal must set out its analysis of the benefits and risks of doing so. Prior to submitting its proposal to the Secretary of State, the DCC shall consult with the other Parties regarding the proposal. The DCC shall also submit copies of the consultation responses received from Parties. Where it has submitted the proposal to the Secretary of State, the DCC shall publish the proposal and such consultation responses (to the extent that they are not marked confidential) on the DCC Website.

T3.7 Where the Secretary of State agrees with the DCC's recommendation pursuant to Section T3.6, then Interface Testing shall commence from the time recommended for the Regions included in the recommendation (notwithstanding anything to the contrary in the Interface Testing Approach Document or the SIT Approach Document).

Interface Testing Approach Document

T3.8 The DCC shall develop a document (the "**Interface Testing Approach Document**") which sets out:

(a) the reasonable entry criteria to be satisfied by the DCC with respect to the DCC Systems and the Communications Hubs selected pursuant to Section T1, and to be met by the Registration Data Providers with respect to the RDP Systems

prior to commencement of Interface Testing in each Region;

(b) the entry criteria to be met by the Parties prior to their commencing the User Entry Process Tests (which criteria shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of Interface Testing);

(c) the manner in which Interface Testing is to be undertaken, including the respective obligations of the DCC, each other Party and each Registration Data Provider and the Volume Scenarios to be used;

(d) a reasonable timetable for undertaking and completing Interface Testing;

(e) the frequency and content of progress reports concerning Interface Testing to be provided by the DCC to the Panel (which the Panel shall make available to the Secretary of State, the Authority and Testing Participants), which reports must include details of Testing Issues identified and resolved and of any problems and solutions encountered with respect to Devices (the details of such Testing Issues to be anonymised and redacted as required in accordance with Section H14.44 (General: Testing Issue Resolution Process);

(f) (to the extent it is not reasonably practicable to use actual Devices) details of the alternative arrangements (which may include Test Stubs) to be used in their place (together with an explanation of how such arrangements will provide sufficient assurance that the Interface Testing Objective has been met), in which case there must also be a process describing whether and how to switch to the use of actual Devices as they become available;

(g) where a Device Model is de-selected pursuant to the Device Selection Methodology, the process for switching to an alternate Device Model where practicable, or otherwise to Tests Stubs or an alternative arrangement;

(h) the process by which the DCC will facilitate the Parties undertaking and completing the User Entry Process Tests (which process shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of Interface Testing);

(i) how, to the extent it is reasonably practicable to do so, the DCC will allow persons who are eligible to undertake User Entry Process Tests (pursuant to the Interface Testing Approach Document) to undertake those tests concurrently (provided that, where it is not reasonably practicable to do so, the DCC shall give priority to completion of the User Entry Process Tests by the Supplier Parties);

(j) a Good Industry Practice methodology for determining whether or not the Interface Testing Objective has been achieved in respect of each Region, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria (including, as described in Section T3.27, completion of User Entry Process Tests for that Region by two Large Supplier Parties and (where applicable pursuant to Section T3.21) by at least one Network Party in respect of the 'Electricity Distributor' User Role and/or at least one Network Party in respect of the 'Gas Transporter' User Role); and

(k) how the DCC will report to the Panel where the DCC considers that the exit criteria referred to in (j) above have been achieved in respect of a Region (providing evidence of such achievement), having consulted with the Registration Data Providers and the Parties who are obliged by this Section T3 to undertake the User Entry Process Tests.

Approval of Interface Testing Approach Document

T3.9 The DCC shall submit the Interface Testing Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T3.

T3.10 Before submitting the Interface Testing Approach Document to the Panel, the DCC shall consult with the other Parties, the Panel and the Registration Data Providers regarding the Interface Testing Approach Document. When submitting the Interface Testing Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the other Parties or the Registration Data Providers. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T3.11 Where the Panel decides not to approve the Interface Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the other Parties and the Registration Data Providers; and

(c) re-submit the document to the Panel for approval and comply with Section T3.10 (following which this Section T3.11 or Section T3.12 shall apply).

T3.12 Where the Panel decides to approve the Interface Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC, the other Parties and the Registration Data Providers giving reasons for such decision. In such circumstances, the DCC and each other Party and each Registration Data Provider shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the Interface Testing Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T3;

(b) is not fit for the purposes envisaged by this Section T3, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T3 and should be revised and re-submitted by the DCC in accordance with Section T3.11,

(which determination shall be final and binding for the purposes of this Code).

Commencement of Interface Testing

T3.13 Subject to Section T3.14, once the Interface Testing Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T3.12(b)), the DCC shall publish the approved document on the DCC Website and give at least 6 months' (or such shorter period as the Secretary of State may direct) notice to the other Parties of the date on which Interface Testing is to commence. Where directed to do so by the Secretary of State, the DCC shall determine a revised commencement date for

Interface Testing (provided that the DCC shall first consult on such date with such persons as the Secretary of State may specify in such direction), and shall (where specified by the Secretary of State in such direction) make consequential revisions to the Interface Testing Approach Document (which date (and, where relevant, revisions) must be published at least 6 months (or such shorter period as the Secretary of State may direct) in advance of the date on which Interface Testing is to commence).

T3.14 Where the Panel's approval of the Interface Testing Approach Document is appealed by one or more persons under Section T3.12, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay publication and the giving of notice under Section T3.13, in which case the DCC shall publish the document and give notice under Section T3.13 (noting the appeal). Subject to the foregoing provisions of this Section T3.14, the DCC shall not publish the Interface Testing Approach Document and give notice under Section T3.13 where the Panel's decision has been appealed under Section T3.12 (pending the approval of the document thereunder or revision in accordance with a determination made under Section T3.12(b)).

T3.15 Prior to the commencement of Interface Testing and in accordance with the Interface Testing Approach document, the DCC shall assess whether or not each Large Supplier Party (and, where directed pursuant to Section T3.21, each Network Party) meets the entry criteria referred to in Section T3.8(b), and report to the Panel and that Party on the same. Each Large Supplier Party (and, where directed pursuant to Section T3.21, each Network Party) shall:

(a) take all reasonable steps to ensure that it meets the entry criteria referred to in Section T3.8(b) by the date required in accordance with the Interface Testing Approach Document; and

(b) notify the Panel and the DCC as soon as reasonably practicable if the Party considers that it will not meet those criteria by that date.

T3.16 Section H14.16 (User Entry Process Tests) shall apply where there is any disagreement between the DCC and a Party as to whether that Party has met the entry criteria for the User Entry Process Tests (as modified by the Interface Testing Approach Document), provided that:

(a) the Panel's decision on any such matter may be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code; and

(b) in the case of the Parties referred to in Section T3.15, any such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to that Party and any appeal must be brought within 14 days after the Panel's decision.

Interface Testing

T3.17 The DCC shall comply with its obligations under the approved Interface Testing Approach Document. The DCC shall take reasonable steps~~use its reasonable endeavours~~ to ensure that Interface Testing is completed as soon as it is reasonably practicable to do so.

T3.18 Each Network Party shall ensure that its Registration Data Provider complies with its obligations under the approved Interface Testing Approach Document.

T3.19 Each Party that undertakes the User Entry Process Tests prior to completion of Interface Testing shall do so in accordance with Section H14 (Testing Services) and the approved Interface Testing Approach Document.

T3.20 Each Large Supplier Party shall ~~use its reasonable endeavours~~take reasonable steps to commence the User Entry Process Tests as soon as reasonably practicable (in respect of the User Roles of 'Import Supplier' and/or 'Gas Supplier', depending on which Energy Supply Licence or Energy Supply Licences it holds). Each Large Supplier Party shall, on request, notify the Panel and the DCC of the Party's progress towards completing such User Entry Process Tests.

T3.21 Where directed to do so by the Secretary of State, each Network Party shall take reasonable steps~~use its reasonable endeavours~~ to commence the User Entry Process Tests as soon as reasonably practicable (in respect of the User Roles of 'Electricity Distributor' or 'Gas Transporter', as applicable). Following any such direction, each Network Party shall, on request, notify the Panel and the DCC of the Party's progress towards completing such User Entry Process Tests.

T3.22 Section H14.21 (User Entry Process Tests) shall apply where there is any disagreement between the DCC and a Party as to whether that Party has completed the User Entry Process Tests (as modified by the Interface Testing Approach Document), provided that:

(a) the Panel's decision on any such matter be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code; and

(b) in the case of the Parties referred to in Section T3.15, any such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to that Party and any appeal must be brought within 14 days after the Panel's decision.

T3.23 Where the DCC wishes to make amendments to the Interface Testing Approach Document (other than consequential revisions in accordance with Section T3.13), the DCC shall consult with the other Parties regarding those amendments and submit those amendments to the Panel (in accordance with Section T3.10) for approval (following which Sections T3.11 to T3.14 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Sections T3.13 and T3.14 to giving notice were not included).

Completion of Interface Testing

T3.24 The DCC shall, once the DCC considers that the exit criteria (as envisaged by Section T3.8(j)) have been met in respect of any Region, in accordance with the Interface Testing Approach Document:

(a) provide to the Panel a report evidencing that such criteria have been met;

(b) where relevant, list those sections of the report which the DCC considers should be redacted prior to circulation of the report to the Parties, where the DCC considers that those sections contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems; and

(c) apply to the Panel to determine whether or not such exit criteria have been met,

and the DCC may either (as it reasonably considers appropriate in accordance with the Interface Testing Objective) do so in respect of individual Regions or some or all of the Regions collectively.

T3.25 On application of the DCC pursuant to Section T3.24, the Panel shall:

(a) determine whether or not the exit criteria have been met;

(b) notify its decision to the Secretary of State, the Authority and the Parties, giving reasons for its decision; and

(c) direct the DCC to publish its report, subject to the redaction of those sections of the report which the Panel considers to contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction).

T3.26 Where the DCC has provided a report to the Panel in accordance with Section T3.24, the Panel shall provide a complete copy on request to the Secretary of State and/or the Authority.

T3.27 Subject to Section T3.28, Interface Testing shall be completed once the Panel has confirmed that the exit criteria referred to Section T3.8(j) have been met in respect of each and every Region, which must include (in respect of each Region) that the following persons have completed User Entry Process Tests (for that Region):

(a) at least two Large Supplier Parties who are not an Affiliate of one another in respect of the 'Import Supplier' User Role, and at least two Large Supplier Parties who are not an Affiliate of one another in respect of the 'Gas Supplier' User Role; and

(b) (only where applicable pursuant to Section T3.21) at least one Network Party in respect of the 'Electricity Distributor' User Role and/or at least one Network Party in respect of the 'Gas Transporter' User Role.

T3.28 Each Party shall have the ability (within the 14 days after notification by the Panel) to refer each of the Panel's decisions pursuant to Section T3.25 to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the

Secretary of State directs) to determine whether or not the exit criteria have been met in respect of the Region in question (which determination shall be final and binding for the purposes of this Code).

T3.29 Where, following the application of the DCC pursuant to Section T3.24, the Panel or the person which determines a referral under Section T3.28 determines that one or more of the exit criteria have not been met, the DCC shall undertake further testing in order to demonstrate that the exit criteria have been met and shall resubmit its report under Section T3.24.

Testing Issues

T3.30 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of Interface Testing. Each Party participating in Interface Testing shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of Interface Testing.

T3.31 During Interface Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

Definitions of Large and Small Suppliers

T3.32 For the purpose of this Section T3, the question of whether a Supplier Party is a Large Supplier or a Small Supplier shall be assessed at the time that this Code is first modified to include this Section T3.32.

T3.33 Each Supplier Party that is a Large Supplier in accordance with Section T3.32 shall notify the DCC of their status as such within one month after the time that this Code is first modified to include Section T3.32.

Additional Interface Testing

T3.34 On each occasion that the Secretary of State so directs for the purpose of this Section T3.34, the DCC shall undertake testing against the Interface Testing Objective in respect of such Services that have not previously been the subject of testing under this

Section T3 as the Secretary of State may direct (each such round of testing being "**Additional Interface Testing**").

T3.35 The purpose of each round of Additional Interface Testing shall be to demonstrate the Interface Testing Objective as described in Sections T3.2 and T3.3, but subject to the following variations (the Interface Testing Objective as so varied being the "**Additional Interface Testing Objective**"):

(a) the only variations pursuant to Section X (Transition) that will be taken into account in interpreting the relevant Sections are those that will continue to apply following commencement of the provision of the Services that are the subject of that round of Additional Interface Testing; and

(b) the Additional Interface Testing Objective shall not apply by reference to the document published from time to time by the Secretary of State for the purpose of Section T3.3(b), but instead by reference to the document published from time to time by the Secretary of State for the purposes of that round of Additional Interface Testing.

T3.36 The provisions of this Section T3 shall apply to each round of Additional Interface Testing, subject to the following:

(a) all references in this Section T3 to "Interface Testing" shall be read as references to "the relevant round of Additional Interface Testing";

(b) Sections T3.34 and T3.35 shall apply in place of Sections T3.2 and T3.3; for which purpose it is acknowledged that some of the capability and interoperability to be demonstrated via Additional Interface Testing will already have been demonstrated via previous testing undertaken pursuant to this Section T3 (and further testing of such capability or interoperability shall not be required to the extent that it has already been sufficiently proven for the Additional Interface Testing Objective as part of such earlier testing);

(c) the Additional Interface Testing shall be undertaken only in respect of the Region or Regions directed by the Secretary of State;

(d) to the extent that the Additional Interface Testing relates to Additional Release

Services, the references to User Entry Process Tests in Sections T3.16, T3.20, T3.21, T3.22 and T3.27 shall be read as references to the corresponding Additional SR Tests;

(e) the Interface Testing Approach Document shall apply to the Additional Interface Testing (without prejudice to the DCC's ability to make changes to the Interface Testing Approach Document in accordance with this Section T3);

(f) one month's notice must be given by the DCC in advance of commencement of Additional Interface Testing (or such shorter period as the Secretary of State may direct);

(g) the Device Models to be used for Additional Interface Testing are those selected pursuant to the previous phase of testing pursuant to this Section T.

T4 END-TO-END TESTING

Overview

T4.1 End-to-End Testing allows for provision of the User Entry Process Tests and Device and User System Tests, subject to any modifications necessary for the purposes of transition.

Overlapping Provision of Interface Testing and End-to-End Testing

T4.2 Prior to the start of End-to-End Testing, the DCC may recommend to the Panel, having regard to the overriding objective of completing Interface Testing in a timely manner, that End-to-End Testing should be provided from the commencement of or from some point during Interface Testing. Where the DCC so recommends, it must provide a report to the Panel on the benefits and risks of the DCC providing End-To-End Testing in parallel with Interface Testing (rather than following completion of Interface Testing). Prior to submitting its report to the Panel, the DCC shall consult with the other Parties regarding the recommendation. The DCC shall also submit copies of the consultation responses received from Parties. Where it has submitted its report to the Panel, the DCC shall publish the report and such consultation responses (to the extent that they are not marked confidential) on the DCC Website.

T4.3 Where the Panel agrees with the DCC's recommendation pursuant to Section T4.2, then End-to-End Testing shall commence from the time recommended (notwithstanding the notice period in Section T4.9). Otherwise, End-to-End Testing shall commence on completion of Interface Testing (or such later date as is necessary to allow compliance with Section T4.9).

End-to-End Testing Approach Document

T4.4 The DCC shall develop a document (the "**End-to-End Testing Approach Document**") which sets out:

(a) the manner in which User Entry Process Tests and Device and User System Tests are to be provided during End-to-End Testing, which shall be consistent with the relevant requirements of Section H14 (Testing Services) subject only to amendments reasonably required for the purposes of transition;

(b) that, to the extent it is reasonably practicable to do so, the DCC shall allow persons who are eligible to undertake tests pursuant to the End-to-End Testing Approach Document to undertake those tests concurrently (provided that, where it is not reasonably practicable to do so, the DCC shall give priority to completion of the User Entry Process Tests by the Supplier Parties during the period prior to the completion of Interface Testing and the DCC shall otherwise schedule Testing Participants as is reasonable for the purposes of transition); and

(c) the latest date from which the DCC will first make Test Communications Hubs available pursuant to Section F10 (Test Communications Hubs).

Approval of End-to-End Testing Approach Document

T4.5 The DCC shall submit the End-to-End Testing Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T4.

T4.6 Before submitting the End-to-End Testing Approach Document to the Panel, the DCC shall consult with the other Parties, the Panel and those persons entitled to undertake Device and User System Tests regarding the End-to-End Testing Approach Document. When submitting the End-to-End Testing Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the other Parties and such persons. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T4.7 Where the Panel decides not to approve the End-to-End Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the other Parties and those persons entitled to undertake Device and User Systems Tests; and

(c) re-submit the document to the Panel for approval and comply with Section T4.6 (following which this Section T4.7 or Section T4.8 shall apply).

T4.8 Where the Panel decides to approve the End-to-End Testing Approach Document

submitted for approval, the Panel shall notify such decision to the DCC, the other Parties and the other persons who provided consultation responses in accordance with Section T4.6, giving reasons for such decision. In such circumstances, the DCC and each other Party shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the End-to-End Testing Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T4;

(b) is not fit for the purposes envisaged by this Section T4, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T4 and should be revised and re-submitted by the DCC in accordance with Section T4.7,

(and any such determination shall be final and binding for the purposes of this Code).

Commencement of End-to-End Testing

T4.9 Subject to Section T4.10, once the End-to-End Testing Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T4.8(b)), the DCC shall publish the approved document on the DCC Website and (subject to Section T4.3) give at least 6 months' prior notice to Testing Participants of the date on which End-to-End Testing is to commence (or such shorter period as the Secretary of State may direct). Where directed to do so by the Secretary of State, the DCC shall determine a revised commencement date for End-to-End Testing (provided that the DCC shall first consult on such date with such persons as the Secretary of State may specify in such direction), and shall (where specified by the Secretary of State in such direction) make consequential revisions to the End-to-End Testing Approach Document (which date (and, where relevant, revisions) must be published at least 6 months (or such shorter period as the Secretary of State may direct) in advance of the revised date on which End-to-End Testing is to commence).

T4.10 Where the Panel's approval of the End-to-End Testing Approach Document is appealed by one or more persons, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay publication and the giving of notice under Section

T4.9, in which case the DCC shall publish the document and give notice under Section T4.9 (noting the appeal). Subject to the foregoing provisions of this Section T4.10, the DCC shall not publish the End-to-End Testing Approach Document and give notice under Section T4.9 where the Panel's decision has been appealed under Section T4.8 (pending the approval of the document thereunder or revision in accordance with a determination made under Section T4.8(b)).

End-to-End Testing

T4.11 The DCC shall comply with its obligations under the approved End-to-End Testing Approach Document.

T4.12 Each Party that seeks to undertake User Entry Process Tests or Device and System Tests during End-to-End Testing shall do so in accordance with the approved End-to-End Testing Approach Document. Where the DCC is to provide Testing Services during End-to-End Testing to a person that is not a Party, the DCC shall act in accordance with any relevant provisions of the End-to-End Testing Approach Document.

T4.13 Where the DCC wishes to make amendments to the End-to-End Testing Approach Document (other than consequential revisions in accordance with Section T4.9), the DCC shall consult with the other Parties, the Panel and those persons entitled to undertake Device and User System Tests regarding those amendments and submit those amendments to the Panel (in accordance with Section T4.6) for approval (following which Sections T4.7 to T4.10 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Section T4.9 and T4.10 to giving notice were not included).

Disputes

T4.14 Section T3.16 shall apply during Interface Testing in respect of the entry criteria for the User Entry Process Tests. Otherwise, in the case of those disputes relating to User Entry Process Tests and Device and User System Tests that would ordinarily be subject to the Authority's determination pursuant to Section H14 (Testing Services), during End-to-End Testing, the Secretary of State may direct that such disputes are determined by the Secretary of State (or, where the Secretary of State so directs such other person

as the Secretary of State directs), rather than the Authority. The determination of such disputes by the Secretary of State (or such other person as the Secretary of State directs) shall be final and binding for the purposes of this Code.

Completion of End-to-End Testing

T4.15 Subject to Section T4.17, End-to-End Testing shall cease on the date 12 months after it commenced (or 12 months after such later date as the Secretary of State may direct for the purpose of this Section T4.15).

T4.16 During the third~~ninth~~ month prior to the date on which~~of~~ End-to-End Testing is due to complete in accordance with Section T4.15 (or at such other time as the DCC and the Panel may agree), the DCC shall submit a recommendation to the Panel as to whether or not the period of End-to-End Testing should be extended by an additional 6 months. Prior to submitting such recommendation to the Panel, the DCC shall consult the Testing Participants on the matter. When submitting such recommendation to the Panel, the DCC shall also submit copies of any consultation responses received from the Testing Participants. The DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T4.17 The Panel shall, after receipt of the DCC's recommendation in accordance with Section T4.16, decide whether or not the period of End-to-End Testing should be extended by an additional 6 months. The Panel shall notify the Testing Participants of its decision, and of the reasons for its decision. Where the Panel decides that the period of End-to-End Testing should be extended by an additional 6 months, then End-to-End Testing shall end on the date 18 months after the date it started (which decision shall be final and binding for the purposes of this Code).

Testing Issues

T4.18 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of End-to-End Testing. Each Party participating in User Entry Process Tests or Device and System Tests during End-to-End Testing shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of End-to-End Testing.

T4.19 During End-to-End Testing, the DCC shall provide the Secretary of State with copies of

the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

T5 SMKI AND REPOSITORY TESTING

Overview

T5.1 SMKI and Repository Testing tests the capability of the DCC and the component parts of the DCC Systems to interoperate with the Systems of Parties to the extent necessary for the SMKI Services and the SMKI Repository Service.

SRT Objective

T5.2 The objective of SMKI and Repository Testing (the "**SRT Objective**") is to demonstrate that the DCC and the DCC Systems interoperate with each other and with Systems of Parties to the extent necessary in order that the DCC is capable of complying with its obligations under Section L (Smart Metering Key Infrastructure) at (during the relevant period) the levels of activity reasonably anticipated during the relevant period, and (thereafter) the levels of activity set out in Section L (Smart Metering Key Infrastructure). For the purposes of this Section T5.2, the relevant period is the period from commencement of the SMKI Services until the date from which Smart Meters are capable of being Commissioned pursuant to Section H5 (Smart Metering Inventory and Enrolment Services).

T5.3 For the purposes of Section T5.2, the Sections referred to in that Section shall be construed by reference to:

(a) the decision or consultation document concerning the intended future content of those Sections most recently published by the Secretary of State prior to [DATE~~14 December 2015~~] [3] (regardless of whether the content of those documents has yet been incorporated into this Code~~,~~ or whether those Sections ~~are stated to not~~ yet have effect~~apply under Section X (Transition)~~, but taking into account any variations to this Code pursuant to Section X (Transition) that apply (or are due to apply on the Section or a relevant Subsidiary Document coming into effect) and that will continue to apply following the date on which the provisions in relation to the Issue of Device Certificates and Organisation Certificates under Section L3 (SMKI Services) take effect); and

[3] This date is to reflect the date on which the modification to this section is laid before Parliament.

(b) to the extent not inconsistent with any document referred to in (a), any document regarding technical or procedural requirements which support those Sections which is published from time to time by the Secretary of State for the purposes of this Section T5.3.

T5.4 From the date on which the SMKI and Repository Entry Process Tests can be commenced (as set out in the SRT Approach Document), Parties who wish to do so, and who are ready to do so in accordance with the entry criteria for the SMKI and Repository Entry Process Tests, shall be able to undertake the SMKI and Repository Entry Process Tests (pursuant to Section H14 (Testing Services)).

SRT Approach Document

T5.5 The DCC shall develop a document (the "**SRT Approach Document**") which sets out:

(a) the reasonable entry criteria to be satisfied by the DCC with respect to the DCC Systems and the Communications Hubs selected pursuant to Section T1 prior to commencement of SMKI and Repository Testing;

(b) the entry criteria to be met by each Party prior to its commencing the SMKI and Repository Entry Process Tests (which criteria shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of SMKI and Repository Testing);

(c) the manner in which SMKI and Repository Testing is to be undertaken, including the respective obligations of the DCC and each other Party;

(d) a reasonable timetable for undertaking and completing SMKI and Repository Testing (including the date from which the SMKI and Repository Entry Process Tests can be commenced);

(e) the frequency and content of progress reports concerning SMKI and Repository Testing to be provided by the DCC to the Panel (which the Panel shall make available to the Secretary of State, the Authority and Testing Participants), which reports must include details of Testing Issues identified and resolved and of any problems and solutions encountered with respect to Devices (the details

of such Testing Issues to be anonymised and redacted as required in accordance with Section H14.44 (General: Testing Issue Resolution Process));

(f) the process by which the DCC will facilitate Parties undertaking and completing the SMKI and Repository Entry Process Tests (which process shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of SMKI and Repository Testing);

(g) a Good Industry Practice methodology for determining whether or not the SRT Objective has been achieved, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria (including completion of SMKI and Repository Entry Process Tests by two Large Supplier Parties as described in Section T5.20); and

(h) how the DCC will report to the Panel where the DCC considers that the exit criteria referred to in (g) above have been achieved (providing evidence of such achievement), having consulted with the Parties who have participated in SMKI and Repository Testing.

Approval of SRT Approach Document

T5.6 The DCC shall submit the SRT Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T5.

T5.7 Before submitting the SRT Approach Document to the Panel, the DCC shall consult with the other Parties, the Panel and the SMKI PMA regarding the SRT Approach Document. When submitting the SRT Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the other Parties. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T5.8 The Panel shall consult with the SMKI PMA prior to deciding whether or not to approve the SRT Approach Document submitted for approval.

T5.9 Where the Panel decides not to approve the SRT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving

reasons for such decision. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the other Parties; and

(c) re-submit the document to the Panel for approval and comply with Section T5.7 (following which Section T5.8 shall apply and this Section T5.9 or Section T5.10 shall apply).

T5.10 Where the Panel decides to approve the SRT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC and each other Party shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the SRT Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T5;

(b) is not fit for the purposes envisaged by this Section T5, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T5 and should be revised and re-submitted by the DCC in accordance with Section T5.9,

(which determination shall be final and binding for the purposes of this Code).

Commencement of SMKI and Repository Testing

T5.11 Subject to Section T5.12, once the SRT Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T5.10(b)), the DCC shall publish the approved document on the DCC Website and give at least 3 months' (or such shorter period as the Secretary of State may direct) notice to the other Parties of the date on which SMKI and Repository Testing is to commence. Where directed to do so by the Secretary of State, the DCC shall determine a revised commencement date for SMKI and Repository Testing (provided that the DCC shall first consult on such date with such persons as the Secretary of State may specify in such direction), and shall

(where specified by the Secretary of State in such direction) make consequential revisions to the SRT Approach Document (which date (and, where relevant, revisions) must be published at least 3 months (or such shorter period as the Secretary of State may direct) in advance of the revised date on which SKMI and Repository Testing is to commence).

T5.12 Where the Panel's approval of the SRT Approach Document is appealed by one or more persons under Section T5.10, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay publication and the giving of notice under Section T5.11, in which case the DCC shall publish the document and give notice under Section T5.11 (noting the appeal). Subject to the foregoing provisions of this Section T5.12, the DCC shall not publish the SRT Approach Document and give notice under Section T5.11 where the Panel's decision has been appealed under Section T5.10 (pending the approval of the document thereunder or revision in accordance with a determination made under Section T5.10(b)).

T5.13 Prior to the date from when the SMKI and Repository Entry Process Tests can be commenced and in accordance with the SRT Approach document, the DCC shall assess whether or not each Large Supplier Party meets the entry criteria referred to in Section T5.5(b), and report to the Panel and that Party on the same. Each Large Supplier Party shall:

(a) take all reasonable steps to ensure that it meets the entry criteria referred to in Section T5.5(b) prior to the date from which the SMKI and Repository Entry Process Tests can be commenced; and

(b) notify the Panel and the DCC as soon as reasonably practicable if the Party considers that it will not meet those criteria prior to the date from which the SMKI and Repository Entry Process Tests can be commenced.

T5.14 Section H14.25 (SMKI and Repository Entry Process Tests) shall apply where there is any disagreement between the DCC and a Party as to whether that Party has met the entry criteria for the SMKI and Repository Entry Process Tests (as modified by the SRT Approach Document), provided that:

(a) the Panel's decision on any such matter may be appealed to the Authority (or,

where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code; and

(b) in the case of the Parties referred to in Section T5.13, such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to that Party and any appeal must be brought within 14 days after the Panel's decision.

SMKI and Repository Testing

T5.15 The DCC shall comply with its obligations under the approved SRT Approach Document. The DCC shall take reasonable steps~~use its reasonable endeavours~~ to ensure that SMKI and Repository Testing is completed as soon as it is reasonably practicable to do so.

T5.16 Each Party that undertakes the SMKI and Repository Entry Process Tests pursuant to the SRT Approach Document shall do so in accordance with Section H14 (Testing Services) and the approved SRT Approach Document.

T5.17 Each Large Supplier Party shall take reasonable steps~~use its reasonable endeavours~~ to commence the SMKI and Repository Entry Process Tests as soon as reasonably practicable (in respect of all the roles to which the SMKI and Repository Entry Process Tests apply). Each Large Supplier Party shall, on request, notify the Panel and the DCC of the Party's progress towards completing such SMKI and Repository Entry Process Tests.

T5.18 Where the DCC wishes to make amendments to the SRT Approach Document (other than consequential revisions in accordance with Section T5.11), the DCC shall consult with the other Parties regarding those amendments and submit those amendments to the Panel (in accordance with Section T5.7) for approval (following which Sections T5.8 to T5.12 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Sections T5.11 and T5.12 to giving notice were not included).

Completion of SMKI and Repository Testing

T5.19 The DCC shall, once the DCC considers that the exit criteria (as envisaged by Section

T5.5(g)) have been met, in accordance with the SRT Approach Document:

(a) provide to the Panel a report evidencing that such criteria have been met;

(b) where relevant, list those sections of the report which the DCC considers should be redacted prior to circulation of the report to the Parties, where the DCC considers that those sections contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems; and

(c) apply to the Panel to determine whether or not such exit criteria have been met.

T5.20 Such exit criteria must include a requirement that at least two Large Supplier Parties who are not an Affiliate of one another have each completed the SMKI and Repository Entry Process Tests to become:

(a) an Authorised Subscriber under the Organisation Certificate Policy;

(b) an Authorised Subscriber under the Device Certificate Policy; and

(c) eligible to access the SMKI Repository.

T5.21 On application of the DCC pursuant to Section T5.19, the Panel shall:

(a) determine whether or not the exit criteria have been met;

(b) notify its decision to the Secretary of State, the Authority and the Parties, giving reasons for its decision ; and

(c) direct the DCC to publish its report, subject to the redaction of those sections of the report which the Panel considers to contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction).

T5.22 Where the DCC has provided a report to the Panel in accordance with Section T5.19, the Panel shall provide a complete copy on request to the Secretary of State and/or the Authority.

T5.23 Subject to Section T5.24, SMKI and Repository Testing shall be completed once the

Panel has determined that the exit criteria referred to Section T5.5(g) have been met in respect of the Parties referred to in Section T5.20.

T5.24 Each Party shall have the ability (within the 14 days after notification by the Panel) to refer the Panel's decision pursuant to Section T5.21 to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether or not the exit criteria have been met in respect of the Parties referred to in Section T5.20 (which determination shall be final and binding for the purposes of this Code).

T5.25 Where, on the application of the DCC pursuant to Section T5.19, it has been determined that one or more of the exit criteria have not been met, the DCC shall undertake further testing in order to demonstrate that the exit criteria have been met and shall resubmit its report in accordance with Section T5.19.

Testing Issues

T5.26 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of SMKI and Repository Testing. Each Party participating in SMKI and Repository Testing shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of SMKI and Repository Testing.

T5.27 During SMKI and Repository Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

Definitions of Large and Small Suppliers

T5.28 For the purpose of this Section T5, the question of whether a Supplier Party is a Large Supplier or a Small Supplier shall be assessed at the time that this Code is first modified to include this Section T5.28.

T5.29 Each Supplier Party that is a Large Supplier in accordance with Section T5.28 shall notify the DCC of their status as such within one month after the time that this Code is first modified to include Section T5.28.

Additional SMKI and Repository Testing

T5.30 On each occasion that the Secretary of State so directs for the purpose of this Section T5.30, the DCC shall undertake testing against the SRT Objective in respect of such Services that have not previously been the subject of testing under this Section T5 as the Secretary of State may direct (each such round of testing being "**Additional SMKI and Repository Testing**").

T5.31 The purpose of each round of Additional SMKI and Repository Testing shall be to demonstrate the SRT Objective as described in Sections T5.2 and T5.3, but subject to the following variations (the SRT Objective as so varied being the "**Additional SRT Objective**"):

(a) the only variations pursuant to Section X (Transition) that will be taken into account in interpreting the relevant Sections are those that will continue to apply following commencement of the provision of the Services that are the subject of that round of Additional SMKI and Repository Testing; and

(b) the Additional SRT Objective shall not apply by reference to the document published from time to time by the Secretary of State for the purpose of Section T5.3(b), but instead by reference to the document published from time to time by the Secretary of State for the purposes of that round of Additional SMKI and Repository Testing.

T5.32 The provisions of this Section T5 shall apply to each round of Additional SMKI and Repository Testing, subject to the following:

(a) all references in this Section T5 to "SMKI and Repository Testing" shall be read as references to "the relevant round of Additional SMKI and Repository Testing";

(b) Sections T5.30 and T5.31 shall apply in place of Sections T5.2 and T5.3; for which purpose it is acknowledged that some of the capability and interoperability to be demonstrated via Additional SMKI and Repository Testing will already have been demonstrated via previous testing undertaken pursuant to this Section T5 (and further testing of such capability or interoperability shall not be required to the extent that it has already been

sufficiently proven for the Additional SRT Objective as part of such earlier testing);

(c) the SRT Approach Document shall apply to the Additional SMKI and Repository Testing (without prejudice to the DCC's ability to make changes to the SRT Approach Document in accordance with this Section T5);

(d) no period of notice need be given by the DCC in advance of commencement of Additional SMKI and Repository Testing (unless otherwise directed by the Secretary of State);

(e) the following Sections concerning commencement and completion of SMKI and Repository Entry Process Tests by Large Supplier Parties shall not apply: Sections T5.5(g), T5.13, T5.14, T5.17, and T5.20; and

(f) notwithstanding paragraph (e) above, Large Supplier Parties shall be required to participate in Additional SMKI and Repository Testing if so directed by the Secretary of State in respect of that round of Additional SMKI and Repository Testing and in the manner set out in such direction.

T6 DEVELOPMENT OF ENDURING TESTING DOCUMENTS

Overview

T6.1 The Common Test Scenarios Document, the SMKI and Repository Test Scenarios Document and the Enduring Testing Approach Document are to be developed by the DCC pursuant to this Section T6, and incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the Test Scenarios Documents

T6.2 The purpose of each of the Common Test Scenarios Document and the SMKI and Repository Test Scenarios Document is set out in Section H14 (Testing Services).

T6.3 The Common Test Scenarios Document must include test scenarios for testing use of the Self-Service Interface and the DCC User Interface and any entry requirements (for particular User Roles) prior to execution of those tests. In respect of the DCC User Interface, such tests must include (for each User Role) a requirement for the successful testing of Service Requests for each Service set out in the DCC User Interface Services Schedule in respect of that User Role.

Purpose of the Enduring Testing Approach Document

T6.4 The purpose of the Enduring Testing Approach Document is to set out (in respect of persons who are eligible to undertake tests pursuant to the Testing Services) how and in what circumstances the Testing Services are to be provided, including details of:

(a) the obligations with which the DCC and Testing Participants must comply in respect of the Testing Services (including in relation to security);

(b) how the DCC will provide any Testing Services remotely (including over DCC Gateway Connections);

(c) how the DCC will provide a connection to a simulation of the SM WAN pursuant to Section H14.31 (Device and User System Tests); and

(d) how the DCC will make Test Certificates available pursuant to Section H14.11 (General: Test Certificates), which may make different provision in respect of

different categories of Test Certificates.

Process to Develop Documents

T6.5 The procedure by which the DCC is to develop each of the Common Test Scenarios Document, the SMKI and Repository Test Scenarios Document and the Enduring Testing Approach Document is as follows:

(a) the DCC shall produce draft documents by such date as is reasonably necessary to meet the applicable date under Section T6.5(d);

(b) in producing each draft document, the DCC must consult appropriately with the Parties;

(c) where disagreements with the Parties arise concerning the proposed content of either document, the DCC shall seek to reach an agreed solution with them, but without prejudice to the purposes of the document;

(d) having complied with (b) and (c) above, the DCC shall submit each draft document to the Secretary of State as soon as is reasonably practicable, and:

(i) in the case of the Common Test Scenarios Document and the SMKI and Repository Test Scenarios Document, in any case by the date seven months prior to the expected commencement date of Interface Testing as set out in the Interface Testing Approach Document (or such later date as the Secretary of State may direct); or

(ii) in the case of the Enduring Testing Approach Document, in any case by the date three months prior to the expected commencement date of End-to-End Testing as set out in the End-to-End Testing Approach Document (or such later date as the Secretary of State may direct);

(e) when submitting a draft document under (d) above, the DCC shall indicate to the Secretary of State:

(i) why the DCC considers the draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) any areas of disagreement that arose during the consultation process and that have not been resolved; and

(f) the DCC must comply with the requirements with respect to process and timeframe of any direction that is given by the Secretary of State to resubmit either document.

T7 ENDING OF THE APPLICATION OF THIS SECTION T

T7.1 This Section T shall cease to apply, and this Code shall automatically be modified so as to delete this Section T, on the last to occur of the following:

(a) completion of Interface Testing;

(b) completion of End-to-End Testing; and

(c) completion of SMKI and Repository Testing.

SECTION X: TRANSITION

X1 GENERAL PROVISIONS REGARDING TRANSITION

Overriding Nature of this Section

X1.1 The provisions of this Section X shall apply notwithstanding, and shall override, any other provision of this Code.

Transition Objective

X1.2 The objective to be achieved pursuant to this Section X (the "**Transition Objective**") is the efficient, economical, co-ordinated, timely, and secure process of transition to the Completion of Implementation.

X1.3 The "**Completion of Implementation**" shall occur on the date designated for the purpose of this Section X1.3 by the Secretary of State (or such person as the Secretary of State may designate for the purposes of this Section X1.3), once the Secretary of State (or the person so designated) is of the opinion that:

(a) the documents referred to in Section X5 and that the Secretary of State (or the person so designated) considers material to the implementation of this Code have been incorporated into this Code in accordance with that Section;

(b) the provisions of this Code that the Secretary of State (or the person so designated) considers material to the implementation of this Code apply in full without any variation pursuant to this Section X (or, where any such variations do apply, the requirements of Sections X1.3(c) will still be met despite such variations ending in accordance with Section X1.5(a)); and

(c) each Party that holds an Energy Licence is (or would be had such Party acted in accordance with Good Industry Practice) reasonably able (on the assumption that such Party acts in accordance with Good Industry Practice) to perform its obligations, and to exercise its rights, under this Code to the extent that the Secretary of State (or the person so designated) considers such obligations or rights material to the implementation of this Code.

X1.4 Before designating a date for the purpose of Section X1.3, the Secretary of State (or the person designated for the purposes of this Section X1.3) must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State (or the person so designated) considers appropriate in the circumstances within which representations or objections may be made.

Ending of the Application of this Section X

X1.5 With effect from the earlier of:

(a) Completion of Implementation; or

(b) 31 October 2018,

this Section X (and any variations to this Code provided for in, or made by directions pursuant to, this Section X) shall cease to apply (save as set out in Section X5.8), and this Code shall automatically be modified so as to delete this Section X.

General Obligations

X1.6 Each Party shall take all reasonable steps to do all such things as are within its power and necessary or expedient in order to facilitate achievement of the Transition Objective.

X1.7 Each Party shall provide such reasonable co-operation and assistance to the other Parties and to the Panel as may be necessary to facilitate compliance with the provisions of this Section X, and with any variations to this Code provided for in (or made by directions pursuant to) this Section X.

X1.8 Without prejudice to its legal rights, no Party shall take any step, or exercise any right, which is intended to (or might reasonably be expected to) hinder or frustrate the achievement of the Transition Objective.

Information

X1.9 Each Party shall provide to the Secretary of State, in such manner and at such times as the Secretary of State may reasonably require, such Data as the Secretary of State may

reasonably require in order to enable the Secretary of State to assess progress towards (and to facilitate) achievement of the Transition Objective. No Party shall be obliged to provide information under this Section X1.9 where such Party is obliged to provide such information under its Energy Licence, or where such information is expressly excluded from the information that such Party is obliged to provide under its Energy Licence.

X1.10 If a Party is aware of any matter or circumstance which it considers will materially delay or frustrate the achievement of the Transition Objective, that Party shall promptly inform the Secretary of State of such matter or circumstance.

Network Parties to become Subscribers

X1.11 Prior to the commencement of the provision of Enrolment Services by the DCC pursuant to Section H5 (Smart Metering Inventory and Enrolment Services), each Network Party shall ensure that it has become a Subscriber for those Organisation Certificates which pertain to it and that are required by Responsible Suppliers for the purpose of complying with their obligations under Clause 5 (Post-Commissioning Obligations) of the Inventory Enrolment and Withdrawal Procedures.

Day-One Elective Communication Services

X1.12 Where the Secretary of State designates one or more draft Bilateral Agreements for the purposes of this Section X1.12 (each of which drafts must specify the potential Elective Communication Services to be provided thereunder, and the DCC's potential counterparty thereunder), then:

(a) the DCC shall, within 10 Working Days thereafter, make a formal offer to each of the counterparties in question for the Elective Communication Services in question as if Section H7.12 (Formal Offer) applied;

(b) such offer shall be on the basis of the draft Bilateral Agreement designated by the Secretary of State (subject only to the addition of the applicable Elective Charges, any termination fee and any credit support requirements);

(c) the counterparty shall be under no obligation to accept such offer; and

(d) any agreement entered into pursuant to this Section X1.12 shall be a Bilateral Agreement.

Disputes

X1.13 In the event of any dispute between the Parties (or between the Panel and any Party) as to whether a particular Party is obliged to undertake a particular activity pursuant to Section X1.6 to X1.12 (inclusive), a Party (or the Panel) may refer the matter to the Secretary of State (or, where designated by the Secretary of State for such purposes, the Panel or the Authority) for determination (which determination may include a requirement to comply with such terms and conditions as the person making it considers appropriate in all the circumstances of the case). Any determination by the Secretary of State or by the Authority pursuant to this Section X1.13 shall be final and binding for the purposes of this Section X1. Any determination by the Panel pursuant to this Section X1.13 shall be subject to appeal to the Secretary of State (or, where designated by the Secretary of State for such purposes, to the Authority), the determination of such appeal being final and binding for the purposes of this Section X1.

Modification of this Section X

X1.14 The variations to this Code provided for in, or made by directions pursuant to, this Section X shall not constitute modifications that should be subject to Section D (Modification Process). For the avoidance of doubt, this Section X shall be capable of being modified under Section D (Modification Process).

SECCo

X1.15 The provisions of this Section X1 (and the definitions used in this Section) shall apply to SECCo as if SECCo was a Party.

Publication of Draft Subsidiary Documents by the DCC

X1.16 Where, pursuant to this Code or the DCC Licence, the DCC is required to prepare or produce and to consult upon a draft (or further draft) of a document (or to resubmit a document) that is intended to be incorporated into this Code as a SEC Subsidiary Document, the DCC shall, at or around the same time as the DCC sends such

document to the Secretary of State, publish on the DCC Website:

(a) a copy of the document sent to the Secretary of State; and

(b) a summary of any material comments raised in response to the consultation and a brief description of the reasons why any associated changes to the document were or were not made.

Testing in respect of Additional Release Services

X1.17 A Party seeking to become a User for a particular User Role must undertake the User Entry Process Tests relevant to that User Role, as described in Sections H1 (User Entry Process) and H14 (Testing). Completion of User Entry Process Tests by certain Parties in relation to certain User Roles also forms part of Interface Testing under Section T3 (Interface Testing), and (for so long as Section T4 (End-to-End Testing) applies) User Entry Process Test are to be undertaken as part of End-to-End Testing. Certain Services are only available to Parties that have become a User for the applicable User Role, as described in Section H3 (DCC User Interface) and the DCC User Interface Services Schedule. Where the Secretary of State makes directions pursuant to Section X3 (Provisions to Become Effective Following Designation) whereby the Common Test Scenarios Document is varied on it first becoming effective so that there are Service Requests that are deemed to be omitted from the document, then the following provisions shall apply:

(a) the Service Requests that are subject to such a direction shall, for so long as the variation in respect of that Service Request remains in effect, be "**Additional Release Services**";

(b) Parties that start User Entry Process Tests at a time where there are Additional Release Services shall undertake (and be able to successfully complete) the User Entry Process Tests without reference to those Additional Release Services;

(c) a User that completes User Entry Process Tests that did not include testing of Service Requests that used to be (but are no longer) Additional Release Services shall (notwithstanding any other provision of this Code) not be an

Eligible User for those Service Requests until that User has successfully completed the applicable Additional SR Tests for those Service Requests; and

(d) "**Additional SR Tests**" means, in respect of one or more Service Requests that used to be (but are no longer) Additional Release Services, testing equivalent to User Entry Process Tests but undertaken only in respect of those Service Requests. Accordingly, and without limitation, the following shall apply:

(i) Additional SR Tests shall constitute a Testing Service, and shall therefore be subject to the provisions of Section H14 (Testing Services);

(ii) Additional SR Tests shall be provided by the DCC, and shall be capable of being undertaken by Parties, in accordance with Sections H14.12 to H14.21 (User Entry Process Tests), but:

(A) construed by reference to only those relevant Service Requests;

(B) where a Party has already demonstrated capability for the purposes of User Entry Process Tests, this can be relied upon for the purposes of the Additional SR Tests (unless the DCC considers that this is not appropriate for those Additional SR Tests);

(C) potentially (as provided for in the Common Test Scenarios Document) without the need to re-test the DCC Gateway Connection;

(D) without the need to re-test the Self-Service Interface; and

(E) subject to any other exceptions provided for in the Common Test Scenarios Document; and

~~(c)~~(e) any provisions from time to time applying to User Entry Process Tests pursuant to the Interface Testing Approach Document or the End-to-End Testing Approach Document shall apply equally to Additional SR Tests (unless otherwise set out in those approach documents).

DCC Live Services Criteria Report

~~X1.17~~X1.18 This Section X1.18 shall apply where the DCC produces a report concerning its readiness to commence provision of the Services (or any part of the Services), and where the Secretary of State directs the Panel to review that report. Where this Section X1.18 applies, the Panel shall review the DCC's report and report to the Secretary of State in accordance with the criteria, scope and timing specified in the Secretary of State's direction.

X2 EFFECTIVE PROVISIONS AT DESIGNATION

Provisions to have Effect from Designation

X2.1 The following Sections, Schedules and SEC Subsidiary Documents shall be effective from the date of this Code's designation (subject to the other provisions of this Section X):

(a) Section A (Definitions and Interpretation);

(b) Section B (Accession);

(c) Section C (Governance);

(d) Section D (Modification Process);

(e) Section E (Registration Data);

(f) Section K (Charging Methodology);

(g) Section M (General);

(h) Section X (Transition);

(i) Schedule 1 (Framework Agreement);

(j) Schedule 2 (Specimen Accession Agreement);

(k) Schedule 4 (Establishment of SECCo);

(l) Schedule 5 (Accession Information); and

(m) Schedule 6 (Specimen Form Letter of Credit).

Effectiveness of Section J

X2.2 Section J (Charges) shall be effective (subject to the other provisions of this Section X) from the earlier of:

(a) the date three months after the date of this Code's designation; or

(b) the date notified by the DCC to the other Original Parties on not less than 10

Working Days prior notice (on the basis that the DCC may only specify one such date from which date all of Section J shall be effective),

provided that the DCC shall be entitled to recover Charges in respect of the period from the designation of this Code.

Variations in respect of Section D

X2.3 Notwithstanding that Section D (Modifications) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.3, apply as varied by this Section X2.3. The variations to apply pursuant to this Section X2.3 are that Section D (Modifications) is to apply subject to the following:

(a) the only Modification Proposals that may be raised are:

(i) subject to paragraph (b), a Path 2 Modification or a Path 3 Modification which is not an Urgent Proposal;

(ii) a Fast-Track Modification which is not an Urgent Proposal; and

(iii) a Modification Proposal of any type that is an Urgent Proposal;

(b) where either a Path 2 Modification or Path 3 Modification which is not an Urgent Proposal is raised, Section D (Modifications) shall apply to the Modification Proposal subject to the following variations:

(i) Section D8.20 (Communicating the Change Board Vote) shall apply as if each reference in that Section to "the Authority" referred to "the Secretary of State and the Authority";

(ii) the following provisions shall apply as if each reference in them to “the Authority” referred to “the Secretary of State”: Section D8.3(a) (Effect of Change Board Decision); Section D9.2 (Path 1 Modifications and Path 2 Modifications); Section D9.3 (Send-Back Process); Section D9.4 (Path 3 Modifications); and Sections D10.5 and D10.6 (Subsequent Amendment to Implementation Timetable);

(c) any Modification Proposal that is raised by a Proposer on the basis that it is

urgent, but which is subsequently determined by the Authority (as provided for in Section D4) not to be an Urgent Proposal, shall be cancelled and shall not be progressed;

(d) the Secretary of State shall be entitled to direct the Panel to cancel or suspend any Modification Proposal, in which case the Panel shall cancel or suspend the Modification Proposal in question and it shall not then be further progressed or implemented (or, in the case of suspension, shall not then be further progressed or implemented until the Secretary of State so directs); and

(e) the Change Board need not be established on the designation of this Code, but the Panel shall establish the Change Board as soon as reasonably practicable after the designation of this Code, and until the Change Board is established the Panel shall perform the function of the Change Board in respect of Modification Proposals (in which case, the Panel shall vote on whether to approve or reject a Modification Proposal in accordance with the Panel Objectives and on the basis of a simple majority).

Variations in respect of Section E

X2.4 Notwithstanding that Section E (Registration Data) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.4, apply as varied by this Section X2.4. The variations to apply pursuant to this Section X2.4 are that Section E (Registration Data) is to apply as if:

(a) the information to be provided under Sections E2.1 and E2.2 is (subject to Section X2.4(b)) in respect of each Metering Point or Supply Meter Point (as applicable):

(i) the MPAN or MPRN (as applicable);

(ii) the identity of the person Registered for that Metering Point or Supply Meter Point (as applicable);

(iii) the identity of the Gas Network Party for the network to which the Supply Meter Point relates;

(iv) whether or not the Metering Point has a status that indicates that it is

energised;

(v) whether or not the Supply Meter Point has a status that indicates that gas is offtaken at that point;

(vi) the profile class (as referred to in Section E2.1) relating to each such Metering Point; and

(vii) whether the Supply Meter Point serves a Domestic Premises or a Non-Domestic Premises;

(b) the information to be provided under Section E2.2 in respect of the period until the end of the 15th of September 2015 (or such later date as the Secretary of State may direct) is capable of being provided either by reference to MPRNs or by reference to 'Supply Point Registration Numbers' (as defined in the UNC);

(c) the text at Sections E2.3 and E2.4 (Obligation on the DCC to Provide Data) was deleted;

(d) the text at Section E2.5 (Frequency of Data Exchanges) was replaced with "The Data to be provided in accordance with this Section E2 shall be provided or updated on the last Working Day of each month (or as soon as reasonably practicable thereafter), so as to show the position as at the end of the 15th day of that month";

(e) the text at Section E2.6 (Frequency of Data Exchanges) was replaced with "The Data to be provided in accordance with this Section E2 shall be provided in such format, and shall be aggregated in such manner, as the DCC may reasonably require in order to enable the DCC to comply with its obligations under the DCC Licence or this Code"; and

(f) the text at Sections E2.7 to E2.11 (inclusive) and E2.13 was deleted .

Variations in respect of Section K

X2.5 Notwithstanding that Section K (Charging Methodology) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the

purposes of this Section X2.5, apply as varied by this Section X2.5. The variations to apply pursuant to this Section X2.5 are that:

(a) in respect of the Fixed Charges payable for each of the months up to and including November 2013 (or such later month as the Secretary of State may direct), the DCC shall calculate the Fixed Charges as if there were no Export Suppliers and as if all Export Suppliers were Import Suppliers (and the DCC shall not therefore require data in respect of such months pursuant to Section E2.1 that distinguishes between Import MPANs and Export MPANs); and

(b) insofar as the Registration Data provided to the DCC under Section E2.2 is by reference to 'Supply Points' (as defined in the UNC), rather than MPRNs, the DCC may calculate the number of Mandated Smart Metering Systems (as defined in Section K11.1) by reference to the number of such Supply Points.

Variations in respect of Section M

X2.6 Notwithstanding that Section M (General) is stated in Section X2.1 to be effective, it shall, until the date designated by the Secretary of State for the purposes of this Section X2.6, apply as varied by this Section X2.6. The variation to apply pursuant to this Section X2.6 is that Section M8.1(a) shall not apply.

General

X2.7 Where a Section is stated in this Section X2 to apply subject to more than one variation, then the Secretary of State may:

(a) designate different dates from which each such variation is to cease to apply; and/or

(b) designate a date from which one or more such variations are to cease to apply (without prejudice to the continued application of the other such variations).

X2.8 Before designating any dates for the purpose of this Section X2, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date. The requirement for consultation may be satisfied

by consultation before, as well as after, the designation of this Code.

X3 PROVISIONS TO BECOME EFFECTIVE FOLLOWING DESIGNATION

Effective Dates

X3.1 Each Section, Schedule and SEC Subsidiary Document (or any part thereof) not referred to in Section X2.1 or X2.2 shall only be effective from the date:

(a) set out or otherwise described in this Section X3; or

(b) designated in respect of that provision by the Secretary of State for the purpose of this Section X3.

X3.2 The following Sections, Schedules and Appendices shall be effective from the following dates (subject to the other provisions of this Section X):

(a) the following provisions of Section F (Smart Metering System Requirements) shall have effect as follows:

(i) Section F1 (Technical Architecture and Business Architecture Sub-Committee) shall have effect from the date on which this Code is first modified to include that Section;

(ii) Sections F4.1 (Operational Functionality), F4.2 to F4.4 (Interoperability with DCC Systems), F4.5 (Remote Access by the DCC), F4.6 and F4.7 (Physical Access to Devices by Parties) and F4.8 (Communications with Communication Hubs by DCC over the SM WAN) shall have effect from the date on which this Code is first modified to include this Section X3.2(a)(ii); and

(iii) Sections F4.10 to F4.14 (inclusive) (Communications Hub Procurement) shall have effect from the date on which this Code is first modified to include those Sections;

(b) Section F5 (Communications Hub Forecasting and Orders) shall have effect from the date designated by the Secretary of State for the purposes of this Section X3.2(b);

(c) Section F10 (Test Communications Hubs) shall have effect from the date on

which this Code is first modified to include that Section;

(d) Section G (Security) shall have effect from the date on which this Code is first modified to include that Section;

(e) Section I (Data Privacy) shall have effect from the date on which this Code is first modified to include Section I2 (Other User Privacy Audits);

(f) Sections H10.1 to H10.8 (inclusive) (Emergency Suspension of Services) shall have effect from the date on which this Code is first modified to include those Sections;

(g) Section H12 (Intimate Communications Hub Interface Specification) shall have effect from the date on which this Code is first modified to include this Section X3.2(g);

(h) Section H13 (Performance Reporting) shall have effect from the date on which this Code is first modified to include this Section X3.2(h);

(i) Section H14 (Testing Services) shall have effect as follows:

(i) Section H14.8 (General: Forecasting) shall have effect from the commencement of Interface Testing;

(ii) Section H14.11 (General: SMKI Test Certificates) shall have effect from the commencement of Systems Integration Testing; and

(iii) all the other provisions of Section H14 (Testing Services) shall have effect:

(A) in respect of the User Entry Process Tests, from the commencement of Interface Testing;

(B) in respect of the SMKI and Repository Entry Process Tests, from the date from which the SMKI and Repository Entry Process Tests can be commenced (as set out in the SRT Approach Document);

(C) in respect of Device and User System Testing, from the

commencement of End-to-End Testing;

(D) in respect of Modification Proposal implementation testing (as described in Section H14.34), from the date on which Modification Proposals that are neither Urgent Proposals nor Fast Track Modifications may first be raised under Section D (Modifications); and

(E) in respect of all other Testing Services, from the end of End-to-End Testing;

(j) Sections L1 (SMKI Policy Management Authority), L2 (SMKI Assurance), L4 (The SMKI Service Interface), L6 (The SMKI Repository Interface), L8 (SMKI Performance Standards and Demand Management), L9 (The SMKI Document Set) and L10 (The SMKI Recovery Procedure) shall have effect from the date on which this Code is first modified to include those Sections;

(k) Section N (SMETS1 Meters) shall have effect from the date on which this Code is first modified to include that Section;

(l) Section T (Testing During Transition) shall have effect from the date on which this Code is first modified to include that Section;

(m) Schedule 7 (Specimen Enabling Services Agreement) shall have effect from the date on which this Code is first modified to include that Schedule;

(n) Appendices A (SMKI Device Certificate Policy), B (SMKI Organisation Certificate Policy) and C (SMKI Compliance Policy) shall all have effect from the date on which this Code is first modified to include those Appendices; and

(o) Appendix F (Minimum Communication Services for SMETS1 Meters) shall have effect from the date on which this Code is first modified to include that Appendix.

Variations in respect of Section F

X3.3 Notwithstanding that Section F5 (Communications Hub Forecasting and Orders) is stated in Section X3.2 to be effective from a date to be designated, it shall apply once

effective as varied by this Section X3.3. For the purposes of this Section X3.3, the "**Initial Delivery Date**" shall be 1 November 2015 (or such later date as the Secretary of State may designate as such date for the purposes of this Section X3.3). The variations to apply pursuant to this Section X3.3 are that:

(a) each Supplier Party shall (and each other Party that intends to order Communications Hubs may), subject to any contrary timings specified by the Secretary of State on designating the date from which Section F5 is to have effect:

(i) submit its first Communications Hub Forecast during the month ending nine months in advance of the start of the month in which the Initial Delivery Date occurs;

(ii) submit further Communications Hub Forecasts on a monthly basis until the month ending five months in advance of the month in which the Initial Delivery Date occurs (from which time further Communications Hub Forecasts shall be submitted without reference to this Section X3.3); and

(iii) ensure that the Communications Hub Forecasts submitted pursuant to this Section X3.3 cover a 24-month period commencing with the month in which the Initial Delivery Date occurs;

(b) no Communications Order may specify a Delivery Date that is prior to the Initial Delivery Date;

(c) until 1 June 2015 (or such later date as the Secretary of State may direct for the purposes of this Section X3.3(c)):

(i) the DCC shall not be obliged to make the CH Ordering System available;

(ii) Parties shall submit the Communications Hub Forecasts required in accordance with Section X3.3(a) by a secure means of communication (as reasonably determined by the DCC) using the template made available by the DCC for such purposes (such template to be in a

readily available and commonly used electronic format);

(iii) the DCC shall accept Communications Hub Forecasts submitted by other Parties in accordance with Section X3.3(c)(ii), and shall take all reasonable steps to verify that the forecasts so submitted were submitted by the Party by which they are purported to have been submitted; and

(iv) the DCC shall make the following information available to other Parties (using a readily available and commonly used electronic format), in respect of each post code area within Great Britain:

(A) that the SM WAN is expected to be available within that post code area on the date from which the Enrolment Services first become available;

(B) where the SM WAN is not expected to be available within that post code area on that date but is expected to be available within that postcode area before 1 January 2021, the date from which the SM WAN is expected to first become available within that post code area; or

(C) that the SM WAN is not expected to be available within that post code area before 1 January 2021;and

(d) (until the following information is available via the Self-Service Interface) the DCC shall (using a readily available and commonly used electronic format) make information available to the other Parties concerning any requirement to use a particular WAN Variant (and, where applicable, in combination with any particular Communications Hub Auxiliary Equipment) for any given location in order that the Communications Hub will be able to establish a connection to the SM WAN (such information to be made available as far in advance of the date from which the SM WAN is expected to be available in that location as is reasonably practicable (and, in any event, at least 8 months in advance)).

X3.3A Notwithstanding that Section F1 (Technical Architecture and Business Architecture Sub-Committee) is stated in Section X3.2 to be effective, it shall apply as varied by

this Section X3.3A. The variation to apply pursuant to this Section X3.3A is that no review under Section F1.4(f) or F1.4(g) is required before the date from which Smart Meters are first capable of being Commissioned pursuant to Section H5 (Smart Metering Inventory and Enrolment Services).

Variations in respect of Sections G and I

X3.4 Notwithstanding that Sections G (Security) and I (Data Privacy) are stated in Section X3.2 to be effective, they shall apply as varied by this Section X3.4. The variations to apply pursuant to this Section X3.4 are that:

(a) the process to appoint the first User Independent Security Assurance Service Provider and the process to appoint the first Independent Privacy Auditor shall be run concurrently with the intent (subject to paragraph (ii) below) that one and the same person is appointed to carry out both such roles, but:

(i) for the avoidance of doubt, this requirement shall apply only in respect of the process to appoint the first person to carry out each such role; and

(ii) where it is not possible to appoint to both such roles one person who would be suitably independent (in accordance with Sections G8.7 and I2.4) in performing the functions under Sections G8 and I2 in respect of every Party, the Panel may designate another person to perform either such role to the extent necessary to ensure that a suitably independent person is available to perform those functions in relation to each Party; and

(b) the first annual SOC2 assessments pursuant to Section G9.3(b)(i) do not need to be completed until 12 months after the commencement of any Enrolment Services or Communications Services.

Variations in respect of Section L

X3.5 Notwithstanding that Section L8 (SMKI Performance Standards and Demand Management) is stated in Section X3.2 to be effective, it shall apply as varied by this Section X3.5. The variation to apply pursuant to this Section X3.5 is that Sections

L8.1 (SMKI Services: Target Response Times) to L8.6 (Code Performance Measures) will not apply until the Stage 2 Assurance Report has been published (or such later date as the Secretary of State may designate for the purposes of this Section X3.5.

Provisions to be Effective Subject to Variations

X3.6 In designating the date from which a provision of this Code is to be effective for the purpose of this Section X3, the Secretary of State may direct that such provision is to apply subject to such variation as is necessary or expedient in order to facilitate achievement of the Transition Objective (which variation may or may not be specified to apply until a specified date).

X3.7 Where the Secretary of State directs that a provision of this Code is to apply subject to such a variation, the Secretary of State may subsequently designate a date from which the provision is to apply without variation.

X3.8 Where the Secretary of State directs that a provision of this Code is to apply subject to more than one such variation, then the Secretary of State may:

(e) designate different dates from which each such variation is to cease to apply; and/or

(f) designate a date from which one or more such variations are to cease to apply (without prejudice to the continued application of the other such variations).

General

X3.9 Before designating any dates and/or making any directions for the purpose of this Section X3, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date and/or the draft direction (as applicable). Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date and/or the draft direction (as applicable).

X4 GOVERNANCE SET-UP ARRANGEMENTS

General

X4.1 The provisions of Section C (Governance) shall have effect subject to the provisions of this Section X4.

Elected Members

X4.2 The Elected Members to be appointed on the designation of this Code shall be the individuals nominated by the Secretary of State for the purposes of this Section X4.2 (chosen on the basis of the election process administered by the Secretary of State on behalf of prospective Parties prior to the designation of this Code).

X4.3 Of the persons appointed as Elected Members in accordance with Section X4.2:

(a) certain of them shall retire 12 months after the designation of this Code; and

(b) certain of them shall retire 24 months after the designation of this Code,

as specified in the document by which they are nominated by the Secretary of State for the purposes of Section X4.2.

Panel Chair

X4.4 There shall be no separate Panel Chair on the designation of this Code. The Panel Members shall select (and may deselect and reselect) from among the Elected Members a person to act as Panel Chair until a person is appointed as Panel Chair pursuant to Section X4.6.

X4.5 The Elected Member acting, from time to time, as Panel Chair in accordance with Section X4.4 shall retain his or her vote as a Panel Member, but shall have no casting vote as Panel Chair.

X4.6 The Panel shall appoint a separate Panel Chair by a date no later than five months after the designation of this Code. The Panel Chair shall be appointed in accordance with a process developed by the Panel for such purpose; provided that such process must be designed to ensure that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the appointment is conditional on the Authority approving the candidate;

(c) the Panel Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(d) the Panel Chair is remunerated at a reasonable rate;

(e) the Panel Chair's appointment is subject to Section C3.8 (Panel Member Confirmation) and terms equivalent to those set out in Section C4.6 (Removal of Elected Members); and

(f) the Panel Chair can be required to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her successor.

X4.7 Until such time as a separate Panel Chair has been appointed pursuant to Section X4.6, the Panel Chair shall only be entitled to appoint an additional Panel Member under Section C3.6 (Panel Chair Appointee) with the unanimous approval of the Panel.

DCC Member and Consumer Members

X4.8 The DCC Member and the Consumer Members to be appointed on the designation of this Code shall be the individuals nominated as such by the Secretary of State for the purposes of this Section X4.8.

Code Administrator and Secretariat

X4.9 The Panel shall, on the designation of this Code, be deemed to have appointed as Code Administrator and Secretariat such person or persons as the Secretary of State nominates for the purposes of this Section X4.9 (chosen on the basis of the procurement process administered by the Secretary of State on behalf of the prospective Panel prior to the designation of this Code).

X4.10 As soon as reasonably practicable following the designation of this Code, the Panel

shall direct SECCo to enter into contracts with such person or persons under which they are to perform the roles of Code Administrator and Secretariat. Such contracts shall be on terms and conditions approved by the Secretary of State for the purposes of this Section X4.10.

X4.11 Without prejudice to the ongoing duties of the Panel, the appointments of, and contracts with, the Code Administrator and Secretariat made in accordance with this Section X4 are deemed to have been properly made.

Recoverable Costs

X4.12 The requirement for Recoverable Costs to be provided for in, or otherwise consistent with, an Approved Budget (as set out in Section C8.2 (SEC Costs and Expenses)) shall not apply until such time as the first Approved Budget is established. The Panel shall establish the first Approved Budget (to cover the period from the designation of this Code) as soon as reasonably practicable following the designation of this Code.

X5 INCORPORATION OF CERTAIN DOCUMENTS INTO THIS CODE

Smart Metering Equipment Technical Specification

X5.1 The document designated by the Secretary of State as the Smart Metering Technical Specification in accordance with paragraph 27(b) Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and of this Section X5.1, be incorporated into this Code as the Schedule specified in such designation.

Communications Hub Technical Specification

X5.2 The document designated by the Secretary of State as the Communications Hub Technical Specification in accordance with paragraph 27(b) of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and this Section X5.2, be incorporated into this Code as the Schedule specified in such designation.

Certificate Policies

X5.3 Any document designated by the Secretary of State as a Certificate Policy in accordance with paragraph 27(c) of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and this Section X5.3, be incorporated into this Code as the Schedule or SEC Subsidiary Document specified in such designation.

Other Technical Specifications

X5.4 Each of the technical specifications and procedural or associated documents designated by the Secretary of State in accordance with paragraph 27(d) of Condition 22 of the DCC Licence shall, from the relevant date designated by the Secretary of State for the purpose of such document and this Section X5.4, be incorporated into this Code as the Schedule or SEC Subsidiary Document specified in such designation.

Re-Designation of Documents

X5.5 Paragraph 28(b) of Condition 22 of the DCC Licence includes a power for the Secretary of State to re-designate any document of a type referred to in Sections X5.1

to X5.4, subject to such amendments as he considers requisite or expedient. Where the Secretary of State exercises that power in relation to any such document:

(a) it shall be incorporated into this Code in substitution for the form of that document that was previously incorporated;

(b) the other provisions of this Section X5 shall apply to it as if it were a document being designated for the first time; and

(c) references in those provisions to the document being designated shall be read as referring to it being re-designated

Supplementary Provisions

X5.6 Paragraph 29 of Condition 22 of the DCC Licence includes a power for the Secretary of State to specify supplementary, incidental, consequential, governance or other provisions which are to have effect in this Code from the date designated for such purpose by the Secretary of State. This Code shall automatically be amended so as to include such provisions with effect from such date.

General

X5.7 This Code provides for the development of certain documents which may then be incorporated into this Code pursuant to this Section X5. Where this Code sets out the required purpose or content of such documents, the Secretary of State may designate for incorporation under this Section X5 documents that fulfil only part of that purpose or include only part of that content, with a view to subsequently re-designating more complete documents at a later date.

X5.8 The incorporation of documents into this Code pursuant to this Section X5 (and any provisions made pursuant to Section X5.6) shall not constitute a modification that should be subject to Section D (Modification Process). The incorporation of documents into this Code pursuant to this Section X5 (and any provisions made pursuant to Section X5.6) shall not constitute a variation of this Code that is time limited in accordance with Section X1.5 (and such documents and provisions shall remain part of this Code notwithstanding the deletion of this Section X on Completion of Implementation).

X5.9 The documents incorporated into this Code pursuant to this Section X5 (and any provision made pursuant to Section X5.6) shall, from the date of their incorporation, be subject to modification in accordance with the provisions of this Code.

X5.10 Before designating any dates for the purpose of this Section X5, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date. Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which to make representations or objections with respect to the proposed date to be designated. The requirement for consultation may be satisfied by consultation before, as well as after, the designation of this Code.

X5.11 Before designating any date from which a document is to be incorporated into this Code pursuant to this Section X5, the content of such document must have been subject to such consultation as the Secretary of State considers appropriate in the circumstances (whether or not under this Code, whether or not undertaken by the Secretary of State and whether before or after the designation of this Code).

X6 TRANSITIONAL VARIATIONS

Status of this Section X6

X6.1 This Section X6 is without prejudice to Section D (Modification Process), as (where applicable) varied pursuant to Section X2.

Secretary of State's Power to Vary for Purposes of Transition

X6.2 In pursuance of facilitating the achievement of the Transition Objective, the Secretary of State may direct that such provisions of this Code as the Secretary of State may specify are to apply subject to such variations as the Secretary of State may specify.

X6.3 Such a direction shall only be validly made if it specifies a date or dates from which the specified provision or provisions shall apply without variation. The Secretary of State may subsequently designate an earlier date from which the relevant provision is to apply without variation.

X6.4 The purposes for which such directions may be made includes purposes relating to the design, trialling, testing, set-up, integration, commencement and proving of the DCC Systems and the User Systems and the processes and procedures relating to the SEC Arrangements.

X6.5 The variations referred to in Section X6.2 may suspend the application of specified provisions of this Code and/or specify additional provisions to apply in this Code, and may include variations which:

(a) add additional limitations on Liability provided for in this Code;

(b) provide for indemnities against Liabilities to which a Party might be exposed; and/or

(c) provide for the referral to, and final determination by, the Secretary of State (or, where designated by the Secretary of State for such purposes, the Panel or the Authority) of certain Disputes.

General

X6.6 Before designating any dates and/or making any directions for the purpose of this

Section X6, the Secretary of State must consult the Authority, the Panel and the Parties in respect of the proposed date and/or the draft direction (as applicable). Such consultation must allow such period of time as the Secretary of State considers appropriate in the circumstances within which representations or objections may be made.

X7 TRANSITIONAL INCIDENT MANAGEMENT PROCEDURES

Period of Application

X7.1 This Section X7 shall have effect from the date on which this Code is first modified to include this Section X7.

X7.2 This Section X7 shall have effect until such time as the relevant enduring policy has been incorporated into this Code (or, if later, the time from which such policy is stated in Section X3 (Provisions to Become Effective following Designation) to have effect).

X7.3 For the purposes of Section X7.2, the relevant enduring policy is the Incident Management Policy.

X7.4 [Not used]

Transitional Provisions for Incident Management

X7.5 Each Party other than the DCC that has rights and/or obligations under those Sections referred to in the definition of Services (and which are effective in accordance with Section X3 (Provisions to Become Effective following Designation)) shall provide the DCC with an up-to-date list from time to time of nominated individuals who are authorised to log Incidents on behalf of such Party, including for each such individual suitable contact details as reasonably requested by the DCC.

X7.6 Each Network Party shall ensure that its Registration Data Provider provides the DCC with an up-to-date list from time to time of nominated individuals who are authorised to log Incidents on behalf of such Registration Data Provider, including for each such individual suitable contact details as reasonably requested by the DCC.

X7.7 The individuals identified from time to time pursuant to Section X7.5 or X7.6 in respect of each Party or Registration Data Provider shall be the "**Nominated Incident Contacts**" for that Party or Registration Data Provider.

X7.8 Each Party shall (and each Network Party shall ensure that its Registration Data Provider shall) comply with any reasonable request of the DCC in relation to the validation of the information provided by that Party (or that Registration Data Provider) in relation to its Nominated Incident Contacts.

X7.9 The DCC shall treat the information from time to time provided to it pursuant to Section X7.5 or X7.6 as Confidential Information.

X7.10 For those Parties and Registration Data Providers that have provided details of their Nominated Incident Contacts, the DCC shall provide a means by which Incidents can be reported to the DCC and information regarding Incidents sought from the DCC (the "**Interim Service Desk**"), which shall include (as a minimum) one or more email addresses and telephone numbers.

X7.11 The DCC shall ensure that the Interim Service Desk operates between 08.00 hours and 18.00 hours on Working Days.

X7.12 Parties and Registration Data Providers may report Incidents with the DCC by their Nominated Incident Contacts contacting the Interim Service Desk and providing their contact details, the nature of the Incident, the time and date of the occurrence, and the impact of the Incident.

X7.13 The DCC shall determine the prioritisation of Incidents, but subject to such prioritisation shall take all reasonable steps to mitigate and resolve each Incident such that its impact on Parties is minimised.

X7.14 The DCC shall have the right to assign reasonable actions to other Parties and/or the Registration Data Providers as reasonably required by the DCC in order to assist the DCC in mitigating and/or resolving one or more Incidents. Each Party shall (and each Network Party shall ensure that its Registration Data Provider shall) comply with any such actions so assigned to them.

X7.15 The DCC shall notify any Parties and Registration Data Providers likely to be affected by an Incident of which the DCC has become aware of: the occurrence of such Incident; its priority status; progress regarding its resolution; and its resolution. The DCC shall provide such notifications to the Nominated Incident Contacts. The DCC shall provide such notification of an Incident's resolution within one Working Day following its resolution.

X7.16 The DCC shall establish a process by which Nominated Incident Contacts can discuss with DCC the priority assigned to an Incident where a Party or Registration Data Provider disagrees with the prioritisation assigned to an Incident by the DCC.

Transitional Provisions Relating to Business Continuity and Disaster Recovery

X7.17 In the event that the Interim Service Desk is unavailable and is unlikely to resume availability within two Working Days, then the DCC shall establish an alternative means of communication by which Incidents can be reported to the DCC and information regarding Incidents sought from the DCC. Such alternative means of communication must include a telephone number that can be used to contact the DCC's Incident manager in the case of disaster events.

X7.18 In the event that an alternative means of communication is established by the DCC pursuant to Section X7.17, the DCC shall notify the Parties and the Registration Data Providers of such alternative means of communication. Such notification shall be given to the Nominated Incident Contacts via (as a minimum) email (or, if email is unavailable, SMS). Such a notification shall include a brief explanation of the reason for the Interim Service Desk's unavailability and the expected time by which it will be available as normal.

X7.19 Once the Interim Service Desk is available as normal (following a period of unavailability), the DCC shall notify the Parties and the Registration Data Providers that this is the case (such notification to be given to the Nominated Incident Contacts via (as a minimum) email).

X7.20 In the event of the Interim Service Desk being unavailable for two Working Days or more, the DCC shall (within five Working Days following the Interim Service Desk's return to normal availability) compile a report on such event setting out the cause and future mitigation. The DCC shall make any such report available to Parties, Registration Data Providers and the Panel (and, upon request, to the Authority or the Secretary of State).

X8 DEVELOPING CH SUPPORT MATERIALS

Overview

X8.1 The CH Support Materials are to be developed by the DCC pursuant to this Section X8.1, and incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the CH Support Materials

X8.2 The purpose of the CH Support Materials is to make provision for such matters as are specified in Sections F5 (Communications Hub Forecasting and Orders), F6 (Delivery and Acceptance of Communications Hubs), F7 (Installation and Maintenance of Communications Hubs), F8 (Removal and Return of Communications Hub), F9 (Categories of Communications Hub Responsibility), and F10 (Test Communications Hubs), and to provide further processes and detail required to facilitate the delivery, installation, maintenance and return of Communications Hubs and Test Communications Hubs pursuant to this Code.

Process to Develop Documents

X8.3 The DCC shall develop and consult on the CH Support Materials so that drafts of each document are submitted to the Secretary of State by 1 March 2015 (or by such later date as the Secretary of State may direct for the purposes of this Section X8.3).

X8.4 The procedure by which the DCC is to develop each of the documents comprising the CH Support Materials is as follows:

(a) the DCC shall, in consultation with the Parties and such other persons as are likely to be interested, produce a draft of each of the documents;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the documents, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the CH Support Materials;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the

Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft document, including:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

X9 ~~NOT USED~~INTERIM DEVICE AND USER SYSTEM TESTING

Interim Device Testing

X9.1 The DCC shall provide a testing service (referred to in this Section X9 as "**GFI Testing**") to enable eligible persons to test the interoperability of Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs to be provided as part of the Testing Services, such that those Devices are able to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification. The DCC shall provide GFI Testing with effect from as soon as reasonably practicable after this Section X9.1 takes effect, and (in any event) from the commencement of End-to-End Testing.

X9.2 The following shall apply in respect of GFI Testing:

(a) the following persons shall be eligible to undertake GFI Testing: Parties and persons that have signed agreements based on the Specimen Enabling Services Agreement (subject only to such variations from such specimen form as are reasonable in the circumstances, including so as to require compliance with this Section X9.2);

(b) the references in Section X9.1 to "Communications Hubs", "DCC Systems" and "Devices" shall be interpreted as including reference to prototypes or simulations of those things (and GFI Testing shall not include communication via the SM WAN, or a simulation of the SM WAN);

(c) Section H14 (Testing Services) shall apply in respect of GFI Testing as if GFI Testing was a Testing Service, and the DCC and each person undertaking GFI Testing shall comply with Sections H14 in respect of GFI Testing as if GFI Testing was a Testing Service (provided that none of the following shall apply: Sections H14.3, H14.4, H14.9, H14.10 and H14.11);

(d) persons undertaking GFI Testing must each comply with such supplemental obligations as the DCC may notify to them from time to time (provided that such obligations are not inconsistent with the provisions of the Code that are in effect at that time); and

(e) the Testing Issue process in Section H14.37 to H14.45 (General: Testing Issue Resolution Process) shall not apply to GFI Testing, but the DCC must take reasonable steps to provide support and assistance to a person undertaking GFI Testing in order to assist that person in resolving Testing Issues encountered when undertaking GFI Testing.

Pre-UEPT Testing

X9.3 The DCC shall provide a testing service (referred to in this Section X9 as "**Pre-UEPT Testing**") that enables Parties to test their capability (and that of their Systems) to undertake the following activities over a DCC Gateway Connection:

(a) the sending of (at least) the following Service Requests (which are identified by reference to the numbering used in the Common Test Scenarios Document):

(i) 4.1.1;

(ii) 5.1, 5.2 and 5.3;

(iii) 6.2.7, 6.11, 6.15.1, 6.15.2, 6.17, 6.20.1, 6.21 and 6.23;

(iv) 8.1.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7.1, 8.7.2, 8.8.1, 8.8.2, 8.9, 8.11, 8.12.1, 8.12.2, 8.13, 8.14.1, 8.14.2, 8.14.3 and 8.14.4; and

(v) 11.1, 11.2, 11.3, 12.1 and 12.2;

(b) the sending of one or more Signed Pre-Commands; and

(c) the receipt of Pre-Commands and Service Responses in respect of (at least) the Service Requests set out in paragraph (a) above (in the case of Pre-Commands, only to the extent those Service Requests are designed to generate Pre-Commands).

X9.4 The following shall apply in respect of Pre-UEPT Testing:

(a) the references in Section X9.3 to "Service Requests", "Signed Pre-Commands", "Pre-Commands", "Service Responses", "Device Alerts" and "DCC Alerts" shall be interpreted as including simulations of those things,

which simulations may:

(i) include standardised or sample Data; and

(ii) omit Certificates, GBCS Payloads, Digital Signatures or Message Authentication Codes that would otherwise be required;

(b) Section H14 (Testing Services) shall apply in respect of Pre-UEPT Testing as if Pre-UEPT Testing was a Testing Service, and the DCC and each Party undertaking Pre-UEPT Testing shall comply with Sections H14 in respect of Pre-UEPT Testing as if Pre-UEPT Testing was a Testing Service (provided that none of the following shall apply: Sections H14.3, H14.4, H14.9, H14.10 and H14.11);

(c) persons undertaking Pre-UEPT Testing must each comply with such supplemental obligations as the DCC may notify to them from time to time (provided that such obligations are not inconsistent with the provisions of the Code that are in effect at that time); and

(d) the Testing Issue process in Section H14.37 to H14.45 (General: Testing Issue Resolution Process) shall not apply to Pre-UEPT Testing, but the DCC must take reasonable steps to provide support and assistance to a Party undertaking Pre-UEPT Testing in order to assist that Party in resolving Testing Issues encountered when undertaking Pre-UEPT Testing.

Interaction with Device and User Systems Tests

X9.5 The DCC shall not provide (and no Party shall be entitled to undertake) any testing of Devices under Section H14.31(a) (Device and User System Tests) during the period (if any) between commencement of GFI Testing and commencement of End-to-End Testing.

X9.6 The DCC shall not provide (and no Party shall be entitled to undertake) any testing of Systems under Section H14.31(b) (Device and User System Tests) during the period between commencement of Pre-UEPT Testing and commencement of End-to-End Testing.

X9.7 The DCC shall continue to make the tests under this Section X9 available following the commencement of End-to-End Testing.

X10 THRESHOLD ANOMALY DETECTION PROCEDURES

Overview

X10.1 The Threshold Anomaly Detection Procedures are to be developed by the DCC pursuant to this Section X10.1, and incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the Threshold Anomaly Detection Procedures

X10.2 The purpose of the Threshold Anomaly Detection Procedures is to make provision for such matters as are described in Section G6.1 (Threshold Anomaly Detection Procedures), and to provide further processes and detail required to facilitate those matters.

Process to Develop Document

X10.3 The DCC shall develop and consult on the Threshold Anomaly Detection Procedures in accordance with Section X10.4, and submit the document to the Secretary of State by no later than the date which falls seven months prior to the commencement of Interface Testing (or by such later date as the Secretary of State may direct).

X10.4 The procedure by which the DCC is to develop the Threshold Anomaly Detection Procedures is as follows:

(a) the DCC shall, in consultation with the Parties and such other persons as are likely to be interested, produce a draft of the document;

(b) where a disagreement arises with any Party or other person with regard to any proposal as to the content of the document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the Threshold Anomaly Detection Procedures;

(c) the DCC shall send a draft of Threshold Anomaly Detection Procedures to the Secretary of State as soon as is practicable after completion of the process described in (a) and (b) above, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft to be fit for purpose;

(ii) copies of the consultation responses received; and

(iii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal; and

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft document, including:

(i) any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

SECTION Z: THE ALT HAN ARRANGEMENTS

Z1 THE ALT HAN FORUM

Establishment of the Alt HAN Forum

Z1.1 The Alt HAN Forum (the **Forum**) is hereby established.

Z1.2 The Forum shall:

(a) pursue the objectives, carry out the functions and have the powers set out in Sections Z1.3 to Z1.5;

(b) have the composition described in Sections Z1.6 to Z1.12;

(c) conduct its activities in accordance with the procedures set out in Sections Z1.13 to Z1.40;

(d) have the ability to establish, and to delegate its duties, powers and functions to, Sub-Groups in accordance with Sections Z1.41 to Z1.59,

and appeals from decisions of the Forum may be made to the Authority in accordance with Sections Z1.60 to Z1.66.

Forum Objectives, Functions and Powers

Forum Objectives

Z1.3 The Forum shall, in the performance of its functions and exercise of its powers, always act in a manner designed to achieve the objectives (the **Forum Objectives**) that:

(a) by virtue of the operation of this Section Z, Relevant Supplier Parties are able to comply with their obligations under Standard Condition 55.2 of the Electricity Supply Licence and Standard Condition 49.2 of the Gas Supply Licence;

(b) the Alt HAN Arrangements are given effect so as:

(i) to facilitate the economic and efficient acquisition of Alt HAN Service Capacity and provision of the Alt HAN Services;

(ii) to facilitate competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy;

(iii) to ensure that Energy Consumers' experience of the installation of Alt HAN Equipment at their premises is consistent with their reasonable expectations;

(iv) to ensure that all activities undertaken by or on behalf of Relevant Supplier Parties in relation to the installation, operation, maintenance, removal and replacement of Alt HAN Equipment are carried out in a fair, transparent, appropriate and professional manner;

(v) to ensure the protection of Data and the security of Data and Systems used for the purpose of the acquisition of Alt HAN Service Capacity and provision of the Alt HAN Services; and

(vi) to ensure that the Alt HAN Arrangements are administered in an economic, efficient and transparent manner; and

(c) the Forum conducts its affairs in an open and transparent manner.

Forum Functions

Z1.4 The Forum shall, in accordance with the provisions of this Section Z:

(a) make all decisions required for the purpose of the acquisition of Alt HAN Service Capacity and provision of the Alt HAN Services, except for any decisions which may from time to time be delegated by it to AltHANCo or any Forum Sub-Group;

(b) determine which (if any) decisions are to be delegated to AltHANCo or any Forum Sub-Group;

(c) give such directions to AltHANCo or any Forum Sub-Group as the Forum may consider appropriate (which may include directions in relation to any

decisions otherwise delegated by the Forum);

(d) approve the annual budget of AltHANCo;

(e) determine any appeals made to it from decisions made by AltHANCo or a Forum Sub-Group; and

(f) make such other decisions as may from time to time be required in accordance with the provisions of this Section Z.

Forum Powers

Z1.5 Without prejudice to any other rights or powers granted to the Forum in this Section Z, the Forum shall, in accordance with the provisions of this Section Z, have the power to:

(a) make written representations in relation to the purpose or effect of any Modification Proposal which:

(i) is likely to affect this Section Z;

(ii) is likely to affect the provisions relating to the Alt HAN Charges at Section K (Charging Methodology);

(iii) relates to other parts of the Code, but may have a material effect on the Alt HAN Arrangements;

(b) appoint and remove professional advisers;

(c) consider, approve and authorise the entering into by AltHANCo of contracts; and

(d) do anything else necessary for, or reasonably incidental to, the fulfilment of its functions under this Section Z.

Forum Membership

Appointment of Members

Z1.6 Each Relevant Supplier Party:

(a) shall nominate one person to represent it in the Forum; and

(b) may at any time nominate a different person for that purpose, in replacement for any person previously nominated,

where all such nominations shall be made in writing to the Alt HAN Secretariat, and the Forum shall be composed of each of the persons (**Forum Members**) who are from time to time so nominated by the Relevant Supplier Parties.

Z1.7 A person may be nominated as a Forum Member by, may represent, and may vote on behalf of any two or more Relevant Supplier Parties (but shall not be entitled to exercise any rights to vote in such manner as to vote for more than one outcome in respect of any resolution).

Z1.8 Each Forum Member must be an individual, and cannot be a body corporate, association or partnership.

Election of Forum Chair and Alternate Chair

Z1.9 The Forum Members:

(a) shall, as the first item of business at the first meeting of the Forum, elect one person to serve as chair of the Forum (the **Forum Chair**) and one person to serve as alternate to the chair of the Forum (the **Alternate Chair**); and

(b) may at any subsequent time elect a different person to either role, in replacement for any person previously elected.

Z1.10 The Forum Chair and Alternate Chair may each be a Forum Member or any other person on whose appointment to such role the Forum is resolved.

Z1.11 The Forum may decide that the person elected as the Forum Chair (or, where that person is in employment, his or her employer) shall be compensated for such time as he or she spends performing the role of the Forum Chair in such amount, or at such rate, as the Forum may determine.

Z1.12 Notwithstanding the provisions of Section Z1.25, the election of a Forum Chair and Alternate Chair shall be by a simple majority vote of Forum Members present at the

meeting at which that election takes place, each Forum Member being entitled to exercise a single vote.

Proceedings of the Forum

Meetings of the Forum

Z1.13 The Forum shall hold meetings with such frequency as it may determine or the Forum Chair may direct, but in any event shall meet as often as necessary in order to ensure the efficient performance of its functions, and at least once in every two month period.

Z1.14 The location and timing of each meeting shall be determined by the Forum or, where no such determination has been made, by the Forum Chair.

Z1.15 Forum Members may attend a meeting by telephone conference or other technological means (provided that each Forum Member attending the meeting acknowledges that he or she can communicate with each of the others).

Z1.16 Subject to the other provisions of this Section Z, the Forum may regulate the conduct of its meetings as it sees fit.

Alternates

Z1.17 Each Forum Member may, in each case by notice in writing to the Alt HAN Secretariat, appoint another person from time to time to act as his or her alternate.

Z1.18 Where a Forum Member does not attend a Forum meeting, his or her alternate shall be entitled to attend (and count, in the capacity of alternate, towards the quorum at) that meeting, and to exercise all of the functions and powers of the Forum Member at that meeting.

Z1.19 A person appointed as an alternate by any Forum Member:

(a) shall immediately cease to be an alternate if the appointing person ceases to be a Forum Member; and

(b) may be removed or replaced by that Forum Member from time to time, by notice in writing to the Alt HAN Secretariat.

Z1.20 A person may be appointed as an alternate by:

(a) a Forum Member who represents two or more Relevant Supplier Parties; or

(b) two or more Forum Members,

but in either case shall not be entitled to exercise any rights to vote in such manner as to vote for more than one outcome in respect of any resolution.

Z1.21 Unless the context otherwise requires, any reference in this Section Z to:

(a) a Forum Member shall be construed as including a reference to that Forum Member's alternate;

(b) the Forum Chair shall be construed as including, where the Forum is Chair is unable to be available to perform his or her role, a reference to the Alternate Chair.

Quorum and Attendance of the Forum Chair

Z1.22 No decision may be made at any meeting of the Forum unless:

(a) that meeting is quorate, which shall be treated as being the case only if either:

(i) at least one half of all Forum Members nominated at that time are present at that meeting; or

(ii) the Forum Members who are present at that meeting are entitled to exercise at least two-thirds of the votes available to be cast; and

(b) the Forum Chair is present at that meeting.

Forum Chair

Z1.23 The Forum Chair shall preside at every meeting of the Forum and, if he or she is unable to attend any meeting, shall ensure that the Alternate Chair attends the meeting to act as Forum Chair.

Voting

Z1.24 Each Forum Member shall be entitled to attend, and to speak and vote, at every meeting of the Forum.

Z1.25 All decisions of the Forum shall be by resolution. Subject to Section Z1.12, in order for a resolution of the Forum to be passed at a meeting, a weighted majority of Forum Members present at that meeting must vote in favour of that resolution.

Z1.26 For these purposes:

(a) a number of votes shall be attributed to each Relevant Supplier Party in accordance with Sections Z1.27 to Z1.29 (the **Supplier Weighted Vote**); and

(b) each Forum Member shall be entitled to exercise a number of votes corresponding to the aggregate of the Supplier Weighted Votes of the Relevant Supplier Parties which that Forum Member represents.

Z1.27 Where one or more Supplier Parties have been notified by the DCC that Alt HAN Charges are payable in respect of all or any part of the Relevant Preceding Period, the Supplier Weighted Vote for each Relevant Supplier Party shall be calculated as follows:

$$SWV_p = \frac{AHC_{RPP}}{TAHC_{RPP}} \times 1000$$

Where:

SWV_p means the Supplier Weighted Vote for that Relevant Supplier Party;

AHC_{RPP} means the Alt HAN Charges that were payable by that Relevant Supplier Party in respect of the Relevant Preceding Period, as calculated by the DCC in accordance with the Charging Methodology;

$TAHC_{RPP}$ means the total amount of the Alt HAN Charges that were payable by all Relevant Supplier Parties in respect of the Relevant Preceding Period, as calculated by the DCC in accordance with the Charging Methodology.

Z1.28 Where the circumstances described in Section Z1.27 do not apply, the Supplier Weighted Vote for each Relevant Supplier Party shall be calculated as follows:

$$SWV_p = \frac{MPxN_p}{MPxN_{All_p}} \times 1000$$

Where:

SWV_p means the Supplier Weighted Vote for that Relevant Supplier Party;

$MPxN_p$ means the total number of MPANs and MPRNs related to Smart Metering Systems at Domestic Premises for which the Relevant Supplier Party was the Responsible Supplier at 24:00 on the last day of the Relevant Preceding Period;

$MPxN_{All_p}$ means the sum of the values of $MPxN_p$ for all Relevant Supplier Parties.

Z1.29 For the purposes of Sections Z1.27 and Z1.28:

(a) in calculating the Supplier Weighted Vote, any fraction of a number of votes shall be rounded to the nearest whole number (and 0.5 of a vote shall be rounded upwards);

(b) the Supplier Weighted Vote shall never have a value less than 1 (one); and

(c) the **Relevant Preceding Period** shall be:

(i) in relation to any vote at a Forum meeting taking place in the period between 1 June and 30 November (inclusive) in any year, the month of April falling immediately prior to the start of that period; and

(ii) in relation to any vote at a Forum meeting taking place in the period between 1 December in any year and 31 May in the following year, the month of October falling immediately prior to the start of that period.

Z1.30 A resolution put to a vote at a Forum meeting shall be passed if the number of votes in favour of that resolution correspond to more than 50% of the total number of votes

which all Forum Members attending that meeting are entitled to exercise.

Z1.31 The voting process, counting of votes, and calculation of Supplier Weighted Votes in respect of all resolutions which are required to be passed by a weighted majority of Forum Members shall take place in accordance with the Forum Voting Protocol. The Forum Voting Protocol may specify obligations on any Parties to provide information, or otherwise take any steps, for the purpose of facilitating that process, count or calculation.

Meeting Notice and Papers

Z1.32 Each meeting that the Forum determines, or the Forum Chair directs, is to be held shall be convened by the Alt HAN Secretariat. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Forum may approve). Such notice shall be given to:

(a) each of the Forum Members (and any appointed alternates);

(b) each of the persons referred to in Section Z1.36; and

(c) each of the Relevant Supplier Parties.

Z1.33 The notice of each Forum meeting shall contain or be accompanied by a statement of the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and any supporting papers.

Z1.34 The agenda for each Forum meeting shall include any such matters as:

(a) the Forum has determined;

(b) the Forum Chair has directed, or

(c) any two or more Relevant Supplier Parties (not being Parties which have the

same ultimate holding company) have requested for inclusion.

Z1.35 The proceedings of a Forum meeting shall not be invalidated by the accidental omission to give notice of the meeting to (or non-receipt of that notice by) any person entitled to receive it.

Attendance by Other Persons

Z1.36 One representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Forum:

(a) the Secretary of State;

(b) the Authority; and

(c) any other person that the Forum determines, or the Forum Chair directs, should be invited to attend.

Z1.37 The Forum Chair may (at his or her discretion on grounds of confidentiality) exclude from any part of a Forum meeting any person admitted pursuant to Section Z1.36(c).

Minutes of Forum Meetings

Z1.38 The Alt HAN Secretariat shall, within 10 Working Days of each Forum meeting, circulate copies of the minutes of that meeting to each of the Forum Members, the Secretary of State and the Authority.

Z1.39 If any Forum Member, the Secretary of State or the Authority disagrees with any item in the minutes, he or she shall at the next Forum meeting notify the Forum Chair of the matters which are the cause of the disagreement, and those matters shall be discussed at that meeting.

Z1.40 The Alt HAN Secretariat shall maintain a record of all resolutions voted on by the Forum, which shall indicate how each Forum Member voted on each resolution and (where applicable) what voting share was attributable to that Forum Member at that meeting, and shall make such record available on request to any Relevant Supplier Party, the Secretary of State and the Authority.

Forum Sub-Groups

Establishing Forum Sub-Groups

Z1.41 The Forum may establish committees (**Forum Sub-Groups**) for the purposes of doing or assisting the Forum in doing anything to be done by the Forum pursuant to this Section Z.

Z1.42 The Forum may establish a Forum Sub-Group on a standing basis or for a fixed period or a finite purpose.

Z1.43 The Forum may decide that any Forum Sub-Group is to be dissolved.

Z1.44 The Forum may delegate to any Forum Sub-Group such of the duties, powers and functions of the Forum as the Forum may specify.

Membership of Forum Sub-Groups

Z1.45 Each Forum Sub-Group shall be composed of such persons of suitable experience and qualifications as the Forum shall decide and as are willing to serve thereon (**Forum Sub-Group Members**), which may include any Forum Member.

Z1.46 Each Forum Sub-Group Member must be an individual, and cannot be a body corporate, association or partnership.

Z1.47 Before establishing any Forum Sub-Group, the Forum shall invite (by such means as it considers appropriate) applications from individuals who wish to serve on the Forum Sub-Group.

Z1.48 Once a Forum Sub-Group has been established, the Forum may admit such additional persons as Forum Sub-Group Members, or remove any person from being a Forum Sub-Group Member, as the Forum considers appropriate (including on the application of any Relevant Supplier Party or any existing Forum Sub-Group Member).

Z1.49 Each Forum Sub-Group Member shall, when acting in that capacity:

(a) act independently, not as a delegate, and without undue regard to the interests of any Related Person; and

(b) act in a manner designed to facilitate the performance by the Forum of its duties under this Section Z.

Z1.50 Each person appointed as a Forum Sub-Group Member must confirm in writing to the Alt HAN Secretariat (for the benefit of AltHANCo and each Relevant Supplier Party) that that person:

(a) agrees to act as a Forum Sub-Group Member in accordance with this Section Z, including the requirements of Section Z1.49; and

(b) will be available as reasonably required throughout his or her term of office both to attend Forum Sub-Group meetings and to undertake work outside those meetings as may reasonably be required.

Z1.51 The Forum may, either generally or in relation to specific cases, approve:

(a) the payment to a Forum Sub-Group Member (or, where that person is in employment, his or her employer) of compensation for such time as he or she spends performing the role of a Forum Sub-Group Member; and

(b) the amount, rate, or means of calculation of such payment.

Terms of Reference and Procedure of Forum Sub-Groups

Z1.52 The Forum shall set out in writing any such duties, powers and functions of the Forum as it has delegated to each Forum Sub-Group.

Z1.53 The Forum shall specify in writing the terms of reference and procedural rules that are to be followed by each Forum Sub-Group (which may be revised from time to time by the Forum).

Z1.54 Save to the extent otherwise specified by the Forum, a Forum Sub-Group shall conduct its business in such manner as it considers appropriate.

Z1.55 No Forum Sub-Group may delegate any of its duties, powers or functions unless it has been expressly authorised to do so by the Forum.

Z1.56 Any resolutions of a Forum Sub-Group shall:

(a) only have binding effect as a decision of the Forum if the Forum has formally delegated the required decision-making power to that Forum Sub-Group; and

(b) within 10 Working Days of the date of the resolution be notified by the Forum Sub-Group, by means of the Alt HAN Secretariat, to each Relevant Supplier Party.

Appeals from Decisions of a Forum Sub-Group

Z1.57 A Relevant Supplier Party may appeal to the Forum any decision of a Forum Sub-Group which otherwise has binding effect as a decision of the Forum.

Z1.58 An appeal under Section Z1.57 will only be validly made if it is notified to the Alt HAN Secretariat within 20 Working Days of the date on which the Forum Sub-Group made the decision which is subject to appeal.

Z1.59 Where a decision of a Forum Sub-Group is appealed:

(a) the decision shall be treated as having no effect; and

(b) the Forum shall make the decision afresh, which shall then have effect for the purposes of this Section Z in substitution for the decision of the Forum Sub-Group.

Appeals from Decisions of the Forum

Z1.60 A Relevant Supplier Party may appeal to the Authority any decision of the Forum on the ground that it is inconsistent with the Forum Objectives.

Z1.61 An appeal under Section Z1.60 will only be validly made if:

(a) it is notified to the Authority within 30 Working Days of the date on which the Forum made the decision which is subject to appeal;

(b) a copy of the notice is given to the Alt HAN Secretariat on the same date on which it is sent to the Authority; and

(c) the notice specifies why the Relevant Supplier Party which is bringing the appeal considers that the decision which is subject to appeal is inconsistent

with the Forum Objectives.

Z1.62 Where the Alt HAN Secretariat is notified of an appeal, it shall arrange for a copy of the notice of appeal to be provided to all Relevant Supplier Parties.

Z1.63 The Authority may adopt such process and procedure as it thinks fit in relation to the determination of any appeal, and may give interim directions as to the effect of the decision being appealed prior to the appeal being determined.

Z1.64 The Forum shall provide such information, support and assistance to the Authority in relation to the determination of any appeal as the Authority may reasonably request.

Z1.65 Where the Authority considers that the Relevant Supplier Party which brought the appeal:

(a) has failed to establish that the decision being appealed is inconsistent with the Forum Objectives, it shall uphold the decision; or

(b) has established that the decision being appealed is inconsistent with the Forum Objectives, it may:

(i) quash the decision;

(ii) remit the decision to be remade by the Forum; and/or

(iii) substitute its own decision for that of the Forum, which shall then have effect for the purposes of this Section Z as if it had been a decision of the Forum.

Z1.66 Any decision of the Authority in relation to a matter appealed to it under Section Z1.60 shall be final and binding for the purposes of this Section Z.

Z2 THE ALT HAN COMPANY

Establishment of AltHANCo

Z2.1 The Alt HAN Company (**AltHANCo**) shall be established in accordance with the Annex to this Section Z.

Z2.2 AltHANCo shall act as a corporate vehicle in relation to the business of the Forum, including entering into any contractual arrangements in order to give effect to any resolution of the Forum which it is necessary or desirable to implement by means of a binding contract.

Z2.3 AltHANCo shall pursue the objectives, fulfil the duties and have the powers set out in Sections Z2.5 to Z2.7, and all decisions on behalf of AltHANCo shall be made by the board of directors of AltHANCo (the **Board**).

Z2.4 The Board shall:

(a) have the membership described in Sections Z2.8 to Z2.22; and

(b) conduct its activities in accordance with the procedures set out in Sections Z2.23 to Z2.45,

and appeals from decisions of the Board may be made to the Forum in accordance with Sections Z2.46 to Z2.48.

AltHANCo Objectives, Duties and Powers

AltHANCo Objectives

Z2.5 AltHANCo shall, in the discharge of its duties and exercise of its powers, always act in a manner designed to achieve the objectives (the **AltHANCo Objectives**) that:

(a) the Forum Objectives are achieved;

(b) this Section Z is given effect in a fair manner without undue discrimination between the Relevant Supplier Parties or classes of Relevant Supplier Party; and

(c) AltHANCo conducts its affairs in an open, transparent and efficient manner.

AltHANCo Duties

Z2.6 AltHANCo shall, in accordance with the provisions of this Section Z:

(a) make all such decisions as may be delegated to it from time to time by the Forum;

(b) undertake such activities as are necessary for the purpose of giving effect to the decisions of the Forum;

(c) comply with any directions given to it by the Forum; and

(d) undertake such other activities and make such other decisions as may from time to time be required in accordance with the provisions of this Section Z.

AltHANCo Powers

Z2.7 Without prejudice to any other rights or powers granted to AltHANCo in this Section Z, AltHANCo shall, in accordance with the provisions of this Section Z, have the power:

(a) where the Forum has so resolved, to pay compensation to the Forum Chair (or to his or her employer) for such time as he or she spends performing the role of the Forum Chair in such amount, or at such rate, as the Forum has determined;

(b) where the Forum has approved the payment of compensation to any Forum Sub-Group Member (or his or her employer) for time spent performing the role of a Forum Sub-Group Member, to pay compensation to that Forum Sub-Group Member in such amount, at such rate or in accordance with such means of calculation as the Forum has approved;

(c) to appoint and remove professional advisers;

(d) to enter into contracts; and

(e) to do anything else necessary for, or reasonably incidental to, the discharge of

its duties under this Section Z.

Board Membership

Board Composition

Z2.8 The Board shall be composed of the following categories of person (each a **Board Member**):

(a) five persons elected by the Large Relevant Supplier Parties; and

(b) two persons elected by the Small Relevant Supplier Parties.

Z2.9 Each Board Member must be an individual, and cannot be a body corporate, association or partnership.

Election of Board Members

Z2.10 The first Board Members to be appointed shall be the persons elected following an election process administered by the Secretary of State prior to this Section Z coming into effect.

Z2.11 Of the persons appointed in accordance with Section Z2.8:

(a) three of them shall retire 12 months after this Section Z comes into effect; and

(b) four of them shall retire 24 months after this Section Z comes into effect,

as specified by the Secretary of State in a notice informing them of their appointment as Board Members following the election process referred to in that Section.

Z2.12 Each Board Member shall serve as such until his or her retirement in accordance with Section Z2.16 or resignation or removal in accordance with Sections Z2.17 and Z2.18.

Z2.13 The Board shall produce, and submit to the Forum, the draft of a document setting out the process by which Board Members are to be elected following the retirement, resignation or removal of those appointed in accordance with Section Z2.10.

Z2.14 The Forum:

(a) shall, subject to such amendments as it may determine, adopt the document produced by the Board which (in the form in which it is adopted) shall be known as the **AltHANCo Election Protocol**; and

(b) may from time to time determine to modify the AltHANCo Election Protocol in such manner as it may consider appropriate.

Z2.15 The election of Board Members following the retirement, resignation or removal of those appointed in accordance with Section Z2.8 shall be conducted in accordance with the version of the AltHANCo Election Protocol which is in effect at that time.

Retirement of Board Members

Z2.16 Subject to earlier resignation or removal from office in accordance with Sections Z2.17 and Z2.18, and without prejudice to his or her ability to stand for re-election, each Board Member shall retire (at which point his or her office shall become vacant) as follows:

(a) a Board Member appointed in accordance with Section Z2.10 shall retire in accordance with the terms of the appointment specified by the Secretary of State under Section Z2.11; and

(b) a Board Member appointed following a subsequent election shall retire 24 months after that appointment took effect.

Resignation and Removal of Board Members

Z2.17 A Board Member may:

(a) resign his or her office on giving 10 Working Days' notice in writing to the Alt HAN Secretariat;

(b) be removed from office by the AltHANCo Chair on notice to the Alt HAN Secretariat if the Board Member fails to attend in person at least half of the Board meetings held in any period of 12 months; and

(c) be removed from office by the other Board Members (acting unanimously) on notice to the Alt HAN Secretariat if those other Board Members consider that

he or she is in breach of the confirmation that was given in accordance with Section Z2.20.

Z2.18 A Board Member shall automatically be removed from office if he or she:

(a) dies;

(b) is admitted to hospital in pursuance of an application under the Mental Health Act 1983 or the Mental Health (Care and Treatment) (Scotland) Act 2003, or an order is made by a court with competent jurisdiction in matters concerning mental disorder for his detention or for the appointment of a receiver, curator bonis or other person with respect to his or her property or affairs;

(c) becomes bankrupt or makes any arrangement or composition with his or her creditors;

(d) becomes prohibited by law from being a director of a company under the Companies Act 2006; or

(e) is convicted of an indictable criminal offence.

Duties of Board Members

Z2.19 A person appointed as a Board Member, when acting in that capacity, shall:

(a) act independently, not as a delegate, and without undue regard to the interests of any Related Person;

(b) exercise reasonable skill and care to the standard reasonably expected of a director of a company under the Companies Act 2006; and

(c) act in a manner designed to facilitate the performance by AltHANCo of its duties under this Section Z.

Board Member Confirmation

Z2.20 Each person elected as a Board Member must confirm in writing to the Alt HAN Secretariat (for the benefit of AltHANCo and each Relevant Supplier Party) that that person:

(a) agrees to act as a Board Member in accordance with this Section Z, including the requirements of Section Z2.19;

(b) agrees to accept appointment as a director of AltHANCo, and to act in such capacity in accordance with this Section Z; and

(c) will be available as reasonably required throughout his or her term of office both to attend Board meetings and to undertake work outside those meetings as may reasonably be required,

and must further complete any and all forms required to be completed by law in order for that person to become a director of AltHANCo.

Z2.21 The appointment of a person who would otherwise be a Board Member shall lapse (and the relevant office shall become vacant) if that person does not comply with the requirements of Section Z2.20 within 20 Working Days after a request from the Alt HAN Secretariat to do so.

Notification of Related Persons

Z2.22 Each Board Member shall, as soon as reasonably practicable after his or her election and upon any later relevant change in circumstance, disclose in writing to the Alt HAN Secretariat, the name of each Related Person who is a Relevant Supplier Party or is otherwise likely to be materially affected by the Alt HAN Arrangements (other than in the capacity of Energy Consumer).

Proceedings of the Board

Appointment of the Chair

Z2.23 The Board Members:

(a) shall, as the first item of business at the first meeting of the Board, elect from among them one person to serve as chair of AltHANCo (the **Chair**); and

(b) may at any subsequent time elect from among them a different person for that purpose, in replacement for any person previously elected.

Meetings of the Board

Z2.24 The Board shall hold meetings with such frequency as it may determine or the Chair may direct, but in any event shall meet as often as necessary in order to ensure the efficient discharge of its duties, and at least once in every two month period.

Z2.25 The location and timing of each meeting shall be determined by the Board or, where no such determination has been made, by the Chair.

Z2.26 Board Members may attend a meeting by telephone conference or other technological means (provided that each Board Member attending the meeting acknowledges that he or she can communicate with each of the others).

Z2.27 Subject to the other provisions of this Section Z (including the Annex), the Board may regulate the conduct of its meetings as it sees fit.

Alternates

Z2.28 The Chair shall, and each other Board Member may, in each case by notice in writing to the Alt HAN Secretariat, appoint another person from time to time to act as his or her alternate.

Z2.29 Where a Board Member does not attend a Board meeting, his or her alternate shall be entitled to attend (and count, in the capacity of alternate, towards the quorum at) that meeting, and to exercise all of the functions and powers of the Board Member at that meeting.

Z2.30 A person appointed as an alternate by any Board Member:

(a) shall immediately cease to be an alternate if the appointing person ceases to be a Board Member; and

(b) may be removed or replaced by that Board Member from time to time, by notice in writing to the Alt HAN Secretariat.

Z2.31 Unless the context otherwise requires, any reference in this Section Z to a Board Member shall be construed as including a reference to that Board Member's alternate.

Quorum

Z2.32 No decision may be made at any meeting of the Board unless a quorum is present, and the quorum at each meeting of the Board shall be four, at least one of whom must be the Chair.

The Chair

Z2.33 The Chair shall preside at every meeting of the Board and, if he or she is unable to attend any meeting, shall ensure that his or her alternate attends the meeting to act as Chair.

Voting

Z2.34 Each Board Member shall be entitled to attend, and to speak and vote, at every meeting of the Board.

Z2.35 All decisions of the Board shall be by ordinary resolution, passed by a simple majority of Board Members present at the meeting at which the vote takes place.

Z2.36 For these purposes the Chair shall be entitled to vote, and if the votes are tied shall have a second and casting vote.

Meeting Notice and Papers

Z2.37 Each meeting that the Board determines, or the Chair directs, is to be held shall be convened by the Alt HAN Secretariat. Such meeting shall be convened on at least 5 Working Days' advance notice (or such shorter period as the Board may approve). Such notice shall be given to:

(a) each of the Board Members (and any appointed alternates);

(b) each of the persons referred to in Section Z2.40; and

(c) each Relevant Supplier Party.

Z2.38 The notice of each Board meeting shall contain or be accompanied by a statement of the following:

(a) the time, date and location of the meeting;

(b) the arrangements for those wishing to attend the meeting by telephone conference or other technological means; and

(c) an agenda and any supporting papers.

Z2.39 The proceedings of a Board meeting shall not be invalidated by the accidental omission to give notice of the meeting to (or non-receipt of that notice by) any person entitled to receive it.

Attendance by Other Persons

Z2.40 One representative from each of the following persons shall be entitled to attend and speak (but not vote) at any meeting of the Board:

(a) the Secretary of State;

(b) the Authority; and

(c) any other person that the Board determines, or the Chair directs, should be invited to attend.

Z2.41 Any Relevant Supplier Party shall be entitled to send a representative to attend a Board meeting provided that the Relevant Supplier Party gives the Alt HAN Secretariat notice of its intention to do so at least 3 Working Days' notice in advance of that meeting (or such shorter period of notice as the Chair may approve). Such a representative shall be entitled to attend and (at the Chair's invitation) speak (but in no circumstances vote) at the meeting.

Z2.42 The Chair may (at his or her discretion on grounds of confidentiality) exclude from any part of a Forum meeting any person admitted pursuant to Section Z2.40(c).

Minutes of Board Meetings

Z2.43 The Alt HAN Secretariat shall, within 10 Working Days of each Board meeting, circulate copies of the minutes of that meeting to each of the Board Members, each Relevant Supplier Party, the Secretary of State and the Authority.

Z2.44 If any Board Member disagrees with any item in the minutes, he or she shall at the next Board meeting notify the Chair of the matters which are the cause of the disagreement, and those matters shall be discussed at that meeting.

Z2.45 The Alt HAN Secretariat shall maintain a record of all resolutions voted on by the Board, which shall indicate how each Board Member voted on each resolution, and shall make such record available on request to any Relevant Supplier Party.

Appeals from Decisions of the Board

Z2.46 A Relevant Supplier Party may appeal to the Forum any decision of the Board.

Z2.47 An appeal under Section Z2.46 will only be validly made if it is notified to the Alt HAN Secretariat within 20 Working Days of the date on which the Board made the decision which is subject to appeal.

Z2.48 Where a decision of the Board is appealed:

(a) the decision shall be treated as having no effect; and

(b) the Forum shall make the decision afresh, which shall then have effect for the purposes of this Section Z in substitution for the decision of the Board.

Z3 ALT HAN SECRETARIAT

Z3.1 ALtHANCo shall, from time to time, appoint and remove, or make arrangements for the appointment and removal of, one or more persons to be known as the **Alt HAN Secretariat**.

Z3.2 The Alt HAN Secretariat shall perform those tasks and functions expressly ascribed to it under this Section Z, and any other tasks and functions that either the Forum or AltHANCo may assign to it from time to time. In particular, the Alt HAN Secretariat shall:

(a) support the election of Board Members in accordance with the provisions of the AltHANCo Election Protocol;

(b) support the voting of Forum Members in accordance with the Forum Voting Protocol;

(c) provide such other support to the proceedings of the Forum, any Forum Sub-Group and the Board as each of them may respectively require; and

(d) provide or procure such facilities and services in connection with the operation of the Forum, any Forum Sub-Group and the Board as each of them may respectively require.

Z3.3 AltHANCo shall be responsible for ensuring that the Alt HAN Secretariat undertakes its tasks and functions in respect of this Section Z. In particular, AltHANCo shall ensure that the arrangements under which the Alt HAN Secretariat is appointed oblige it to undertake such tasks and functions on terms no less onerous than those provided for by this Code.

Z3.4 Subject to the other requirements of this Section Z3, the Alt HAN Secretariat shall be appointed by AltHANCo on such terms and conditions and in return for such remuneration as AltHANCo sees fit.

Z3.5 The person appointed as the Alt HAN Secretariat may be the person appointed to carry out the role of Code Administrator and/or the Secretariat.

Z4 ALT HAN COSTS AND BUDGETS

General

Z4.1 The costs and expenses incurred by (or on behalf of) the Forum in exercising its powers, performing its functions and discharging its duties in respect of this Section Z shall be incurred by AltHANCo, and the DCC shall provide AltHANCo:

(a) with the funds necessary to meet such costs and expenses;

(b) with the funds necessary to meet all other costs and expenses incurred by AltHANCo in the exercise of its duties, powers and functions under this Section Z.

Alt HAN Costs and Expenses

Z4.2 The costs and expenses capable of recovery under this Section Z4 (the **Alt HAN Costs**) shall be all the reasonable costs and expenses incurred:

(a) subject to Section Z4.3, by the Forum Chair, Alternate Chair, Forum Members, Board Members and Forum Sub-Group Members in their capacities as such;

(b) by AltHANCo under or in connection with contracts that AltHANCo has entered into in accordance with this Section Z, including in particular contracts for:

(i) the acquisition of any Alt HAN Service Capacity;

(ii) the provision of any Alt HAN Services;

(iii) the appointment of the Alt HAN Secretariat; and

(iv) the appointment of advisers; and

(c) by AltHANCo under or in connection with any provision of this Section Z,

(in each case) provided that such costs or expenses are provided for in, or otherwise consistent with, an Alt HAN Budget.

Z4.3 Subject to the terms of those contracts referred to in Section Z4.2(b):

(a) the Forum Chair, Alternate Chair, Forum Members, Board Members and Forum Sub-Group Members shall be entitled to recover all reasonable travel expenses properly incurred by them in their roles as such (and the Board shall adopt a policy that sets out guidelines regarding what constitutes reasonable travel expenses);

(b) no Alternate Chair, Forum Member or Board Member shall be entitled to a salary in respect of his or her role as such, or to any payment in respect of the time he or she spends in performing that role; and

(c) no Forum Sub-Group Member shall be entitled to a salary in respect of his or her role as such, or to any payment in respect of the time he or she spends in performing that role, except to the extent that the Forum has approved any such payment.

Z4.4 Where the Forum Chair, Alternate Chair or any Forum Member, Board Member or Forum Sub-Group Member wishes to recover any Alt HAN Costs, he or she shall submit evidence of the cost or expense in question to the Board (or a named person approved by the Board) for approval. The cost or expense shall only be approved to the extent that it is an Alt HAN Cost, and only if the evidence is submitted in a timely manner (and in any event on or before the 20th Working Day following the end of the relevant Regulatory Year). Once approved, the evidence of the Alt HAN Cost shall be submitted to AltHANCo for payment.

Z4.5 Within 20 Working Days following receipt of evidence of an Alt HAN Cost that has been approved in accordance with Section Z4.4, AltHANCo shall pay the relevant amount to the Forum Chair, Alternate Chair, Forum Member, Board Member or Forum Sub-Group Member making the claim.

Alt HAN Costs to be Reimbursed by the DCC

Reimbursement

Z4.6 The Alt HAN Costs incurred by AltHANCo shall be reimbursed to AltHANCo by the

DCC.

Z4.7 AltHANCo may periodically invoice the DCC for the Alt HAN Costs incurred, or reasonably expected to be incurred, by AltHANCo in accordance with the Approved Alt HAN Budget, provided that AltHANCo shall deduct from such invoice any amounts that represent previous overpayments by the DCC (due to the inaccuracy of AltHANCo estimates, or otherwise).

Z4.8 The DCC shall pay each invoice submitted by AltHANCo in accordance with Section Z4.7 within 10 Working Days of receipt of such invoice by the DCC.

Z4.9 It is acknowledged that the DCC is entitled to recover amounts paid by it to AltHANCo in accordance with this Section Z4 through the Charges (subject to the requirements of the DCC Licence).

Z4.10 In the event that the DCC does not pay AltHANCo in accordance with Section Z4.8, and subject to prior approval from the Authority, AltHANCo may invoice the Relevant Supplier Parties for the unpaid amount (and those Parties shall pay the invoiced amounts to AltHANCo as if they were Charges).

Z4.11 Where Section Z4.10 applies, the amount to be paid by each Relevant Supplier Party shall, unless the Authority approves or directs the use of an alternative methodology, be the same as the amount that the Relevant Supplier Party would have paid in Fixed Alt HAN Charges and in Explicit Charges under Section K7.6(j), calculated in accordance with the Charging Methodology, had the amounts been recovered by the DCC through the Charges.

Z4.12 Any amounts paid by a Relevant Supplier Party in accordance with Section Z4.11 shall be reimbursed by AltHANCo to that Relevant Supplier Party (plus interest at the Non-Default Interest Rate) at such time as the Authority may determine.

Provision of Information

Shared Solution Alt HAN Equipment

Z4.13 In preparing the Draft Alt HAN Budget each year in accordance with Section Z4.21, the Board shall, for the purposes of determining Explicit Charges in accordance with

Section K7.6(j) in respect of the Explicit Charging Metric referred to at Section K7.5(t) ('shared solution Alt HAN Equipment'), prepare its best estimate of the average cost of providing Alt HAN Services in respect of each Smart Metering System that will use (or be capable of using) installed Shared Solution Alt HAN Equipment in the first Regulatory Year to which the Draft Alt HAN Budget relates.

Z4.14 The estimate referred to in Section Z4.13 shall be calculated by taking the Board's best estimate of:

(a) the aggregate cost of providing Alt HAN Services, in respect of all Smart Metering Systems that will use (or be capable of using) installed Shared Solution Alt HAN Equipment during the relevant Regulatory Year; and

(b) the aggregate number of Smart Metering Systems that will use (or be capable of using) installed Shared Solution Alt HAN Equipment during that Regulatory Year,

and dividing (a) by (b).

Point-to-Point Alt HAN Equipment

Z4.15 In preparing the Draft Alt HAN Budget each year in accordance with Section Z4.21, the Board shall, for the purposes of determining Explicit Charges in accordance with Section K7.6(j) in respect of the Explicit Charging Metric referred to at Section K7.5(u) ('point-to-point solution Alt HAN Equipment'), prepare its best estimate of the average cost of providing each category of Alt HAN Service which relates to Point-to-Point Alt HAN Equipment in respect of each Smart Metering System that will use (or be capable of using) installed Point-to-Point Alt HAN Equipment in the first Regulatory Year to which the Draft Alt HAN Budget relates.

Z4.16 The estimate referred to in Section Z4.15 shall be calculated by taking the Board's best estimate of:

(a) the aggregate cost of providing each category of Alt HAN Service which relates to Point-to-Point Alt HAN Equipment, in respect of all Smart Metering Systems that will use (or be capable of using) installed Point-to-Point Alt

HAN Equipment during the relevant Regulatory Year; and

(b) the aggregate number of Smart Metering Systems that will use (or be capable of using) installed Point-to-Point Alt HAN Equipment during that Regulatory Year,

and dividing (a) by (b).

Z4.17 In preparing the Draft Alt HAN Budget each year in accordance with Section Z4.21, the Board shall, for the purposes of determining Explicit Charges in accordance with Section K7.6(j) in respect of the Explicit Charging Metric referred to at Section K7.5(v) ('stock level point-to-point solution Alt HAN Equipment'), prepare its best estimates of the average cost of providing each category of Alt HAN Service which relates to Point-to-Point Alt HAN Equipment in respect of such equipment that is provided to, but not installed by, Relevant Supplier Parties in the first Regulatory Year to which the Draft Alt HAN Budget relates.

Z4.18 The estimates referred to in Section Z4.17 shall be calculated by taking the Board's best estimates of:

(a) the aggregate cost of providing each category of Alt HAN Service which relates to Point-to-Point Alt HAN Equipment in respect of such equipment that is provided to, but not installed by, Relevant Supplier Parties during the relevant Regulatory Year; and

(b) the aggregate number of items of Point-to-Point Alt HAN Equipment relating to each such category that will be provided to, but not installed by, Relevant Supplier Parties, during that Regulatory Year,

and in each case dividing (a) by (b).

Provision of Information to the DCC

Z4.19 The Board shall, promptly upon the approval by the Forum of the Approved Alt HAN Budget in respect of each Regulatory Year:

(a) update, so far as is necessary to ensure that they remain best estimates

following that approval, the estimates that were prepared in accordance with Sections Z4.13, Z4.15 and Z4.17; and

(b) provide those estimates to the DCC.

Z4.20 In each month of each year, the Board shall provide to the DCC:

(a) for the purposes of the Explicit Charging Metric referred to at Section K7.5(t) ('shared solution Alt HAN Equipment'), a list of MPANs and MPRNs at premises associated with a Smart Metering System which is using (or is capable of using) installed Shared Solution Alt HAN Equipment (including where such equipment has been installed but not commissioned);

(b) for the purposes of the Explicit Charging Metric referred to at Section K7.5(u) ('point-to-point solution Alt HAN Equipment'), and in respect of each category of Alt HAN Service which relates to Point-to-Point Alt HAN Equipment, a list of MPANs and MPRNs at premises associated with a Smart Metering System which is using (or is capable of using) installed Point-to-Point Alt HAN Equipment to which that category of Alt HAN Service relates (including where such equipment has been installed but not commissioned);

(c) for the purposes of the Explicit Charging Metric referred to at Section K7.5(v) ('stock level point-to-point solution Alt HAN Equipment'), and in respect of each category of Alt HAN Service which relates to Point-to-Point Alt HAN Equipment:

(i) a list of Relevant Supplier Parties which have been provided with, but have not installed, Point-to-Point Alt HAN Equipment to which that category of Alt HAN Service relates; and

(ii) a statement of the number of items of Point-to-Point Alt HAN Equipment which have been provided to, but not installed by, each such Relevant Supplier Party.

Draft Budgets and Work Plans

Z4.21 The Board shall, during January of each year, prepare and circulate to all Relevant

Supplier Parties, the Secretary of State and the Authority a draft budget in respect of Alt HAN Costs for the next two Regulatory Years commencing thereafter (a **Draft Alt HAN Budget**).

Z4.22 Each Draft Alt HAN Budget:

(a) shall set out the Board's good-faith estimate of the Alt HAN Costs that it anticipates will be incurred (or committed to) during the relevant Regulatory Years;

(b) shall be accompanied by a detailed work plan showing the activities and projects to which the relevant costs and expenses relate; and

(c) may make reasonable provision for contingencies.

Z4.23 Each Draft Alt HAN Budget must provide for limits (both individually and in the aggregate) on costs and expenses not expressly provided for in the budget which can be incurred without having to amend the budget.

Approval of Budgets

Z4.24 In respect of the Draft Alt HAN Budget circulated in January for the next Regulatory Year commencing thereafter, the Board shall:

(a) arrange for the circulation to all the Relevant Supplier Parties of the comments received from each Relevant Supplier Party regarding the Draft Budget in the 20 Working Days following the date of its circulation;

(b) consider and respond to those comments, and circulate its responses to all Relevant Supplier Parties;

(c) to the extent that it considers it appropriate to do so, amend the Draft Alt HAN Budget and/or the accompanying work plan in the light of those comments;

(d) submit the Draft Alt HAN Budget to the Forum for its approval, subject to any amendments that the Forum may determine,

and the Draft Alt HAN Budget in such form as it may be approved by the Forum shall be the **Approved Alt HAN Budget** for the relevant Regulatory Year.

Z4.25 The Board shall, promptly upon its approval by the Forum, provide the DCC with a copy of the Approved Alt HAN Budget.

Amendments to Budgets

Z4.26 The Approved Budget relating to each Regulatory Year may be amended from time to time (whether before, during or after that Regulatory Year, and including in respect of Alt HAN Costs already incurred), provided that:

(a) the Board has first followed the procedure set out in Section Z4.24 in relation to the amendment as if it were a Draft Alt HAN Budget; and

(b) the Forum has approved either the proposed amendment or such alternative amendment as it may determine.

Reports

Z4.27 The Board shall, as soon as is reasonably practicable following the end of each Regulatory Year, produce and circulate to:

(a) the Relevant Supplier Parties; and

(b) on request, the Secretary of State and the Authority,

a report on the Alt HAN Costs incurred (or committed to) during that Regulatory Year and the activities and projects to which those Alt HAN Costs relate.

Audit

Z4.28 The Board shall arrange for the monies paid by and to AltHANCo pursuant to this Section Z4 during each Regulatory Year to be audited by a firm of chartered accountants on an annual basis in order to verify whether the requirements of this Section Z4 have been met.

Z4.29 The Board shall send a copy of such auditor's report to all Relevant Supplier Parties and to the Authority within 10 Working Days of its receipt by the Board.

Z4.30 The Authority may from time to time require the Board to provide any information in relation to the Alt HAN Costs that the Authority may specify or describe in a notice given to the Board in accordance with this Section Z4.30, and the Board shall ensure that all such information is provided to the Authority by any date and in any format that the Authority may specify for that purpose.

Z4.31 The Authority may arrange for any such audit of the accounts and financial information of AltHANCo as it may consider appropriate for the purpose of verifying whether or not the Alt HAN Costs have been economically and efficiently incurred, and where it does so the Board shall co-operate fully with the Authority and any person acting on its behalf in order to ensure that any such audit is effective for that purpose.

Z5 TRANSITIONAL PROVISIONS

Forum Members

Z5.1 Where, prior to the coming into force of this Section Z, a Relevant Supplier Party:

(a) nominated a person to represent it in the Forum; and

(b) did not at a later date nominate any different person for that purpose in replacement for the person previously nominated,

the person so nominated shall be treated as being a Forum Member on the date on which this Section Z comes into force.

Z5.2 For the purposes of this Section Z5, a person shall be treated as having been nominated by a Relevant Supplier Party if:

(a) that nomination was made in writing to the Secretary of State; and

(b) the nominating Party is a Relevant Supplier Party on the date on which this Section Z comes into force.

Forum Decisions

Z5.3 Where, prior to the coming into force of this Section Z, a decision was made:

(a) at a meeting of persons who were, at the date of that meeting, nominated by Relevant Supplier Parties to represent their interests in the Forum;

(b) in circumstances in which that meeting would be quorate if it took place on the day on which this Section Z comes into force;

(c) in relation to a matter on which a decision could be made by the Forum in accordance with this Section Z if it were made on the date on which this Section Z comes into force;

(d) in accordance with a process which could properly be followed by the Forum if it were followed on the date on which this Section Z comes into force;

(e) in a manner that is substantially consistent with the Forum Voting Protocol

applicable on the date on which this Section Z comes into force;

(f) such that, if each person exercising a vote in respect of the relevant resolution at that meeting did so in the same way at a meeting taking place on the day on which this Section Z comes into force, the decision would be the same,

then that decision shall be treated as a decision of the Forum made on the date on which this Section Z comes into force, and for the purposes of this Section Z5 shall be referred to as a **Transitional Decision**.

Contrary Decisions

Z5.4 The making of a Transitional Decision shall not preclude the Forum from making any contrary decision on or after the date on which this Section Z comes into force, in which case the later decision shall prevail.

Forum Sub-Groups

Z5.5 By virtue of one or more Transitional Decisions, a Forum Sub-Group may be treated on the date on which this Section Z comes into force as being established and having duties, powers or functions delegated to it by the Forum, but no decision that was made by any Forum Sub-Group Members in any meeting prior to this Section Z coming into force shall be treated as having any binding effect.

Appeals

Z5.6 A Transitional Decision shall be capable of appeal, and the provisions of Sections Z1.60 to Z1.66 (Appeals from Decisions of the Forum) shall apply to it as they do to any other decision of the Forum.

Board Decisions

Z5.7 Where:

(a) prior to the coming into effect of this Section Z, any decision was made by the Board; and

(b) by virtue of paragraph 3 of the Annex to this Section Z, that decision has effect

on and from the date on which this Section Z comes into effect,

that decision shall be capable of appeal, the provisions of Sections Z2.46 to Z2.48 (Appeals from Decisions of the Board) shall apply in relation to it as they do to any other decision of the Board, and for the purposes of those Sections the decision shall be treated as if it were made on the date on which this Section Z comes into effect.

Z6 DEFINITIONS

Z6.1 For the purpose of this Section Z, unless the context otherwise requires, the following words shall have the meaning given to them below:

Alt HAN Costs	has the meaning given to that expression in Section Z4.2 (Alt HAN Costs and Expenses).
Alt HAN Equipment	has the meaning given to that expression in Standard Condition 55.6 of the Electricity Supply Licence and Standard Condition 49.6 of the Gas Supply Licence.
Alt HAN Secretariat	has the meaning given to that expression in Section Z3.1 (Alt HAN Secretariat).
Alt HAN Service Capacity	has the meaning given to that expression in Standard Condition 55.4 of the Electricity Supply Licence and Standard Condition 49.4 of the Gas Supply Licence.
Alt HAN Services	has the meaning given to that expression in Standard Condition 55.5 of the Electricity Supply Licence and Standard Condition 49.5 of the Gas Supply Licence.
Alternate Chair	has the meaning given to that expression in Section Z1.9 (Election of Forum Chair and Alternate Chair).
AltHANCo	has the meaning given to that expression in Section Z2.1 (Establishment of AltHANCo).
AltHANCo Election Protocol	has the meaning given to that expression in Section Z2.14 (Election of Board Members).
AltHANCo Objectives	has the meaning given to that expression in

	Section Z2.5 (AltHANCo Objectives).
Approved Alt HAN Budgets	has the meaning given to that expression in Section Z4.24 (Approval of Budgets).
Board	has the meaning given to that expression in Section Z2.3 (Establishment of AltHANCo).
Board Member	has the meaning given to that expression in Section Z2.8 (Board Composition).
Chair	has the meaning given to that expression in Section Z2.23 (Appointment of the Chair).
DCC Licence	means the licence for the provision of a smart meter communication service granted pursuant to sections 6(1A) and (1C) of the Electricity Act 1989.
Draft Alt HAN Budget	has the meaning given to that expression in Section Z4.21 (Draft Budgets and Work Plans).
Explicit Charges	has the meaning given to that expression in Section K11.1 (Definitions).
Explicit Charging Metrics	has the meaning given to that expression in Section K11.1 (Definitions).
Forum Chair	has the meaning given to that expression in Section Z1.9 (Election of Forum Chair and Alternate Chair).
Forum Member	has the meaning given to that expression in Section Z1.6 (Appointment of Members).
Forum Objectives	has the meaning given to that expression in Section Z1.3 (Forum Objectives, Functions and

	Powers).
Forum Sub-Group	has the meaning given to that expression in Section Z1.41 (Establishing Forum Sub-Groups).
Forum Sub-Group Member	has the meaning given to that expression in Section Z1.45 (Membership of Forum Sub-Groups).
Forum Voting Protocol	means the SEC Subsidiary Document of that name set out in Appendix [TBC].
Large Relevant Supplier Party	means a Party which is both a Relevant Supplier Party and a Large Supplier Party.
Relevant Preceding Period	has the meaning given to that expression in Section Z1.29 (Voting).
Relevant Supplier Party	means a Supplier Party which is required in accordance with standard condition 39 of an Electricity Supply Licence or standard condition 33 of a Gas Supply Licence (in each case entitled 'Smart Metering – The Alt HAN Arrangements') to install a Smart Metering System at any premises.
Small Relevant Supplier Party	means a Party which is both a Relevant Supplier Party and a Small Supplier Party.
Supplier Weighted Vote	has the meaning given to that expression in Section Z1.26 (Voting).
Transitional Decision	has the meaning given to that expression in Section Z5.3 (Forum Decisions).

SEC – Section Z: February 2016 Consultation (showing changes in mark-up from last published version)

ANNEX – ALTHANCO

1 Background

1.1 Alt HAN Company Limited (registered in England and Wales with company number --------) ("**AltHANCo**") has been established on behalf of the Relevant Supplier Parties in order to fulfil the Objective (as defined below), and in doing so will act as the contracting body for the Forum.

1.2 It is intended that the shareholders of AltHANCo shall be limited to Relevant Supplier Parties in accordance with this Annex.

1.3 The Shareholders have agreed that their respective rights as Shareholders shall be regulated by the provisions of this Annex. The rights of the Relevant Supplier Parties as Shareholders are set out exclusively in this Annex. No other provision of this Code shall apply to the regulation of the rights and obligations of Shareholders in their capacity as Shareholders.

1.4 AltHANCo has agreed with the Shareholders to comply with the provisions of this Annex insofar as it relates to AltHANCo.

2 Additional Definitions and Interpretation

2.1 In this Annex, except where the context otherwise requires, the following words and expressions shall have the following meanings:

AltHANCo Chair	means the chairman of the Board from time to time.
AltHANCo Secretary	means the company secretary of AltHANCo from time to time.
Articles	means the articles of association of AltHANCo, as amended from time to time.
Board	means the board of directors of AltHANCo at the relevant time.

Director	means a director of AltHANCo from time to time.
Objective	means acting as a corporate vehicle to assist the Forum in exercising its powers, duties and functions (including entering into contracts where necessary or desirable in order to implement any Forum decision) and carrying out such other duties, powers and functions as may be allocated to it from time to time in accordance with the Code.
Retiring Shareholder	means a Shareholder that ceases to be a Relevant Supplier Party.
Share	means an ordinary share of £1 each in the share capital of AltHANCo.
Shareholder	means a person from time to time registered as a holder of a Share.
Subscribing Shareholders	means each Relevant Supplier Party that has agreed (prior to Section Z of this Code coming into effect) to become a Shareholder on Section Z of this Code coming into effect.

2.2 Words and expressions defined elsewhere in this Code shall have the same meaning in this Annex unless the context otherwise requires.

3 Acknowledgement of Preliminary Matters Already Undertaken

3.1 It is acknowledged that resolutions of the Board and of the Shareholders were made prior to Section Z of this Code coming into effect, at which the business set out in [ref] to this Annex was undertaken. As set out in that [ref], such business is to have

effect from Section Z of this Code coming into effect.

3.2 The consequence of the resolutions referred to above is that, with effect from Section Z of this Code coming into effect, each of the Subscribing Shareholders is a Shareholder and each of the Board Members is a Director.

4 AltHANCo's Objective

4.1 The Shareholders and AltHANCo acknowledge and agree that AltHANCo shall not undertake any activities other than those that are reasonably necessary for carrying out the Objective.

4.2 Each Shareholder acknowledges and agrees that AltHANCo will have complete independence from its Shareholders in its operations and undertakes not to take any action which obstructs or interferes with, or seeks to obstruct or interfere with, the carrying out of the Objective (provided that this Paragraph 4.2 shall not restrict the exercise of Shareholder rights in order to comply with the requirements of this Annex).

5 AltHANCo's Business

5.1 Each Shareholder agrees with each other Shareholder to exercise its rights under this Annex and as a Shareholder in AltHANCo so as to ensure that:

(a) AltHANCo performs and complies with all its obligations under this Code (including without limitation this Annex) and complies with the restrictions (if any) imposed on it by the Articles; and

(b) AltHANCo's activities are conducted in accordance with sound and good business practice with a view to achieving the Objective.

6 New Shareholders

6.1 Any Relevant Supplier Party, from time to time, which is not a Shareholder shall be deemed to have applied to the AltHANCo Secretary to become a Shareholder on its accession to this Code pursuant to Section B (Accession). Upon any such application, the Directors shall either:

(a) procure the transfer to such Relevant Supplier Party of one Share then held by a nominee in accordance with Paragraph 7.2 or 7.3; or

(b) allot to such Relevant Supplier Party one Share.

6.2 For the purposes of Paragraph 6.1(b), the Shareholders agree that, where no Shares are otherwise available for issue, they will exercise the voting rights attaching to their Shares to procure that all necessary steps are taken to create and/or authorise the issue of further Shares.

7 Dealings with Shares

7.1 Otherwise than in accordance with the following provisions of this Paragraph 7, no Shareholder shall:

(a) pledge, mortgage (whether by way of fixed or floating charge) or otherwise encumber its legal or beneficial interest in its Shares; or

(b) sell, transfer or otherwise dispose of any of such Shares (or any legal or beneficial interest therein); or

(c) enter into any agreement in respect of the votes attached to Shares; or

(d) agree, whether or not subject to any condition precedent or subsequent, to do any of the foregoing.

7.2 Upon written notice by the Board requiring it to do so, a Retiring Shareholder shall pay up all amounts which remain unpaid on any Share held by it. The Retiring Shareholder will transfer its Shares at par to a nominee who will hold the Shares for and on behalf of all the other Shareholders. The nominee will be selected by the Directors. All costs and expenses of such transfer shall be for the account of the

Retiring Shareholder.

7.3 If a Retiring Shareholder fails or refuses to transfer any Shares in accordance with its obligations under Paragraph 7.2, the Retiring Shareholder irrevocably appoints by way of security for the failure to perform obligations under this Paragraph 7.3 any Director to execute and deliver a transfer of the Shares from the Retiring Shareholder to a nominee on behalf of the Retiring Shareholder. AltHANCo may accept the consideration for the transfer (subject to the Retiring Shareholder paying-up all amounts which remain unpaid on any Share) and hold it on trust for the Retiring Shareholder, which acceptance shall be a good discharge to the nominee, and may set off such amounts against the costs and expenses of the transfer. The Directors shall cause the nominee to be registered as the holder of such Share and, following the registration of the transfer, the validity of the proceedings shall not be questioned by AltHANCo or any Shareholder.

7.4 The nominee referred to in Paragraphs 7.2 and 7.3 shall hold Shares transferred to it until such time as it is directed by the Directors to transfer them (or some of them) in accordance with Paragraph 6.1(a) and for such period (and only for such period) as the nominee holds any Shares, all rights attaching to the Share shall be suspended, including:

(a) the right to receive income and/or capital;

(b) the right to attend and vote or appoint proxies to attend and vote at general meetings of AltHANCo (whether on a show of hands or on a poll and in the case of proxies only on a poll); and

(c) the right to appoint and remove a Director.

7.5 The Shareholders shall procure that, save in the case of any nominee for the purposes of Paragraphs 7.2 and 7.3:

(a) no person who is not a Relevant Supplier Party may at any time become a Shareholder; and

(b) no Relevant Supplier Party shall hold more than one Share at any time,

and the Directors shall be entitled to refuse to allot and/or to register any transfer of a Share that would result in a breach of this Paragraph 7.5.

8 Composition and Proceedings of the Board

8.1 AltHANCo and the Shareholders acknowledge that Section Z of this Code contains detailed provisions regarding the composition of the Board, and that it is the intention of AltHANCo and the Shareholders that the composition of the Board is identical to that specified under the Code. The Shareholders shall, accordingly, procure that:

(a) each of the Board Members from time to time shall be appointed as a Director; and

(b) the Chair from time to time shall be appointed as the AltHANCo Chair.

8.2 AltHANCo and the Shareholders acknowledge that this Code contains detailed provisions regarding the procedural rules of the Board, and that it is the intention of AltHANCo and the Shareholders that these procedural rules are followed by the Board. The remaining provisions of this Paragraph 8 shall therefore have effect subject to the procedural rules of the Board set out in Section Z2 (The Alt HAN Company); save only to any extent that such procedural rules applicable are incompatible with Laws and Directives stipulating procedural rules for company boards of directors.

8.3 Each Director shall be deemed to have appointed his or her alternate as his or her alternate Director, and shall be deemed to have removed such person from such position on that person ceasing to be his or her alternate. Any such alternate Director shall be entitled to receive notice of all Board meetings and attend and vote as such at any meeting at which the appointing Director is not present and generally in the absence of his or her appointor to do all the things which his or her appointor is authorised or empowered to do. A Director who is also an alternate is entitled, in the absence of his or her appointor:

(a) to a separate vote on behalf of his or her appointor in addition to his or her own vote; and

(b) to be counted as part of the quorum of the Board on his or her own account and also in respect of the Director for whom he or she is the alternate.

8.4 If a Director ceases to be a Board Member, the Shareholders shall exercise their powers to ensure that such person ceases to be a Director. The Relevant Supplier Parties shall jointly and severally indemnify AltHANCo against all Liabilities which AltHANCo may suffer or incur by reason of any claim by that person in connection with his removal from office as a Director.

8.5 The AltHANCo Chair shall chair any Board meeting. If the AltHANCo Chair is unable to be present at a Board meeting, the AltHANCo Chair's alternate appointed in accordance with Paragraph 8.3 may act as chair of that Board meeting.

8.6 The person appointed from time to time as the Secretariat shall be appointed as the AltHANCo Secretary.

8.7 All resolutions of the Board shall be made by simple majority of those Directors present at the meeting. Each Director (including the AltHANCo Chair in his or her capacity as a Director) shall have one vote, and in the case of an equality of votes the AltHANCo Chair shall have a second and casting vote.

8.8 The Board shall meet at intervals of not less than once in any period of two months unless otherwise agreed by the Directors. A meeting of the Board may be convened at any reasonable time at the request of any Director by written notice to the AltHANCo Secretary.

8.9 Meetings of the Board may be held by means of any telecommunications equipment provided that each of the Directors attending the meeting acknowledges that he or she can communicate with each other. In any such case, the meeting shall be deemed to take place in the location of the AltHANCo Chair during such meeting.

8.10 Each of the Directors shall be given notice by the AltHANCo Secretary of each meeting of the Board setting out details of the time, date and place of meeting at least five Working Days prior to the date of such meeting (provided that such period of notice may be shortened for particular meetings by unanimous written consent of all Directors entitled to attend and vote at the meeting).

8.11 The quorum for each meeting of the Board is one half of all Directors appointed at the relevant time, at least one of whom must be the AltHANCo Chair (or his or her alternate as such).

8.12 A written resolution signed by a majority of the Directors shall be as valid and effective as a resolution passed by a meeting of the Board properly convened and constituted in accordance with the terms of this Annex and the Articles.

8.13 As soon as reasonably practicable and in any event no later than five Working Days after each Board meeting, the AltHANCo Secretary shall circulate minutes of that meeting to each of the Directors.

8.14 The Board may delegate any of its powers to committees of the Board consisting of such persons as the Board may resolve. Any such committee shall exercise only powers expressly delegated to it and shall comply with any regulations imposed on it by the Board.

9 Expenditure and Working Capital

9.1 The Shareholders intend that AltHANCo should be run on a "break even" basis and shall procure that any surplus working capital shall, rather than being distributed to Shareholders, be retained by AltHANCo and applied to subsequent expenditure.

9.2 None of the Shareholders shall be obliged to provide any finance to AltHANCo or to provide any guarantee, indemnity or other security which third parties may require to secure the obligations of AltHANCo.

9.3 The Shareholders shall exercise the rights attaching to their Shares with a view to ensuring that AltHANCo does not incur costs unless authorised to do so in accordance with Section Z4 (Alt HAN Charges), except insofar as is necessary in order to comply with legally binding obligations to which AltHANCo is subject.

10 Accounts

10.1 As soon as reasonably practicable following the end of each Regulatory Year, AltHANCo shall procure that an account shall be taken of all the assets and liabilities of AltHANCo and of all the dealings and transactions of AltHANCo during such

Regulatory Year.

10.2 The Board shall prepare a report and accounts in accordance with the Companies Act 2006 to be audited within three months after the end of each Regulatory Year.

11 Conflict with the Articles

11.1 In the event of any ambiguity created by or discrepancy between the provisions of this Annex and the Articles, it is the intention that the provisions of this Annex shall prevail and accordingly the Shareholders shall exercise all voting and other rights and powers available to them so as to give effect to the provisions of this Annex and shall further, if necessary, procure any required amendment to the Articles.

11.2 Any Shareholder failing to comply with the provisions of Paragraph 11.1 shall be deemed to have appointed AltHANCo as its lawful attorney for the purpose of signing any written resolution (or receiving notices of and attending and voting at all meetings) of the members of the AltHANCo to give effect to the provisions of Paragraph 11.1 and to effect any required amendment to the Articles (including to conform the Articles to this Annex), and this power of attorney (which is given by way of security to secure the performance of obligations owed by the Shareholder to the AltHANCo under Paragraph 11.1) shall be irrevocable.

12 Further Assurance

12.1 Each Shareholder shall co-operate with the other Shareholders and execute and deliver to the other Shareholders such other instruments and documents and take such other actions as may be reasonably requested from time to time in order to carry out, evidence and confirm their rights under, and the intended purpose of, this Annex.

13 Duration and Termination

13.1 This Annex shall continue in full force and effect, save in respect of any antecedent breach, until the earlier of:

(a) the provisions of Section Z of this Code ceasing to have effect;

(b) the termination of this Code;

(c) the date on which an effective resolution is passed, or a binding order is made, for the winding up of AltHANCo,

provided, however, that this Annex shall cease to have effect as regards any Relevant Supplier Party who, having been entitled under the terms of this Annex to hold Shares, ceases to hold any Shares.

SEC SCHEDULE 1 – FRAMEWORK AGREEMENT

Dated: 2013

The Original Parties

and

Smart Energy Code Company Limited

Smart Energy Code Framework Agreement

THIS FRAMEWORK AGREEMENT is made on 2013

BETWEEN:

(1) the persons whose details are set out in the Schedule (the "**Original Parties**"); and

(2) **Smart Energy Code Company Limited** a company incorporated in England and Wales with company number 08430267 ("**SECCo**").

WHEREAS

A) Certain of the Original Parties are the holders of Energy Licences that oblige them to be a party to, and to comply with, the Smart Energy Code.

B) The Original Parties that do not hold an Energy Licence, or do not hold an Energy Licence that obliges them to be party to the Smart Energy Code, have chosen to become a party to the Smart Energy Code in order to receive Services from the DCC.

C) SECCo is a company established to facilitate the operation of the Smart Energy Code.

D) The Original Parties and SECCo have agreed to give effect to, and to be bound by, the Smart Energy Code in accordance with this Framework Agreement.

NOW IT IS HEREBY AGREED as follows:

1 Interpretation

1.1 In this Framework Agreement, including the recitals hereto, "**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 Subject to clause 1.1 above, the words and expressions used in this Framework Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if those definitions and provisions

regarding interpretation were set out in this Framework Agreement and as if the references therein to "this Code" were to "this Framework Agreement".

2 Compliance with the Smart Energy Code

2.1 With effect from the date hereof, SECCo and each of the Original Parties hereby undertakes, for the benefit of each other Party from time to time, to comply with the Smart Energy Code in accordance with, and subject to, its terms and conditions.

3 Identity of the Parties

3.1 SECCo and each of the Original Parties acknowledges that it has agreed a mechanism (set out in Section B (Accession) of the Smart Energy Code) by which New Parties may become bound by the Smart Energy Code, each of whom will then become a Party for the purposes of clause 2 above (and otherwise).

3.2 Each of the Original Parties acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which it may cease to be bound by the Smart Energy Code, from which time it will (subject to Section M8 of the Smart Energy Code) cease to be obliged to comply with the Smart Energy Code.

3.3 SECCo and each of the Original Parties acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which other Parties may cease to be bound by the Smart Energy Code, from which time such other Parties will (subject to Section M8 of the Smart Energy Code) cease to be a Party for the purposes of clause 2 above (and otherwise).

4 Party Details

4.1 The Party Details for each of the Original Parties shall (as at the date hereof, and subject to future amendment in accordance with Section M6 (Party Details) of the Smart Energy Code) be those details set out as such in the Schedule.

5 Third Party Rights

5.1 Without prejudice to any provisions of the Smart Energy Code permitting enforcement of the Smart Energy Code by third parties, the Original Parties do not

intend that any of the terms or conditions of this Framework Agreement will be enforceable by a third party (whether by virtue of the Contracts (Rights of Third Parties) Act 1999 or otherwise).

6 Counterparts

6.1 This Framework Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument. The counterpart executed by each of the Original Parties shall attach a schedule containing details of the relevant Original Party, all of which schedules together shall comprise the "**Schedule**".

7 Governing Law and Jurisdiction

7.1 This Framework Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims arising out of or in connection with the Smart Energy Code.

7.2 In relation to any dispute or claim arising out of or in connection with this Framework Agreement (including in respect of non-contractual claims), each of the Original Parties and SECCo irrevocably agrees to submit to the exclusive jurisdiction of the relevant person, panel, court or other tribunal specified in Section M7 (Dispute Resolution) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS FRAMEWORK AGREEMENT has been executed and delivered as a **DEED** on the date first stated above.

Executed and delivered as a deed by

……	……
Print full name of Original Party	*Print name of attorney*
acting by an attorney appointed under a power of attorney	*Signature* …….
In the presence of:	……
	Print name of witness
	Signature …….
	Address …….

OR

Executed and delivered as a deed by

	……
……	*Print name of person signing*
Print full name of Original Party	
acting by two directors or a director and the company secretary	*Signature* …….
	……
	Print name of person signing
	Signature …….

Schedule to the Framework Agreement – Original Parties

1 The Party's full name.

2 Whether the Party is a company or a natural person or a partnership etc.

3 The Party's jurisdiction of incorporation (if applicable).

4 The Party's registered number (if applicable).

5 The Party's registered address (or, if not applicable, its principal address).

6 Where the Party is incorporated or resident outside Great Britain, an address in Great Britain for the receipt of legal notices on the Party's behalf.

7 The Party's VAT registration number (if applicable).

8 The Party's address for invoices under the Code.

9 The Party's address or addresses for all other notices under the Code.

10 The Party Category into which the Party considers it will initially fall.

11 The Energy Licences held by the Party (including any for which it has applied).

12 Details of any Parties that are Affiliates of the Party (where the Party is a company).

13 Where the Party holds one or more Energy Licences, details of any unique identifiers by which the Party is identified under the MRA and/or the UNC (as applicable).

SEC SCHEDULE 2 – ACCESSION AGREEMENT

Dated: 2[XXX]

[New Party]

and

Smart Energy Code Company Limited

Smart Energy Code Accession Agreement

THIS ACCESSION AGREEMENT is made on 2[XXX]

BETWEEN:

(1) **[TBC]** a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**New Party**"); and

(2) **Smart Energy Code Company Limited** a company incorporated in England and Wales with company number 08430267 ("**SECCo**").

WHEREAS

A) The New Party is either obliged by its Energy Licence to become a party to the Smart Energy Code, or wishes to become a party to the Smart Energy Code in order to receive Services from the DCC.

B) SECCo is authorised by the Parties to the Smart Energy Code to accept the accession to the Smart Energy Code of the New Party.

NOW IT IS HEREBY AGREED as follows:

1 Interpretation

1.1 In this Accession Agreement, including the recitals hereto, "**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 Subject to clause 1.1 above, the words and expressions used in this Accession Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if those definitions and provisions regarding interpretation were set out in this Accession Agreement and as if the references therein to "this Code" were to "this Accession Agreement".

2 Compliance with the Smart Energy Code

2.1 With effect from the date hereof, the New Party hereby undertakes, for the benefit of SECCo and each other Party from time to time, to comply with the Smart Energy Code in accordance with, and subject to, its terms and conditions.

3 Identity of the Parties

3.1 The New Party acknowledges that the Original Parties became bound by the Smart Energy Code pursuant to the Framework Agreement, and that each such Original Party is a Party for the purposes of clause 2 above (and otherwise).

3.2 The New Party acknowledges that it has agreed a mechanism (set out in Section B (Accession) of the Smart Energy Code) by which New Parties other than itself may have (or may in the future) become bound by the Smart Energy Code, each of whom is (or will then become) a Party for the purposes of clause 2 above (and otherwise).

3.3 The New Party acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which it may cease to be bound by the Smart Energy Code, from which time it will (subject to Section M8 of the Smart Energy Code) cease to be obliged to comply with the Smart Energy Code.

3.4 The New Party acknowledges that it has agreed a mechanism (set out in Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code) by which other Parties may cease to be bound by the Smart Energy Code, from which time such other Parties will (subject to Section M8 of the Smart Energy Code) cease to be a Party for the purposes of clause 2 above (and otherwise).

4 Party Details

4.1 The New Party's Party Details shall (as at the date hereof, and subject to future amendment in accordance with Section M6 (Party Details) of the Smart Energy Code) be those details set out as such in the Schedule.

5 Third Party Rights

5.1 Without prejudice to any provisions of the Smart Energy Code permitting

enforcement of the Smart Energy Code by third parties, neither the New Party nor SECCo intends that any of the terms or conditions of this Accession Agreement will be enforceable by a third party (whether by virtue of the Contracts (Rights of Third Parties) Act 1999 or otherwise).

6 Execution

6.1 This Accession Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument.

6.2 Where the Code Administrator has provided unexecuted counterparts of this Accession Agreement to the New Party, the New Party should sign (but not date) both counterparts of this Accession Agreement, and return them to the Code Administrator. In doing so, the New Party will be deemed to have authorised SECCo (by its signature of the counterparts) to complete the agreement and to date the counterparts with the date of such completion.

7 Governing Law and Jurisdiction

7.1 This Accession Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims arising out of or in connection with the Smart Energy Code.

7.2 In relation to any dispute or claim arising out of or in connection with this Accession Agreement (including in respect of non-contractual claims), each of the New Party and SECCo irrevocably agrees to submit to the exclusive jurisdiction of the relevant person, panel, court or other tribunal specified in Section M7 (Dispute Resolution) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS ACCESSION AGREEMENT has been executed and delivered as a **DEED** on the date first stated above.

Executed and delivered as a deed by

…… *Print full name of New Party*

acting by two directors or a director and the company secretary

…… *Print name of person signing*

Signature …….

…… *Print name of person signing*

Signature …….

Executed and delivered as a deed by

Smart Energy Code Company Limited

acting by two directors or a director and the company secretary

…… *Print name of person signing*

Signature …….

…… *Print name of person signing*

Signature …….

Schedule to the Accession Agreement – Party Details

[*To include the information referred to in paragraphs 6 to 15 (inclusive) of Schedule 5 (Accession Information).*]

SEC SCHEDULE 3 – SPECIMEN BILATERAL AGREEMENT

Dated: 2[XXX]

[User]

and

[DCC]

Smart Energy Code Bilateral Agreement

THIS BILATERAL AGREEMENT is made on 2[XXX]

BETWEEN:

(1) **[TBC]** a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**User**"); and

(2) **[TBC]** a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**DCC**").

WHEREAS

A) The User wishes to procure the Elective Communication Service pursuant to the Smart Energy Code.

B) The DCC has agreed to provide the Elective Communication Service pursuant to this Bilateral Agreement and the Smart Energy Code, in consideration of the Elective Charges.

NOW IT IS HEREBY AGREED as follows:

1 Interpretation

1.1 In this Bilateral Agreement, unless the context otherwise requires:

"**Elective Charges**" means the charges described as such in Schedule 1.

"**Elective Communication Service**" means the service described as such in Schedule 2.

"**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted to the DCC pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 In this Bilateral Agreement, unless the context otherwise requires, references to "Clauses" and "Schedules" are to the clauses of, and schedules to, this Bilateral Agreement.

1.3 Subject to Clauses 1.1 and 1.2, the words and expressions used in this Bilateral Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if those definitions and provisions regarding interpretation were set out in this Bilateral Agreement and as if the references therein to "this Code" were to "this Bilateral Agreement".

1.4 The Parties acknowledge that the Smart Energy Code is subject to modification from time to time in accordance with its provisions, and that the Smart Energy Code as so modified from time to time shall apply for the purposes of this Bilateral Agreement. References to Sections of the Smart Energy Code shall be to those sections as modified and/or renumbered from time to time.

1.5 The provisions of this Bilateral Agreement are without prejudice to the rights and obligations of the Parties under the Smart Energy Code. The Parties acknowledge that certain provisions of the Smart Energy Code apply, but such acknowledgments are without prejudice to the potentially broader application of the Smart Energy Code. In the event of any conflict between the provisions of this Bilateral Agreement and the provisions of the Smart Energy Code, the Smart Energy Code shall prevail.

2 Commencement of this Bilateral Agreement

2.1 This Bilateral Agreement shall commence on [TBC][1].

3 Provision of the Elective Communication Services

3.1 The DCC shall provide the Elective Communication Services to the User subject to and in accordance with this Bilateral Agreement and the Smart Energy Code.

3.2 The provision of the Elective Communication Services is subject to the User having completed the User Entry Process. The provision of the Elective Communication Services in respect of any Smart Metering System is subject to that Smart Metering System having been Enrolled.

[1] [*Note: consider whether agreement should be conditional on provision of adequate credit support. If so, also add a termination right linked to failure of credit support.*]

4 Elective Charges

4.1 The User shall pay the Elective Charges in accordance with Section J (Charges) of the Smart Energy Code.

4.2 [The Elective Charges include a standing charge (as further described in Schedule 1) that is payable by the User regardless of whether or not the Elective Communication Services are requested or provided.][2]

5 Security and Data Privacy

5.1 The Parties acknowledge that the provisions of Section G (Security) of the Smart Energy Code apply.

5.2 The Parties acknowledge that the provisions of Section I (Data Privacy) of the Smart Energy Code apply.

6 Termination or Expiry of this Bilateral Agreement

6.1 Subject to earlier termination in accordance with this Clause 6, this Bilateral Agreement shall expire on [TBC].

6.2 This Bilateral Agreement shall automatically terminate on the User being expelled from, or voluntarily ceasing to be party to, the Smart Energy Code in accordance with Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code.

6.3 The User shall, at its discretion, be entitled to terminate this Bilateral Agreement on 20 Working Days' prior notice in writing to the DCC.

6.4 In the event of termination of this Bilateral Agreement in accordance with Clause 6.3, the User shall not be obliged to pay compensation on termination to the extent such compensation is intended to recover investments made for the purposes of providing the Elective Communication Service where (and to the extent that) the DCC subsequently offers a Service listed in the DCC User Interface Services Schedule that relies upon such investments. Any dispute under this Clause 6.4 may be referred to the Panel for initial determination, but shall ultimately be subject to arbitration.

[2] [*Note: delete or retain as applicable.*]

6.5 Where this Bilateral Agreement terminates in accordance with Clause 6.2 or 6.3, the User shall (subject to Clause 6.4) pay any compensation on termination described in Schedule 1.

7 Suspension

7.1 The User acknowledges that the DCC may suspend provision of the Elective Communication Services where the Panel directs that the DCC should do so pursuant to Section M8 (Suspension, Expulsion and Withdrawal) of the Smart Energy Code. Such suspension shall be without prejudice to any take or pay obligation described in Schedule 1.

8 Communications

8.1 The Parties acknowledge and agree that the provisions of Sections H3 (DCC User Interface) and M10 (Notices) apply.

9 Amendments

9.1 Without prejudice to Clause 1.4, this Bilateral Agreement may only be amended by agreement in writing by the Parties or in order to give effect to any determination of disputes by the Authority pursuant to the DCC Licence.

9.2 Without prejudice to Clause 1.5, the Parties shall amend this Bilateral Agreement where it has become inconsistent with the Smart Energy Code in order to correct such inconsistency (including where the Specimen Bilateral Agreement is modified, in which case the Parties shall amend this Bilateral Agreement in the same manner and to the same extent).

9.3 The User hereby authorises the DCC to make the amendments to this Bilateral Agreement required pursuant to Clause 9.2 on the User's behalf. Where the User disputes the requirement for, or form of, any such amendments made by the DCC on the User's behalf, then the User may refer the matter to the Panel for its determination. Nothing in this Clause 9.3 shall fetter the User's right to refer disputes to the Authority pursuant to the DCC Licence.

10 Miscellaneous

10.1 The Parties acknowledge that the provisions of Sections M2 (Limitations of Liability), M3 (Services FM and Force Majeure), M4 (Confidentiality), and M5 (Intellectual Property Rights) of the Smart Energy Code apply.

10.2 The Parties acknowledge and agree that this Bilateral Agreement may be novated to DCC's successor in accordance with Section M9 (DCC Transfer) of the Smart Energy Code.

10.3 This Bilateral Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument.

10.4 The provisions of Section M11 (Miscellaneous) of the Smart Energy Code shall apply as if set out in this Bilateral Agreement and as if the references therein to "this Code" were to "this Bilateral Agreement".

11 Governing Law and Jurisdiction

11.1 This Bilateral Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the relevant laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

11.2 In relation to any dispute or claim arising out of or in connection with this Bilateral Agreement (including in respect of non-contractual claims), each of the Parties irrevocably agrees to submit to the exclusive jurisdiction of the relevant person, panel, court or other tribunal specified in Section M7 (Dispute Resolution) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS BILATERAL AGREEMENT has been entered into on the date first stated above.

SIGNED by

duly authorised for and on behalf of ……

…… *Print name of person signing*

Print full name of User

Signature …….

SIGNED by

duly authorised for and on behalf of the DCC ……

Print name of person signing

Signature …….

Schedule 1 – Elective Charges

[Note: to include charges determined in accordance with the Charging Methodology, and to include standing charges and early termination compensation payments where required in accordance with Section H7.]

Schedule 2 – Elective Communication Services

[Note: to identify services in a manner consistent with the DCC User Interface Services Schedule and Section H7.14.]

SEC SCHEDULE 4 – SECCO

1 Background

1.1 Smart Energy Code Company Limited (registered in England and Wales with company number 08430267) ("**SECCo**") has been established on behalf of the Parties in order to fulfil the Objective (as defined below), and in doing so will act as the contracting body for the Panel.

1.2 It is intended that the shareholders of SECCo shall be limited to Eligible Parties in accordance with this Schedule.

1.3 The Shareholders have agreed that their respective rights as Shareholders shall be regulated by the provisions of this Schedule. The rights of the Eligible Parties as Shareholders are set out exclusively in this Schedule. No other provision of this Code shall apply to the regulation of the rights and obligations of Shareholders in their capacity as Shareholders.

1.4 SECCo has agreed with the Shareholders to comply with the provisions of this Schedule insofar as it relates to SECCo.

2 Additional Definitions and Interpretation

2.1 In this Schedule, except where the context otherwise requires, the following words and expressions shall have the following meanings:

Articles	means the articles of association of SECCo, as amended from time to time.
Board	means the board of directors of SECCo at the relevant time.
Director	means a director of SECCo from time to time.
Eligible Party	means a Party that is not the DCC (which, for the avoidance of doubt, does not include SECCo), and which either:

(a) holds an Energy Licence that obliges it to be a party to this Code; or

(b) does not hold an Energy Licence that obliges it to be a party to this Code, but has opted (by notice in writing to the SECCo Secretary) to be a Shareholder.

Objective means acting as a corporate vehicle to assist the Panel in exercising its powers, duties and functions (including entering into contracts where necessary or desirable in order to implement any Panel Decision).

Panel Decision means a resolution of the Panel (or a resolution made by any Sub-Committee to which the Panel has delegated decision-making authority in accordance with Section C7 (Sub-Committees)), and cognate terms shall be construed accordingly.

Retiring Shareholder means either:

(a) a Shareholder that ceases to be a Party; or

(b) a Shareholder that does not hold an Energy Licence that obliges it to be a party to this Code and which gives notice that it no longer wishes to be a Shareholder (such notice to be given in writing to the SECCo Secretary).

SECCo Chair means the chairman of the Board from time to time.

SECCo Secretary means the company secretary of SECCo from time to time.

Share means an ordinary share of £1 each in the share capital of SECCo.

Shareholder means a person from time to time registered as a holder

	of a Share.
Subscribing Shareholders	means each Eligible Party that agreed (prior to the designation of this Code) to become a Shareholder with effect from the designation of this Code.

2.2 Words and expressions defined elsewhere in this Code shall have the same meaning in this Schedule unless the context otherwise requires.

3 Acknowledgement of Preliminary Matters Already Undertaken

3.1 It is acknowledged that resolutions of the Board and of the Shareholders were made prior to the designation of this Code, at which the business set out in annex 1 to this Schedule was undertaken. As set out in that annex, such business is to have effect from the designation of this Code.

3.2 The consequence of the resolutions referred to above is that, with effect from the designation of this Code, each of the Subscribing Shareholders is a Shareholder and each of the Panel Members is a Director.

4 SECCo's Objective

4.1 The Shareholders and SECCo acknowledge and agree that SECCo shall not undertake any activities other than those that are reasonably necessary for carrying out the Objective.

4.2 Each Shareholder acknowledges and agrees that SECCo will have complete independence from its Shareholders in its operations and undertakes not to take any action which obstructs or interferes with, or seeks to obstruct or interfere with, the carrying out of the Objective (provided that this Paragraph 4.2 shall not restrict the exercise of Shareholder rights in order to comply with the requirements of this Schedule).

5 SECCo's Business

5.1 Each Shareholder agrees with each other Shareholder to exercise its rights under this Schedule and as a Shareholder in SECCo so as to ensure that:

(a) SECCo performs and complies with all its obligations under this Code (including without limitation this Schedule) and complies with the restrictions (if any) imposed on it by the Articles; and

(b) SECCo's activities are conducted in accordance with sound and good business practice with a view to achieving the Objective.

6 New Shareholders

6.1 Any Eligible Party, from time to time, which is not a Shareholder may apply to the SECCo Secretary to become a Shareholder. An Eligible Party holding an Energy Licence that obliges it to be a party to this Code shall be deemed to have so applied on its accession to this Code pursuant to Section B (Accession). Upon any such application, the Directors shall either:

(a) procure the transfer to such Eligible Party of one Share then held by a nominee in accordance with Paragraph 7.2 or 7.3; or

(b) allot to such Eligible Party one Share.

6.2 For the purposes of Paragraph 6.1(b), the Shareholders agree that, where no Shares are otherwise available for issue, they will exercise the voting rights attaching to their Shares to procure that all necessary steps are taken to create and/or authorise the issue of further Shares.

7 Dealings with Shares

7.1 Otherwise than in accordance with the following provisions of this Paragraph 7, no Shareholder shall:

(a) pledge, mortgage (whether by way of fixed or floating charge) or otherwise encumber its legal or beneficial interest in its Shares; or

(b) sell, transfer or otherwise dispose of any of such Shares (or any legal or beneficial interest therein); or

(c) enter into any agreement in respect of the votes attached to Shares; or

(d) agree, whether or not subject to any condition precedent or subsequent, to do

any of the foregoing.

7.2 Upon written notice by the Board requiring it to do so, a Retiring Shareholder shall pay up all amounts which remain unpaid on any Share held by it. The Retiring Shareholder will transfer its Shares at par to a nominee who will hold the Shares for and on behalf of all the other Shareholders. The nominee will be selected by the Directors. All costs and expenses of such transfer shall be for the account of the Retiring Shareholder.

7.3 If a Retiring Shareholder fails or refuses to transfer any Shares in accordance with its obligations under Paragraph 7.2, the Retiring Shareholder irrevocably appoints by way of security for the failure to perform obligations under this Paragraph 7.3 any Director to execute and deliver a transfer of the Shares from the Retiring Shareholder to a nominee on behalf of the Retiring Shareholder. SECCo may accept the consideration for the transfer (subject to the Retiring Shareholder paying-up all amounts which remain unpaid on any Share) and hold it on trust for the Retiring Shareholder, which acceptance shall be a good discharge to the nominee, and may set off such amounts against the costs and expenses of the transfer. The Directors shall cause the nominee to be registered as the holder of such Share and, following the registration of the transfer, the validity of the proceedings shall not be questioned by SECCo or any Shareholder.

7.4 The nominee referred to in Paragraphs 7.2 and 7.3 shall hold Shares transferred to it until such time as it is directed by the Directors to transfer them (or some of them) in accordance with Paragraph 6.1(a) and for such period (and only for such period) as the nominee holds any Shares, all rights attaching to the Share shall be suspended, including:

(a) the right to receive income and/or capital;

(b) the right to attend and vote or appoint proxies to attend and vote at general meetings of SECCo (whether on a show of hands or on a poll and in the case of proxies only on a poll); and

(c) the right to appoint and remove a Director.

7.5 The Shareholders shall procure that, save in the case of any nominee for the

purposes of Paragraphs 7.2 and 7.3:

(a) no person who is not an Eligible Party may at any time become a Shareholder; and

(b) no Eligible Party shall hold more than one Share at any time,

and the Directors shall be entitled to refuse to allot and/or to register any transfer of a Share that would result in a breach of this Paragraph 7.5.

8 Composition and Proceedings of the Board

8.1 SECCo and the Shareholders acknowledge that this Code contains detailed provisions regarding the composition of the Panel, and that it is the intention of SECCo and the Shareholders that the composition of the Board is identical to the composition of the Panel. The Shareholders shall, accordingly, procure that:

(a) each of the Panel Members from time to time shall be appointed as a Director; and

(b) the Panel Chair from time to time shall be appointed as the SECCo Chair.

8.2 SECCo and the Shareholders acknowledge that this Code contains detailed provisions regarding the procedural rules of the Panel, and that it is the intention of SECCo and the Shareholders that the procedural rules of the Board are identical to the procedural rules of the Panel. The remaining provisions of this Paragraph 8 shall therefore have effect subject to the procedural rules of the Board set out in Section C (Governance); save only to the extent that such procedural rules applicable to the Panel are incompatible with Laws and Directives stipulating procedural rules for company boards of directors.

8.3 Each Director shall be deemed to have appointed his or her Alternate as his or her alternate Director, and shall be deemed to have removed such person from such position on that person ceasing to be his or her Alternate. Any such alternate Director shall be entitled to receive notice of all Board meetings and attend and vote as such at any meeting at which the appointing Director is not present and generally in the absence of his or her appointor to do all the things which his or her appointor

is authorised or empowered to do. A Director who is also an alternate is entitled, in the absence of his or her appointor:

(a) to a separate vote on behalf of his or her appointor in addition to his or her own vote; and

(b) to be counted as part of the quorum of the Board on his or her own account and also in respect of the Director for whom he or she is the alternate.

8.4 If a Director ceases to be a Panel Member, the Shareholders shall exercise their powers to ensure that such person ceases to be a Director. The DCC shall indemnify SECCo against all Liabilities which SECCo may suffer or incur by reason of any claim by that person in connection with his removal from office as a Director.

8.5 The SECCo Chair shall chair any Board meeting. If the SECCo Chair is unable to be present at a Board meeting, the SECCo Chair's alternate appointed in accordance with Paragraph 8.3 may act as chair of that Board meeting.

8.6 The person appointed from time to time as the Secretariat shall be appointed as the SECCo Secretary.

8.7 All resolutions of the Board shall be made by simple majority of those Directors present at the meeting. Each Director shall have one vote, provided that the SECCo Chair shall have no vote (except in the case of equality of votes, in which case the SECCo Chair shall have the casting vote). Notwithstanding the foregoing, in the case of the person appointed as SECCo Chair by virtue of being Panel Chair in accordance with Section X (Transition), that person shall have a vote as a Director and shall not have any casting vote.

8.8 The Board shall meet at intervals of not less than once in any period of two months unless otherwise agreed by the Directors. Insofar as reasonably practicable, meetings of the Board shall follow on immediately from meetings of the Panel. A meeting of the Board may be convened at any reasonable time at the request of any Director by written notice to the SECCo Secretary.

8.9 Meetings of the Board may be held by means of any telecommunications equipment provided that each of the Directors attending the meeting acknowledges that he or

she can communicate with each other. In any such case, the meeting shall be deemed to take place in the location of the SECCo Chair during such meeting.

8.10 Each of the Directors shall be given notice by the SECCo Secretary of each meeting of the Board setting out details of the time, date and place of meeting at least 10 Working Days prior to the date of such meeting (provided that such period of notice may be shortened for particular meetings by unanimous written consent of all Directors entitled to attend and vote at the meeting).

8.11 The quorum for each meeting of the Board is one half of all Directors appointed at the relevant time, at least one of whom must be the SECCo Chair (or his or her alternate as such).

8.12 A written resolution signed by a majority of the Directors shall be as valid and effective as a resolution passed by a meeting of the Board properly convened and constituted in accordance with the terms of this Schedule and the Articles.

8.13 As soon as reasonably practicable and in any event no later than five Working Days after each Board meeting, the SECCo Secretary shall circulate minutes of that meeting to each of the Directors.

8.14 The Board may delegate any of its powers to committees of the Board consisting of such persons as the Board may resolve. Any such committee shall exercise only powers expressly delegated to it and shall comply with any regulations imposed on it by the Board.

9 Expenditure and Working Capital

9.1 The Shareholders intend that SECCo should be run on a "break even" basis and shall procure that any surplus working capital shall, rather than being distributed to Shareholders, be retained by SECCo and applied to subsequent expenditure.

9.2 None of the Shareholders shall be obliged to provide any finance to SECCo or to provide any guarantee, indemnity or other security which third parties may require to secure the obligations of SECCo.

9.3 The Shareholders shall exercise the rights attaching to their Shares with a view to ensuring that SECCo does not incur costs unless authorised to do so in accordance

with Section C8 (Panel Costs and Budgets), except insofar as is necessary in order to comply with legally binding obligations to which SECCo is subject.

10 Accounts

10.1 As soon as reasonably practicable following the end of each Regulatory Year, SECCo shall procure that an account shall be taken of all the assets and liabilities of SECCo and of all the dealings and transactions of SECCo during such Regulatory Year.

10.2 The Board shall prepare a report and accounts in accordance with the Companies Act 2006 to be audited within three months after the end of each Regulatory Year.

11 Conflict with the Articles

11.1 In the event of any ambiguity created by or discrepancy between the provisions of this Schedule and the Articles, it is the intention that the provisions of this Schedule shall prevail and accordingly the Shareholders shall exercise all voting and other rights and powers available to them so as to give effect to the provisions of this Schedule and shall further, if necessary, procure any required amendment to the Articles.

11.2 Any Shareholder failing to comply with the provisions of Paragraph 11.1 shall be deemed to have appointed SECCo as its lawful attorney for the purpose of signing any written resolution (or receiving notices of and attending and voting at all meetings) of the members of the SECCo to give effect to the provisions of Paragraph 11.1 and to effect any required amendment to the Articles (including to conform the Articles to this Schedule), and this power of attorney (which is given by way of security to secure the performance of obligations owed by the Shareholder to the SECCo under Paragraph 11.1) shall be irrevocable.

12 Further Assurance

Each Shareholder shall co-operate with the other Shareholders and execute and deliver to the other Shareholders such other instruments and documents and take such other actions as may be reasonably requested from time to time in order to

carry out, evidence and confirm their rights under, and the intended purpose of, this Schedule.

13 Duration and Termination

13.1 This Schedule shall continue in full force and effect, save in respect of any antecedent breach, until the earlier of:

(a) the termination of this Code; and

(b) the date on which an effective resolution is passed, or a binding order is made, for the winding up of SECCo,

provided, however, that this Schedule shall cease to have effect as regards any Eligible Party who, having been entitled under the terms of this Schedule to hold Shares, ceases to hold any Shares.

ANNEX 1

Prior to designation of this Code, SECCo (acting by its directors from time to time) and/or the shareholders of SECCo (as applicable) approved the following matters:

1 the change of name of SECCo to Smart Energy Code Company Limited;

2 the transfer of the subscription share in the capital of SECCo to a nominee as if Paragraph 7.2 applied;

3 the change of the registered office of SECCo to the registered address of the Secretariat;

4 the change of the accounting reference date of SECCo to 31 March;

5 the adoption of new Articles of Association of SECCo as per Annex 2;

6 the subscription for Shares in SECCo by the Subscribing Shareholders;

7 the appointment as Directors of SECCo of the Panel Members nominated pursuant to Section X (Transition);

8 the appointment as the company secretary of SECCo of the Secretariat nominated pursuant to Section X (Transition);

9 conflicts of interest (if any) of the incoming Directors of SECCo;

10 the resignation of the incumbent Director of SECCo appointed at incorporation; and

11 the filings at Companies House and updates to the statutory books of SECCo in relation to the matters referred to at 1 – 10 above.

ANNEX 2

Form of New Articles

ARTICLES OF ASSOCIATION

THE COMPANIES ACT 2006

ARTICLES OF ASSOCIATION

of

Smart Energy Code Company Limited (the "Company")

(Registered No. 08430267)

(adopted by Special Resolution passed on [ ])

1 Defined terms

1.1 In these articles:

"**CA 2006**" means the Companies Act 2006;

"**Code**" means the Smart Energy Code designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions;

"**Companies Acts"** means the Companies Acts (as defined in section 2 of the CA 2006), in so far as they apply to the company;

"**connected persons**" in relation to a director means persons connected with that director for the purposes of section 252 CA 2006;

"**eligible director**" means, in relation to a matter or decision, a director who is or would be entitled to count in the quorum and vote on the matter or decision at a meeting of directors (but excluding any director whose vote is not to be counted in respect of the particular matter or decision);

"**Group Company**" means a body corporate which is at the relevant time:

(a) a subsidiary of the Company; or

(b) the Company's holding company or a subsidiary of that holding company,

and for these purposes "**holding company**" and "**subsidiary**" have the meanings given to those expressions in section 1159 CA 2006;

"**Model Articles**" means the regulations contained in Schedule 3 to The Companies (Model Articles) Regulations 2008; and

"**Panel**" has the meaning given to that expression in the Code.

1.2 Unless the context otherwise requires, other words or expressions contained in these articles bear the same meaning as in the Model Articles and CA 2006, in each case as in force on the date when these articles become binding on the Company.

1.3 For the purposes of these articles a corporation shall be deemed to be present in person if its representative duly authorised in accordance with the Companies Acts is present in person.

1.4 Headings in these articles are used for convenience only and shall not affect the construction or interpretation of these articles.

1.5 A reference in these articles to an "article" is a reference to the relevant article of these articles unless expressly provided otherwise.

1.6 Unless expressly provided otherwise, a reference to a statute, statutory provision or subordinate legislation is a reference to it as it is in force from time to time, taking account of:

(a) any subordinate legislation from time to time made under it; and

(b) any amendment or re-enactment,

and includes any statute, statutory provision or subordinate legislation which it amends or re-enacts.

1.7 Any phrase in these articles or the Model Articles introduced by the terms "including", "include", "in particular" or any similar expression shall be construed

as illustrative and shall not limit the sense of the words preceding those terms.

2 Adoption and variation of Model Articles

2.1 Subject as provided in these articles, the Model Articles shall apply to the Company.

2.2 Model Articles 7, 8(2), 11, 12, 13(3), 16, 17(2), 18(4), 19, 20, 21, 23, 41, 52 – 62 (inclusive), and 70 – 77 (inclusive) shall not apply to the Company.

3 Conflicts of interest

3.1 In this article and articles 4 and 5:

"**authorise**" means to authorise in accordance with section 175(5)(a) CA 2006 and "**authorisation**", "**authorised**" and cognate expressions shall be construed accordingly;

a "**conflict of interest**" includes a conflict of interest and duty and a conflict of duties;

"**conflicted director**" means a director in relation to whom there is a conflicting matter;

"**conflicting matter**" means a matter which would or might (if not authorised or if not permitted under article 4) constitute or give rise to a breach of the duty of a director under section 175(1) CA 2006 to avoid a conflict situation;

"**conflict situation**" means a situation in which a director has, or can have, a direct or indirect interest that conflicts, or possibly may conflict, with the interests of the company (including a conflict of interest);

"**interested director**" means a director who has, in any way, a material direct or indirect interest in a matter or decision;

a conflicting matter, conflict situation or interest is "**material**" unless it cannot reasonably be regarded as likely to give rise to a conflict of interest; and

"**other directors**" means, in relation to a particular conflicting matter, directors who are not interested directors in relation to that conflicting matter.

3.2 Exercise of the power of the directors to authorise a conflicting matter shall be subject to the provisions of this article.

3.3 The provisions of this article apply:

(a) subject to article 4; and

(b) without prejudice (and subject) to the provisions of section 175(6) CA 2006.

Nothing in these articles shall invalidate an authorisation.

3.4 A conflicted director seeking authorisation of any conflicting matter shall disclose to the other directors the nature and extent of the conflicting matter as soon as is reasonably practicable. The conflicted director shall provide the other directors with such details of the conflicting matter as are necessary for the other directors to decide how to address the conflicting matter, together with such additional information as may be requested by the other directors.

3.5 Any director (including the conflicted director) may propose that a conflicted director's conflicting matter be authorised. Any such proposal, and any authorisation given by the directors, shall be effected in the same way as any other matter that may be proposed to and resolved on by the directors under the provisions of these articles, except that:

(a) the conflicted director and any other interested director shall not count towards the quorum nor vote on any resolution giving that authorisation; and

(b) the conflicted director and any other interested director may, if the other directors so decide, be excluded from any meeting of the directors while the conflicting matter and the giving of that authorisation are under consideration.

3.6 Where the directors authorise a conflicted director's conflicting matter:

(a) the directors may (whether at the time of giving the authorisation or

subsequently):

(i) require that the conflicted director is excluded from the receipt of information, the participation in discussions and/or the making of decisions (whether at meetings of the directors or otherwise) in relation to which any actual or potential conflict of interest may arise from the conflicting matter; and

(ii) impose on the conflicted director such other terms or conditions for the purpose of dealing with any actual or potential conflict of interest which may arise from the conflicting matter as they may determine;

(b) the conflicted director shall conduct himself in accordance with any terms or conditions imposed by the directors (whether at the time of giving that authorisation or subsequently);

(c) the directors may provide that, where the conflicted director obtains (otherwise than through his position as a director) information that is confidential to a third party, the conflicted director will not be obliged to disclose the information to the company, or to use or apply the information in relation to the company's affairs, where to do so would amount to a breach of that confidence;

(d) the terms of the authorisation shall be recorded in writing (but the authorisation shall be effective whether or not the terms are so recorded); and

(e) the directors may revoke or vary the authorisation at any time but no such action will affect anything done by the conflicted director prior to that action in accordance with the terms of the authorisation.

4 Permitted conflict situations

4.1 If a director or a connected person of a director:

(a) is or becomes a member, director, manager or employee of the company or any other Group Company; or

(b) acquires and holds shares in the capital of any other body corporate, wherever incorporated, provided that the shares held by the director and his connected persons do not exceed 3% of the nominal value of the issued share capital of that body corporate;

any conflict situation which arises only by reason of such a conflicting matter is permitted by this article and the relevant conflicting matter does not require disclosure and authorisation in accordance with article 3.

4.2 A director shall not, by reason of his office or of the resulting fiduciary relationship, be liable to account to the company for any benefit which he (or a person connected with him) derives from:

(a) a conflicting matter authorised by the directors;

(b) a conflicting matter to which article 4.1 applies; or

(c) a decision of the directors in relation to which, in accordance with article 5.2, the director was an eligible director, notwithstanding his relevant conflicting interest,

and no transaction or arrangement shall be liable to be avoided on the grounds of any such interest or benefit.

5 Directors' interests and decision making

5.1 Model Articles - 8 – 10 (inclusive), 13, 17 and 18 shall take effect subject to the terms of the Code.

5.2 A director who has a direct or indirect interest or duty that conflicts with the interests of the company in relation to a proposed decision of the directors is not an eligible director in relation to that decision unless article 5.3 applies to him.

5.3 A director who has a direct or indirect interest that conflicts with the interests of the company in relation to a proposed decision of the directors (a "**relevant conflicting interest**") shall be an eligible director in relation to that decision, provided that:

(a) in a case where the relevant conflicting interest is in an actual or proposed

transaction or arrangement with the company, the nature and extent of the relevant conflicting interest either:

(i) has been duly declared to the other directors in accordance with section 177 or section 182 CA 2006, as the case may require; or

(ii) is not required by the terms of either of those sections to be declared; and

(A) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and:

1) that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is or has been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members (and that authorisation, permission, approval or ratification has not been revoked, withdrawn or reversed); and

2) the relevant director has not been required to be excluded from participation in discussions and/or the making of decisions in relation to which the director has the relevant conflicting interest; or

(B) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is not or has not been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members:

1) the conflict situation arising by reason of that conflicting matter is not material; or

2) the other directors are aware of the relevant conflicting interest and have determined that the director shall be an eligible director in relation to that decision; and

(b) in any other case:

(i) the director has disclosed the nature and extent of the relevant conflicting interest, or has not done so where:

(A) it cannot reasonably be regarded as likely to give rise to a conflict of interest; or

(B) the other directors are already aware of it; and

(ii) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and:

(A) that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is or has been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members (and that authorisation, permission, approval or ratification has not been revoked, withdrawn or reversed); and

(B) the relevant director has not been required to be excluded from participation in discussions and/or the making of decisions in relation to which the director has the relevant conflicting interest; or

(iii) where the relevant conflicting interest is constituted by, or arises from, a conflicting matter of the director and that conflicting matter (or any breach of the relevant director's duty under section 175(1) CA 2006 by reason of that conflicting matter) is not or has not been authorised, permitted, approved or ratified, either in accordance with article 3 or article 4 or by the members:

(A) the conflict situation arising by reason of that conflicting matter is not material; or

(B) the other directors are aware of the relevant conflicting interest and have determined that the director shall be an eligible director in relation to that decision; but

the provisions of this article do not apply in relation to a decision under article 3.5.

For the purposes of this article, the other directors are to be treated as aware of anything of which they ought reasonably to be aware.

5.4 If a question arises at a meeting of the directors about whether or not a director (other than the chair of the meeting):

(a) has a material conflict situation for the purposes of articles 3 or 4;

(b) can vote (where that director does not agree to abstain from voting) on the issue in relation to which the conflict situation arises; or

(c) can be counted in the quorum (where that director does not agree not to be counted in the quorum) for the purpose of voting on the issue in relation to which the conflict arises,

the question must (unless article 5.5 applies) be referred to the chair of the meeting. The ruling of the chair of the meeting in accordance with this article 5.4 about any director other than himself is final and conclusive, unless the nature or extent of the director's conflict situation (so far as it is known to him) has not been fairly disclosed to the other directors.

5.5 If in relation to a question of the kind referred to in article 5.4 the chair of the meeting is an interested director, the question must be referred to the other directors in accordance with article 5.5 as if it were a question about the chair of the meeting.

5.6 If a question of the kind referred to in article 5.4 arises about the chair of the meeting (or if article 5.5 applies), the question shall be decided by a resolution of the other directors. The chair of the meeting (or conflicted director) cannot vote on

the question but can be counted in the quorum. The other directors' resolution about the chair of the meeting (or conflicted director) is conclusive, unless the nature and extent of the chair's (or conflicted director's) conflict situation (so far as it is known to him) has not been fairly disclosed to the other directors.

5.7 For the purposes of:

(a) any meeting (or part of a meeting) held in accordance with article 3 to authorise a director's conflict; or

(b) any determination in accordance with article 5.4 or 5.6,

if there is only one director present who is not an interested director for the purpose of that authorisation or determination, the quorum for that meeting (or part of a meeting) is one eligible director.

5.8 For the purposes of:

(a) any written directors' resolution to authorise a director's conflict in accordance with article 3; or

(b) any written determination in accordance with article 5.4 or 5.6,

if there is only one director in office who is not an interested director for the purpose of that authorisation or determination, the quorum for the purpose of signing that resolution or determination is one eligible director.

5.9 Nothing in this article 5 shall be taken as absolving any director from any of the obligations set out in article 3. A determination by the directors in accordance with article 5.3(a)(ii)(B)(2) or 5.3(b)(iii)(B) that a conflicted director may be an eligible director in relation to a decision of the directors does not amount to authorisation of the relevant conflict situation.

5.10 The company may, by ordinary resolution, ratify any transaction, arrangement or other matter which has not been properly authorised by reason of a contravention of these articles.

6 Decision-making by directors: general

6.1 Subject to the terms the Code, the general rule about decision-making by directors is that any decision of the directors must be either a majority decision at a meeting or by written resolution in accordance with Model Article 18.

6.2 The quorum for each meeting of the Board is one half of all Directors appointed at the relevant time, at least one of whom must be the SECCo Chair (or his or her alternate as such). If:

(a) the Company only has one director; and

(b) no other provision of these articles requires it to have more than one director,

the general rule does not apply, the quorum for meetings of the directors shall be one and the director may take decisions without regard to any of the provisions of these articles relating to directors' decision-making, other than the provisions of articles 6.3 and 6.7.

6.3 The directors must ensure that the Company keeps a record, in writing, for at least 10 years from the date of the decision recorded, of every unanimous or majority decision taken by the directors.

6.4 Model Article 9(3) shall be modified so that any meeting where all the directors participating are not in the same place shall be treated as taking place in the place where the chair of the meeting is.

6.5 Model Article 10(2) shall be read:

(a) subject to articles 5 and 6.2; and

(b) as if the final word was deleted and the words "two eligible directors" were added in its place.

6.6 The chair of directors' meetings shall have no vote, save in the event of an equality of votes, where he shall have a casting vote, and Model Article 13(2) shall be modified accordingly.

6.7 Model Article 14(2) shall be read as if the words "to be counted" to "voting purposes" inclusive were omitted and the words "an eligible director for the purposes of that meeting (or part of a meeting)" were added in their place.

6.8 For the purposes of Model Articles 17 and 18, a written resolution of the directors may be in electronic form. Model Article 18 shall be read as if the words "all the directors" were omitted and the words "a simple majority of the directors" were added in their place.

6.9 A decision may not be taken in accordance with Model Article 18 if the eligible directors making that decision would not have formed a quorum at a directors' meeting resolving on the same matter.

6.10 Save for the chair person, the directors shall not be entitled to any remuneration from the Company. This is without prejudice to the recovery of reasonable expenses properly incurred in connection with the Company.

7 General meetings and written resolutions

7.1 Voting rights attaching to a share may be exercised, either at a general meeting or on any written resolution, notwithstanding that amounts are outstanding, due and payable to the Company in respect of that share.

8 Allotment of shares

8.1 Without prejudice to any special rights previously conferred on the holders of any existing shares or class of shares, all shares shall be issued to the persons, on the terms and conditions and with the rights, priorities, privileges or restrictions in each case as provided in the resolution creating or issuing the relevant shares. In the absence of any such provision, the directors may issue the shares, subject to section 551 CA 2006, to such persons at such times and generally on such terms and conditions and with such rights, priorities, privileges or restrictions as they may think fit. Accordingly, and in accordance with section 570 CA 2006, sections 561(1) and 562 CA 2006 shall not apply to the Company.

8.2 No share shall be issued to any infant, bankrupt, insolvent body corporate or person who, by reason of that person's mental health, is subject to a court order which

wholly or partly prevents that person from personally exercising any powers or rights which that person would otherwise have.

9 Transmission of shares

9.1 Nothing in these articles or the Model Articles releases the estate of a deceased member from any liability in respect of a share solely or jointly held by that member.

10 Return of capital

10.1 The Shareholders intend that the Company should be run on a "break even" basis and shall procure that any surplus working capital shall, rather than being distributed to Shareholders, be retained by the Company and applied to subsequent expenditure.

10.2 Subject to articles 10.1 and 10.3, on a return of capital on liquidation, capital reduction or otherwise, the surplus assets of the Company remaining after the payment of its liabilities shall be applied:

(a) in paying to each holder of shares an amount in respect of each share held equal to the amount paid up thereon (including any premium); and

(b) thereafter, in distributing the balance of such assets amongst the holders of the shares in proportion to the amounts paid up or credited as paid up on the shares and held by them.

10.3 Any Shareholder may elect (by notice to the Company secretary) to pay up all amounts which remain unpaid on any Share immediately prior to any return of capital of the kind referred to in article 10.2.

11 Delivery of documents and information

11.1 Any notice, document or other information shall be deemed to be served on and delivered to the intended recipient:

(a) if properly addressed and sent by prepaid United Kingdom first class post to an address in the United Kingdom, 48 hours after it was posted (or five business days after posting either to an address outside the United Kingdom

or from outside the United Kingdom to an address within the United Kingdom, if (in each case) sent by reputable international overnight courier addressed to the intended recipient, provided that delivery in at least five business days was guaranteed at the time of sending and the sending party receives a confirmation of delivery from the courier service provider);

(b) if properly addressed and delivered by hand, when it was given or left at the appropriate address; and

(c) if sent or supplied by means of a website, when the material is first made available on the website or (if later) when the recipient receives (or is deemed to have received) notice of the fact that the material is available on the website.

For the purposes of this article, no account shall be taken of any part of a day that is not a working day.

11.2 In proving that any notice, document or other information was properly addressed, it shall be sufficient to show that the notice, document or other information was delivered to an address permitted for the purpose by CA 2006.

11.3 For the purposes of section 1147(3) CA 2006, where a document or information is sent or supplied by the Company to any member by electronic means, and the Company is able to show that it was properly addressed, it is deemed to have been received by the intended recipient one hour after it was sent (but subject to section 1147(5)).

11.4 Where a document or information is sent or supplied to the Company by one person (the "**agent**") on behalf of another person (the "**sender**"), the Company may require reasonable evidence of the authority of the agent to act on behalf of the sender.

12 The Code

12.1 In addition to the provisions of these Articles, the members shall be obliged (except to the extent, if any, prohibited by law) to give effect to the Code in force at the relevant time.

12.2 Each Shareholder shall procure, to the extent reasonably possible, that the Directors

shall act in all reasonable respects in relation to the Company so as to give effect to the Code, provided always that each Director will not be required to act in any manner prejudicial to his fiduciary duties as a Director of the Company.

SEC SCHEDULE 5 – ACCESSION INFORMATION

1 The Applicant's full name.

2 Whether the Applicant is a company or a natural person or a partnership etc.

3 The Applicant's jurisdiction of incorporation (if applicable).

4 The Applicant's registered number (if applicable).

5 The Applicant's registered address (or, if not applicable, its principal address).

6 Where the Applicant is incorporated or resident outside Great Britain, an address in Great Britain for the receipt of legal notices on the Applicant's behalf.

7 The Applicant's VAT registration number (if applicable).

8 The Applicant's address for invoices under the Code.

9 The Applicant's address or addresses for all other notices under the Code.

10 The Party Category into which the Applicant considers it will initially fall.

11 The Energy Licences held by the Applicant (including any for which it has applied).

12 Details of any Parties that are Affiliates of the Applicant (where the Applicant is a company).

13 Where the Applicant holds one or more Energy Supply Licences, details of the unique identifiers by which the Applicant is identified under the MRA or the UNC (as applicable) for the purposes of recording the Applicant's Registration for an MPAN or MPRN. [This information shall be treated as confidential and not disclosed on the Website.]

14 Where the Applicant holds an Electricity Distribution Licence or a Gas Transporter Licence, details of the unique identifier by which the Applicant is identified under the MRA and/or the UNC (as applicable) for the purposes of recording the network to which an MPAN or MPRN relates. [This information shall be treated as confidential and not disclosed on the Website.]

15 Where applicable, details of the unique identifiers by which the Applicant is identified under the MRA or the UNC (as applicable) for the purposes of recording the Applicant's status as a Meter Operator or a Meter Asset Manager for an MPAN or MPRN. [This information shall be treated as confidential and not disclosed on the Website.]

16 The name of the person or persons who will enter into the Accession Agreement on behalf of the Applicant.

SEC SCHEDULE 6 - FORM OF LETTER OF CREDIT

Form of Document: Irrevocable Standby Letter of Credit

Documentary Credit Number: [ ]

Date of Issue: [ ]

Issuing Bank: [ ]

At the request of the Applicant, the Issuing Bank issues this irrevocable standby letter of credit ("**Standby Letter of Credit**") in the Beneficiary's favour on the following terms and conditions.

In this Standby Letter of Credit:

"**Applicant**" means [insert User's name]

"**Beneficiary**" means [DCC] [insert company number and address], and its successors as the DCC under the Smart Energy Code

"**Beneficiary Statement**" means a demand on the Beneficiary's letterhead, stating the name and title of the person signing on behalf of the Beneficiary, in the form set out at in the schedule to this Standby Letter of Credit.

"**Effective Date**" means [ ] (London, UK)

"Expiry Date" means [ ] (London, UK)

"**Maximum Amount**" means [ ]

"**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time.

1. From the Effective Date, this Standby Letter of Credit is available for payment at sight against presentation to the Issuing Bank of a Beneficiary Statement.

2. The Issuing Bank will not be obliged to make a payment under this Standby Letter of Credit if as a result the aggregate of all payments made by it under this Standby Letter of Credit would exceed the Maximum Amount.

3. The Beneficiary Statement must be presented to the Issuing Bank on or before the Expiry Date.

4. All payments under this Letter of Credit shall be made in Pounds Sterling in immediately available, freely transferable funds and for value on the due date to the account set out in the Beneficiary Statement.

5. The Issuing Bank hereby waives any right to set off or counterclaim whatsoever against any amounts payable under this Standby Letter of Credit in respect of any claims the Issuing Bank may have against the Beneficiary and such amounts shall be paid free and clear of all deductions or withholdings whatsoever. If the Issuing Bank is required by law to make a tax deduction from any amounts payable under this Standby Letter of Credit, the amount due from the Issuing Bank shall be increased to an amount which (after such tax deduction) leaves an amount equal to the payment which would have been due if no tax deduction had been required.

6. This Standby Letter of Credit is personal to the Beneficiary, and the Beneficiary's rights hereunder (including the right to receive proceeds) are not assignable; provided that such rights shall enure for the benefit of the DCC's successors under the Smart Energy Code.

7. Except to the extent it is inconsistent with the express terms of this Standby Letter of Credit, this Standby Letter of Credit is subject to the Uniform Customs and Practice for Documentary Credits (2007 Revision), International Chamber of Commerce Publication No. 600 other than Article 38 thereof which is hereby waived and Article 36 is varied as below. Other than a person to whom this Standby Letter of Credit has been transferred in accordance with clause 6, this Standby Letter of Credit shall not confer any benefit on or be enforceable by any third party. If this Standby Letter of Credit expires during any interruption of business as described in Article 36 of said Publication 600, the Issuing Bank specifically agrees to honour any demand made

under this Standby Letter of Credit within thirty (30) days after the resumption of business.

8. This Standby Letter of Credit and any non-contractual obligations or disputes arising out of or in connection with it shall be governed by and construed in accordance with the laws of England and the parties submit to the exclusive jurisdiction of the Courts of England for all disputes arising under, out of, or in relation to this Letter of Credit.

Signed for and on behalf of

Issuing Bank

Schedule - Form of Beneficiary Statement

We, the DCC under the Smart Energy Code (the "Beneficiary"), hereby state that we are entitled, in accordance with the Smart Energy Code, to demand ……..[insert amount being claimed] under Standby Letter of Credit number……... issued by ……[insert name of Issuing Bank]. Payment in respect of this demand shall be effected immediately to [insert relevant account details]. We confirm that the signatory(ies) to this demand are empowered to sign and make this demand on behalf of the Beneficiary.

SEC SCHEDULE 7 – SPECIMEN ENABLING SERVICES AGREEMENT

Dated: 2[XXX]

[Participant]

and

[DCC]

Smart Energy Code Enabling Services Agreement

THIS ENABLING SERVICE AGREEMENT is made on 2[XXX]

BETWEEN:

(1) **[TBC]** a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**Participant**"); and

(2) **[TBC]** a company incorporated in [*Jurisdiction*] (registered number [TBC]) whose registered office is at [TBC] (the "**DCC**").

WHEREAS

A) The Participant wishes to procure the Enabling Services pursuant to the Smart Energy Code.

B) The DCC has agreed to provide the Enabling Services pursuant to this Enabling Services Agreement, in consideration of the Enabling Service Charges.

NOW IT IS HEREBY AGREED as follows:

1 Interpretation

1.1 In this Enabling Services Agreement, unless the context otherwise requires:

"**Enabling Service Charges**" means those charges described in Schedule 2.

"**Enabling Services**" means the services described in Schedule 1.

"**Event of Default**" means that the Participant:

(a) is in material breach of any of its material obligations under this Enabling Services Agreement, and the Participant has failed to remedy the breach within 20 Working Days after a notice from the DCC requiring such remedy; and/or

(b) suffers an Insolvency Type Event.

"**Party**" means the DCC or the Participant; and "**Parties**" means both of them.

"**Smart Energy Code**" means the code of that name designated by the Secretary of State pursuant to the smart meter communication licences granted to the DCC pursuant to the Electricity Act 1989 and the Gas Act 1986, as such code is modified from time to time in accordance with its provisions.

1.2 In this Enabling Services Agreement, unless the context otherwise requires, references to "Clauses" and "Schedules" are to the clauses of, and schedules to, this Enabling Services Agreement.

1.3 Subject to Clauses 1.1 and 1.2, the words and expressions used in this Enabling Services Agreement shall be construed and interpreted in accordance with the definitions and provisions regarding interpretation set out in Section A (Definitions and Interpretation) of the Smart Energy Code, as if:

(a) those definitions and provisions regarding interpretation were set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1; and

(c) the references therein to:

(i) "Charges" were to "Enabling Service Charges";

(ii) "Services" were to "Enabling Services";

(iii) "User" were to "Participant"; and

(iv) "this Code" or "this Code and/or any Bilateral Agreement" were to "this Enabling Services Agreement".

1.4 The Parties acknowledge that the Smart Energy Code is subject to modification from time to time in accordance with its provisions and law, and that the Smart Energy Code as so modified from time to time shall apply for the purposes of this Enabling Services Agreement.

1.5 References in this Enabling Services Agreement (or in provisions incorporated herein by reference) to Sections of the Smart Energy Code shall be to those sections as

incorporated into this Enabling Services Agreement, as such sections are modified and/or renumbered from time to time.

2 Commencement of this Enabling Services Agreement

2.1 This Enabling Services Agreement shall commence on [TBC].

3 Provision of the Enabling Services

3.1 The DCC shall provide the Enabling Services to the Participant subject to and in accordance with this Enabling Services Agreement.

3.2 The DCC and the Participant shall each comply with the additional obligations assigned to them in Schedule 1.

4 Enabling Service Charges

4.1 The Participant shall pay the Enabling Service Charges in respect of which Sections J1 (Payment of Charges) and J2 (Payment Default and Disputes) shall apply as if:

(a) those Sections were set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1;

(c) the references therein to expressions referred to in Clause 1.3(c) were interpreted as referred to in that Clause; and

(d) Section J2.7 (Pursing Non-Payment) did not apply.

5 Limitations of Liability

5.1 The DCC's and the Participant's liability under or in connection with this Enabling Services Agreement shall be limited in accordance with Section M2 (Limitations of Liability) as if:

(a) that Section was set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1;

(c) the references therein to expressions referred to in Clause 1.3(c) were interpreted as referred to in that Clause; and

(d) Sections M2.17 and M2.18 (SECCo) did not apply.

6 Termination or Expiry of this Enabling Services Agreement

6.1 Subject to earlier termination in accordance with this Clause 6, this Enabling Services Agreement shall expire on [TBC].

6.2 The Participant shall, at its discretion, be entitled to terminate this Enabling Services Agreement on 20 Working Days' prior notice in writing to the DCC.

6.3 The DCC shall be entitled to immediately terminate this Agreement on notice to the Participant where an Event of Default occurs.

6.4 The expiry or earlier termination of this Agreement shall be without prejudice to:

(a) those rights and obligations under this Enabling Services Agreement that may have accrued prior to such expiry or termination; or

(b) those provisions of this Enabling Services Agreement that are expressly or by implication intended to survive such expiry or termination, including Clauses 4 and 5.

7 Amendments

7.1 Without prejudice to Clause 1.4, this Enabling Services Agreement may only be amended by agreement in writing by the Parties or in order to give effect to any determination of disputes by the Authority pursuant to the DCC Licence.

7.2 The Parties shall amend this Enabling Services Agreement where it has become inconsistent with the Smart Energy Code in order to correct such inconsistency (including where the Specimen Enabling Services Agreement is modified, in which case the Parties shall amend this Enabling Services Agreement in the same manner and to the same extent).

7.3 The Participant hereby authorises the DCC to make the amendments to this Enabling

Services Agreement required pursuant to Clause 7.2 on the Participant's behalf. Where the Participant disputes the requirement for, or form of, any such amendments made by the DCC on the Participant's behalf, then the Participant may refer the matter to the Panel for its determination. Nothing in this Clause 7.3 shall fetter the Participant's right to refer disputes to the Authority pursuant to the DCC Licence.

8 Miscellaneous

8.1 The Parties agree that the provisions of Sections M3 (Services FM and Force Majeure), M4 (Confidentiality), M7 (Dispute Resolution), M9 (DCC Transfer), M10 (Notices) and M11 (Miscellaneous) of the Smart Energy Code shall apply to this Enabling Services Agreement, as if:

(a) those Sections were set out in this Enabling Services Agreement;

(b) the uses therein of the words defined in Clause 1.1 were interpreted in accordance with Clause 1.1;

(c) the references therein to expressions referred to in Clause 1.3(c) were interpreted as referred to in that Clause; and

(d) the following Sections did not apply: Sections M3.14 (SECCo), M7.16 (SECCo), M10.1 (Communication via Specified Interfaces), M10.6 (The Panel, Code Administrator, Secretariat and SECCo), M11.5 (Third Party Rights), and M11.15 (SECCo).

8.2 This Enabling Services Agreement may be executed in any number of counterparts, each of which shall be an original but all of which together shall constitute one and the same instrument.

9 Governing Law

9.1 In accordance with Clause 8, this Enabling Services Agreement and any dispute or claim arising out of or in connection with it (including non-contractual claims) shall be governed by, and construed in accordance with, the relevant laws specified in Section M11 (Miscellaneous) of the Smart Energy Code from time to time for the purpose of disputes or claims of that nature.

THIS ENABLING SERVICES AGREEMENT has been entered into on the date first stated above.

SIGNED by

duly authorised for and on behalf of ……

…… *Print name of person signing*

Print full name of Participant

Signature …….

SIGNED by

duly authorised for and on behalf of the DCC ……

Print name of person signing

Signature …….

Schedule 1 – Enabling Services

[The Enabling Services shall comprise the provision of Test Communications Hubs in accordance with Section F10 (Test Communications Hubs). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section F10 (the Participant complying with those obligations assigned to TCH Participants).]

[The Enabling Services shall comprise the provision of those Device and User System Tests described in Section H14.31(a) (Device and User System Tests) in accordance with Section H14 (Testing Services). The DCC and the Participant shall each comply with their respective obligations set out or referred to in that Section H14 (the Participant complying with those obligations assigned to Testing Participants).]

Schedule 2 – Enabling Service Charges

The Enabling Service Charges shall comprise those charges set out in the Charging Statement from time to time that apply to the Explicit Charging Metrics (as defined in the Charging Methodology) that comprise the Enabling Services, being the Explicit Charge applicable to the:

[ordering of Test Communications Hubs pursuant to Section F10 (Test Communications Hubs)] / [the provision of a connection to the SM WAN pursuant to Section H14.31 (Device and User System Testing)] / [the provision of additional testing support pursuant to Section H14.33 (Device and User System Testing)].

APPENDIX A – DEVICE CERTIFICATE POLICY

CONTENTS

Part Heading Page

1 INTRODUCTION 8
1.1 OVERVIEW 8
1.2 DOCUMENT NAME AND IDENTIFICATION 8
1.3 SMKI PARTICIPANTS 8
1.3.1 The Device Certification Authority 8
1.3.2 Registration Authorities 9
1.3.3 Subscribers 9
1.3.4 Subjects 9
1.3.5 Relying Parties 10
1.3.6 SMKI Policy Management Authority 10
1.3.7 SMKI Repository Provider 10
1.4 USAGE OF DEVICE CERTIFICATES AND DCA CERTIFICATES 10
1.4.1 Appropriate Certificate Uses 10
1.4.2 Prohibited Certificate Uses 11
1.5 POLICY ADMINISTRATION 12
1.5.1 Organisation Administering the Document 12
1.5.2 Contact Person 12
1.5.3 Person Determining Device CPS Suitability for the Policy 12
1.5.4 Device CPS Approval Procedures 12
1.5.5 Registration Authority Policies and Procedures 12
1.6 DEFINITIONS AND ACRONYMS 12
1.6.1 Definitions 12
1.6.2 Acronyms 12
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 13
2.1 REPOSITORIES 13
2.2 PUBLICATION OF CERTIFICATION INFORMATION 13
2.3 TIME OR FREQUENCY OF PUBLICATION 13
2.4 ACCESS CONTROLS ON REPOSITORIES 14
3 IDENTIFICATION AND AUTHENTICATION 15
3.1 NAMING 15
3.1.1 Types of Names 15
3.1.2 Need for Names to be Meaningful 15
3.1.3 Anonymity or Pseudonymity of Subscribers 15
3.1.4 Rules for Interpreting Various Name Forms 15
3.1.5 Uniqueness of Names 15
3.1.6 Recognition, Authentication, and Role of Trademarks 15
3.2 INITIAL IDENTITY VALIDATION 15
3.2.1 Method to Prove Possession of Private Key 16
3.2.2 Authentication of Organisation Identity 16
3.2.3 Authentication of Individual Identity 16
3.2.4 Authentication of Devices 17
3.2.5 Non-verified Subscriber Information 17
3.2.6 Validation of Authority 17

3.2.7 Criteria for Interoperation 17
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 17
3.3.1 Identification and Authentication for Routine Re-Key 17
3.3.2 Identification and Authentication for Re-Key after Revocation 17
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 17
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 18
4.1 CERTIFICATE APPLICATION 18
4.1.1 Submission of Certificate Applications 18
4.1.2 Enrolment Process and Responsibilities 18
4.1.3 Enrolment Process for the Registration Authority and its Representatives 18
4.2 CERTIFICATE APPLICATION PROCESSING 19
4.2.1 Performing Identification and Authentication Functions 19
4.2.2 Approval or Rejection of Certificate Applications 19
4.2.3 Time to Process Certificate Applications 19
4.3 CERTIFICATE ISSUANCE 20
4.3.1 DCA Actions during Certificate Issuance 20
4.3.2 Notification to Eligible Subscriber by the DCA of Issuance of Certificate 21
4.4 CERTIFICATE ACCEPTANCE 21
4.4.1 Conduct Constituting Certificate Acceptance 21
4.4.2 Publication of Certificates by the DCA 22
4.4.3 Notification of Certificate Issuance by the DCA to Other Entities 22
4.5 KEY PAIR AND CERTIFICATE USAGE 22
4.5.1 Subscriber Private Key and Certificate Usage 22
4.5.2 Relying Party Public Key and Certificate Usage 22
4.6 CERTIFICATE RENEWAL 22
4.6.1 Circumstances of Certificate Renewal 23
4.6.2 Circumstances of Certificate Replacement 23
4.6.3 Who May Request a Replacement Certificate 24
4.6.4 Processing Replacement Certificate Requests 24
4.6.5 Notification of Replacement Certificate Issuance to a Subscriber 24
4.6.6 Conduct Constituting Acceptance of a Replacement Certificate 24
4.6.7 Publication of a Replacement Certificate by the DCA 24
4.6.8 Notification of Certificate Issuance by the DCA to Other Entities 24
4.7 CERTIFICATE RE-KEY 24
4.7.1 Circumstances for Certificate Re-Key 24
4.7.2 Who may Request Certification of a New Public Key 24
4.7.3 Processing Certificate Re-Keying Requests 24
6.2.3 Notification of New Certificate Issuance to Subscriber 25
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 25
4.7.6 Publication of the Re-Keyed Certificate by the DCA 25
4.7.7 Notification of Certificate Issuance by the DCA to Other Entities 25
4.8 CERTIFICATE MODIFICATION 25
4.8.1 Circumstances for Certificate Modification 25
4.8.2 Who may request Certificate Modification 25
4.8.3 Processing Certificate Modification Requests 25
4.8.4 Notification of New Certificate Issuance to Subscriber 25
4.8.5 Conduct Constituting Acceptance of Modified Certificate 25
4.8.6 Publication of the Modified Certificate by the DCA 25
4.8.7 Notification of Certificate Issuance by the DCA to Other Entities 26
4.9 CERTIFICATE REVOCATION AND SUSPENSION 26

4.9.1 Circumstances for Revocation 26
4.9.2 Who can Request Revocation 26
4.9.3 Procedure for Revocation Request 26
4.9.4 Revocation Request Grace Period 26
4.9.5 Time within which DCA must process the Revocation Request 26
4.9.6 Revocation Checking Requirements for Relying Parties 26
4.9.7 CRL Issuance Frequency (if applicable) 26
4.9.8 Maximum Latency for CRLs (if applicable) 26
4.9.9 On-line Revocation/Status Checking Availability 26
4.9.10 On-line Revocation Checking Requirements 27
4.9.11 Other Forms of Revocation Advertisements Available 27
4.9.12 Special Requirements in the Event of Key Compromise 27
4.9.13 Circumstances for Suspension 27
4.9.14 Who can Request Suspension 27
4.9.15 Procedure for Suspension Request 27
4.9.16 Limits on Suspension Period 27
4.10 CERTIFICATE STATUS SERVICES 27
4.10.1 Operational Characteristics 27
4.10.2 Service Availability 27
7.3.2 Optional Features 27
4.11 END OF SUBSCRIPTION 28
8.5 KEY ESCROW AND RECOVERY 28
4.12.1 Key Escrow and Recovery Policies and Practices 28
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 28
5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 29
5.1 PHYSICAL CONTROLS 29
5.1.1 Site Location and Construction 29
5.1.2 Physical Access 30
5.1.3 Power and Air Conditioning 30
5.1.4 Water Exposure 30
5.1.5 Fire Prevention and Protection 30
5.1.6 Media Storage 31
5.1.7 Waste Disposal 31
5.1.8 Off-Site Back-Up 31
5.2 PROCEDURAL CONTROLS 32
5.2.1 Trusted Roles 32
5.2.2 Number of Persons Required per Task 33
5.2.3 Identification and Authentication for Each Role 33
5.2.4 Roles Requiring Separation of Duties 33
5.3 PERSONNEL CONTROLS 33
5.3.1 Qualification, Experience and Clearance Requirements 33
5.3.2 Background Check Procedures 34
5.3.3 Training Requirements 34
5.3.4 Retraining Frequency and Requirements 34
5.3.5 Job Rotation Frequency and Sequence 34
5.3.6 Sanctions for Unauthorised Actions 35
5.3.7 Independent Contractor Requirements 35
5.3.8 Documentation Supplied to Personnel 35
5.4 AUDIT LOGGING PROCEDURES 35
5.4.1 Types of Events Recorded 35

5.4.2 Frequency of Processing Log 36
5.4.3 Retention Period for Audit Log 37
5.4.4 Protection of Audit Log 37
5.4.5 Audit Log Back-Up Procedures 38
5.4.6 Audit Collection System (Internal or External) 38
5.4.7 Notification to Event-Causing Subject 38
5.4.8 Vulnerability Assessments 38
5.5 RECORDS ARCHIVAL 39
5.5.1 Types of Records Archived 39
5.5.2 Retention Period for Archive 39
5.5.3 Protection of Archive 39
5.5.4 Archive Back-Up Procedures 39
5.5.5 Requirements for Time-Stamping of Records 39
5.5.6 Archive Collection System (Internal or External) 40
5.5.7 Procedures to Obtain and Verify Archive Information 40
5.6 KEY CHANGEOVER 40
5.6.1 Device Certificate Key Changeover 40
5.6.2 DCA Key Changeover 40
5.7 COMPROMISE AND DISASTER RECOVERY 41
5.7.1 Incident and Compromise Handling Procedures 41
5.7.2 Computing Resources, Software and/or Data are Corrupted 42
5.7.3 Entity Private Key Compromise Procedures 42
5.7.4 Business Continuity Capabilities after a Disaster 42
5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION 43
6 TECHNICAL SECURITY CONTROLS 43
6.1 KEY PAIR GENERATION AND INSTALLATION 43
6.1.1 Key Pair Generation 43
6.1.2 Private Key Delivery to Subscriber 43
6.1.3 Public Key Delivery to Certificate Issuer 44
6.1.4 DCA Public Key Delivery to Relying Parties 44
6.1.5 Key Sizes 44
6.1.6 Public Key Parameters Generation and Quality Checking 44
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 45
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 45
6.2.1 Cryptographic Module Standards and Controls 45
6.2.2 Private Key (n out of m) Multi-Person Control 46
6.2.3 Private Key Escrow 46
6.2.4 Private Key Back-Up 46
6.2.5 Private Key Archival 47
6.2.6 Private Key Transfer into or from a Cryptographic Module 47
6.2.7 Private Key Storage on Cryptographic Module 47
6.2.8 Method of Activating Private Key 47
6.2.9 Method of Deactivating Private Key 48
6.2.10 Method of Destroying Private Key 48
6.2.11 Cryptographic Module Rating 48
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 48
6.3.1 Public Key Archival 48
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 48

6.4 ACTIVATION DATA 49
6.4.1 Activation Data Generation and Installation 49
6.4.2 Activation Data Protection 49
6.4.3 Other Aspects of Activation Data 49
6.5 COMPUTER SECURITY CONTROLS 49
6.5.1 Specific Computer Security Technical Requirements 49
6.5.2 Computer Security Rating 50
6.6 LIFE-CYCLE TECHNICAL CONTROLS 50
6.6.1 System Development Controls 50
6.6.2 Security Management Controls 50
6.6.3 Life-Cycle Security Controls 51
6.7 NETWORK SECURITY CONTROLS 51
6.7.1 Use of Offline Root DCA 51
6.7.2 Protection Against Attack 51
6.7.3 Separation of Issuing DCA 51
6.7.4 Health Check of DCA Systems 51
6.8 TIME-STAMPING 52
6.8.1 Use of Time-Stamping 52
7 CERTIFICATE, CRL AND OCSP PROFILES 53
7.1 CERTIFICATE PROFILES 53
7.1.1 Version Number(s) 53
7.1.2 Certificate Extensions 53
7.1.3 Algorithm Object Identifiers 53
7.1.4 Name Forms 53
7.1.5 Name Constraints 53
7.1.6 Certificate Policy Object Identifier 53
7.1.7 Usage of Policy Constraints Extension 53
7.1.8 Policy Qualifiers Syntax and Semantics 53
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 53
7.2 CRL PROFILE 53
7.2.1 Version Number(s) 54
7.2.2 CRL and CRL Entry Extensions 54
7.3 OCSP PROFILE 54
7.3.1 Version Number(s) 54
7.3.2 OCSP Extensions 54
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 55
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 55
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 55
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 55
8.4 TOPICS COVERED BY ASSESSMENT 55
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 55
8.6 COMMUNICATION OF RESULTS 55
9 OTHER BUSINESS AND LEGAL MATTERS 56
9.1 FEES56
9.1.1 Certificate Issuance or Renewal Fees 56
9.1.2 Device Certificate Access Fees 56
9.1.3 Revocation or Status Information Access Fees 56
9.1.4 Fees for Other Services 56
9.1.5 Refund Policy 56
9.2 FINANCIAL RESPONSIBILITY 56

9.2.1 Insurance Coverage 56
9.2.2 Other Assets 56
9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects 56
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 57
9.3.1 Scope of Confidential Information 57
9.3.2 Information not within the Scope of Confidential Information 57
9.3.3 Responsibility to Protect Confidential Information 57
9.4 PRIVACY OF PERSONAL INFORMATION 57
9.4.1 Privacy Plan 57
9.4.2 Information Treated as Private 57
9.4.3 Information not Deemed Private 57
9.4.4 Responsibility to Protect Private Information 57
9.4.5 Notice and Consent to Use Private Information 57
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 57
9.4.7 Other Information Disclosure Circumstances 57
9.5 INTELLECTUAL PROPERTY RIGHTS 58
9.6 REPRESENTATIONS AND WARRANTIES 58
9.6.1 Certification Authority Representations and Warranties 58
9.6.2 Registration Authority Representations and Warranties 58
9.6.3 Subscriber Representations and Warranties 58
9.6.4 Relying Party Representations and Warranties 58
9.6.5 Representations and Warranties of Other Participants 58
9.7 DISCLAIMERS OF WARRANTIES 58
9.8 LIMITATIONS OF LIABILITY 58
9.9 INDEMNITIES 58
9.10 TERM AND TERMINATION 58
9.10.1 Term 58
9.10.2 Termination of Device Certificate Policy 59
9.10.3 Effect of Termination and Survival 59
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 59
9.11.1 Subscribers 59
9.11.2 Device Certification Authority 59
9.11.3 Notification 59
9.12 AMENDMENTS 59
9.12.1 Procedure for Amendment 59
9.12.2 Notification Mechanism and Period 59
9.12.3 Circumstances under which OID Must be Changed 59
9.13 DISPUTE RESOLUTION PROVISIONS 59
9.14 GOVERNING LAW 59
9.15 COMPLIANCE WITH APPLICABLE LAW 60
9.16 MISCELLANEOUS PROVISIONS 60
9.16.1 Entire Agreement 60
9.16.2 Assignment 60
9.16.3 Severability 60
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 60
9.16.5 Force Majeure 60
9.17 OTHER PROVISIONS 60
9.17.1 Device Certificate Policy Content 60
9.17.2 Third Party Rights 60
Annex A: Definitions and Interpretation 61

SEC - Appendix A: February 2016 Consultation (showing changes in mark-up from last published version)

Annex B: DCA CERTIFICATE AND DEVICE CERTIFICATE PROFILES 67

1 INTRODUCTION

The document comprising this Appendix A (together with its Annexes A and B):

- shall be known as the " **Device Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) Device Certificates; and

(ii) DCA Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New` font;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(iii) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been assigned an OID of 1.2.826.0.1. 8641679.1.2.1.2.

1.3 SMKI PARTICIPANTS

1.3.1 The Device Certification Authority

(A) The definition of Device Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SMKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SMKI RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code.

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of a Device Certificate must be a Device (other than a Type 2 Device) represented by the identifier in the `subjectAltName` field of the Device Certificate Profile in accordance with Annex B.

(B) The Subject of a DCA Certificate must be the entity identified by the `subject` field of the Root DCA Certificate Profile or Issuing DCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code.

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF DEVICE CERTIFICATES AND DCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The DCA shall ensure that Device Certificates are Issued only:

(i) subject to paragraph (B), to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Devices in accordance with or pursuant to the Code.

(B) For the purposes of paragraph (A), the DCA may treat any of the following as if they were an Eligible Subscriber:

(i) in relation to a Device that has an SMI Status that is not set to

'commissioned' or 'installed not commissioned', any Authorised Subscriber; or

(ii) in relation to a Device that has an SMI Status of 'commissioned' or 'installed not commissioned', the DCC or any Authorised Subscriber that is a User which acts (or is to act) in the User Role of either Import Supplier or Gas Supplier.

(C) The DCA shall ensure that DCA Certificates are Issued only to the DCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the Root DCA; and

(ii) in its capacity as, and for the purposes of exercising the functions of, the Issuing DCA.

(D) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(A) No Party shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the DCA or the SMKI PMA.

1.5.3 Person Determining Device CPS Suitability for the Policy

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the SMKI PMA to approve the Device CPS.

1.5.4 Device CPS Approval Procedures

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the procedure by which the SMKI PMA may approve the Device CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The Registration Authority Policies and Procedures (the **SMKI RAPP**) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

(A) Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The DCA shall lodge copies of the following in the SMKI Repository:

(i) each Device Certificate that has been accepted by a Subscriber;

(ii) each DCA Certificate;

(iii) each version of the SMKI RAPP;

(iv) each version of the SMKI Recovery Procedure; and

(v) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

(B) The DCA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The DCA shall ensure that:

(i) each Device Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each DCA Certificate is lodged to the SMKI Repository promptly on being Issued;

(iii) the SMKI RAPP is lodged in the SMKI Repository, and a revised

version of the SMKI RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) the SMKI Recovery Procedure is lodged in the SMKI Repository, and a revised version of the SMKI Recovery Procedure is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code; and

(v) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Provision is made in the SMKI RAPP to:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) permit the DCA to Authenticate each Eligible Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

(A) Provision is made in the SMKI RAPP in relation to:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP in relation to the:

(i) procedure to be followed by a Party in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the DCA will determine whether a Party is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party shall be Authenticated by the DCA for that purpose.

(B) Provision is made in the SMKI RAPP for the purpose of ensuring that the criteria in accordance with which the DCA shall Authenticate a Party shall be set to Level 3 pursuant to GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.4 Authentication of Devices

(A) Provision is made in the SMKI RAPP in relation to the Authentication of Devices.

3.2.5 Non-verified Subscriber Information

(A) The DCA shall:

(i) verify all information in relation to DCA Certificates;

(ii) require each Eligible Subscriber to verify the information contained in any Certificate Signing Request in respect of a Device Certificate.

(B) Further provision on the content of DCA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.6 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.7 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The DCA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

[*Not applicable in this Policy*]

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

(A) Provision is made in the SMKI RAPP in relation to:

(i) in respect of a Device Certificate:

(a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System; and

(ii) in respect of a DCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a DCA Certificate.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made where applicable in the SMKI RAPP in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber or Authorised Subscriber in its capacity as such; and

(ii) maintenance by the DCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP in relation to the establishment of an enrolment process in respect of DCA Personnel and DCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the DCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP in relation to the Authentication by the DCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the DCA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) may give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the DCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the DCA

is made in Section L8 of the Code (SMKI Performance Standards and Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 DCA Actions during Certificate Issuance

(A) The DCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy and the SMKI RAPP; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the SMKI RAPP.

(B) The DCA shall ensure that:

(i) each DCA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each Device Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) A DCA Certificate may only be:

(i) Issued by the DCA; and

(ii) for that purpose, signed using the Root DCA Private Key.

(D) A Device Certificate may only be:

(i) Issued by the DCA; and

(ii) for that purpose, signed using an Issuing DCA Private Key.

(E) The DCA shall not Issue a Device Certificate which is signed using an Issuing DCA Private Key after the first in time of the following:

(i) the time which is three months after the time at which any element of the Issuing DCA Private Key first became operational;

(ii) the time at which the DCA Issues the 100,000th Device Certificate which is signed using that Issuing DCA Private Key.

(F) For the purposes of paragraph (E), the DCA shall ensure that the Device CPS incorporates:

(i) a procedure for determining:

(a) how the DCA will calculate when each of the times specified in that paragraph occurs; and

(b) for that purpose, when any element of the Issuing DCA Private Key first became operational; and

(ii) provisions for notifying the SMKI PMA when either of the times specified in that paragraph is approaching.

(G) The DCA shall not issue a Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously issued by it.

4.3.2 Notification to Eligible Subscriber by the DCA of Issuance of Certificate

(A) Provision is made in the SMKI RAPP for the DCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the SMKI RAPP to:

(i) specify a means by which an Eligible Subscriber may clearly indicate to the DCA its rejection of a Certificate which has been Issued to it; and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued, and which has not rejected it, is treated as having accepted

that Certificate.

(B) A Certificate which has been Issued by the DCA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

(C) The DCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(D) Further provision in relation to the rejection and acceptance of Certificates is made in Section L11 of the Code (Subscriber Obligations).

4.4.2 Publication of Certificates by the DCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate Issuance by the DCA to Other Entities

(A) The DCA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11 of the Code (Subscriber Obligations); and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates

(B) The DCA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where any DCA System or any DCA Private Key is (or is suspected by the DCA of being) Compromised, the DCA shall:

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to a DCA Private Key:

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any Device Certificates Issued using that Private Key; and

(c) promptly both notify the SMKI PMA and verifiably destroy the DCA Private Key Material.

(B) Where the Root DCA Private Key is Compromised (or is suspected by the DCA of being Compromised), the DCA:

(i) may issue a replacement for any DCA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that DCA Certificate applies for the Issue of a new Certificate in accordance with this Policy.

(C) An Eligible Subscriber may request a replacement for a Certificate at any time by applying for the Issue of a new Device Certificate in accordance with this Policy.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the DCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the DCA to Other Entities

See Part 4.4.3 of this Policy

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The DCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated by a Device, the Eligible Subscriber which is responsible for that Device shall apply for the Issue of a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

4.7.6 Publication of the Re-Keyed Certificate by the DCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the DCA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the DCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) This Policy does not support the revocation or suspension of Certificates.

(B) The DCA shall not provide any service of revoking or suspending a Certificate.

4.9.2 Who can Request Revocation

[*Not applicable in this Policy*]

4.9.3 Procedure for Revocation Request

[*Not applicable in this Policy*]

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which DCA must process the Revocation Request

[*Not applicable in this Policy*]

4.9.6 Revocation Checking Requirements for Relying Parties

[*Not applicable in this Policy*]

4.9.7 CRL Issuance Frequency (if applicable)

[*Not applicable in this Policy*]

4.9.8 Maximum Latency for CRLs (if applicable)

[*Not applicable in this Policy*]

4.9.9 On-line Revocation/Status Checking Availability

[*Not applicable in this Policy*]

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

[*Not applicable in this Policy*]

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The DCA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[*Not applicable in this Policy*]

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The DCA shall ensure that the DCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The DCA shall ensure that:

(i) all of the physical locations in which the DCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The DCA shall ensure that the DCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with:

(i) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(ii) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

(E) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the DCA are stored in secure

containers accessible only to appropriately authorised individuals.

(F) The DCA shall ensure that the DCA Systems are Separated from any OCA Systems, save that any Systems used for the purposes of the Registration Authority functions of the DCA and OCA shall not require to be Separated.

5.1.2 Physical Access

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to DCA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the DCA Systems are situated.

5.1.4 Water Exposure

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to water exposure at all physical locations in which the DCA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the DCA Systems are situated.

5.1.6 Media Storage

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the DCA.

5.1.7 Waste Disposal

(A) The DCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the DCA are disposed of only using secure methods of disposal in accordance with:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time.

5.1.8 Off-Site Back-Up

(A) The DCA shall regularly carry out a Back-Up of:

(i) all Data held on the DCA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the DCA shall ensure that the Device CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The DCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the Device CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise DCA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The DCA shall ensure that, where any elements of the DCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of DCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The DCA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the DCA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of DCA Personnel has a clearly defined level of access to the DCA Systems and the premises in which they are located;

(iii) no individual member of DCA Personnel is capable, by acting alone, of engaging in any action by means of which the DCA Systems may

be Compromised to a material extent; and

(iv) the Device CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the DCA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of DCA Personnel; and

(ii) the application of controls to the actions of all members of DCA Personnel who are Privileged Persons, identifying in particular any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions.

(B) The DCA shall ensure that the Device CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) DCA Systems administration;

(ii) DCA Systems operations;

(iii) DCA Systems security; and

(iv) DCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The DCA shall ensure that all DCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the DCA, not have been previously relieved of any past assignment (whether for the DCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The DCA shall ensure that all DCA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of DCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be

undertaken by members of DCA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of DCA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the DCA in this Policy include references to persons with whom the DCA contracts in order to secure performance of its obligations as the DCA.

5.3.8 Documentation Supplied to Personnel

(A) The DCA shall ensure that all DCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the Device CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The DCA shall ensure that:

(i) the DCA Systems record all systems activity in an audit log;

(ii) the Device CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of DCA Personnel;

(b) the use of DCA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the DCA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the DCA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The DCA shall ensure that:

(i) the audit logging functionality in the DCA Systems is fully enabled at all times;

(ii) all DCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the DCA Systems in compliance with:

(a) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(b) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time;

(B) The DCA shall ensure that the Device CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The DCA shall ensure that the Device CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of DCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The DCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The DCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The DCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the DCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The DCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the Device CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the DCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The DCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The DCA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The DCA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The DCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the DCA's operations.

(B) The DCA shall ensure that the Device CPS incorporates provisions in relation to the periodic verification by the DCA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 Device Certificate Key Changeover

(A) The DCA shall Issue a new Device Certificate in relation to a Device where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI RAPP and this Policy.

5.6.2 DCA Key Changeover

(A) Where the DCA ceases to use an Issuing DCA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) verifiably destroy the Issuing DCA Private Key Material;

(ii) not revoke the related Issuing DCA Certificate (which may continue to be used for the purpose of validating Digital Signatures generated

using the Issuing DCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any Device Certificate subsequently Issued by it is Issued using the Issuing DCA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(v) in its capacity as the Root DCA:

(a) Issue a new Issuing DCA Certificate; and

(b) promptly lodge that Issuing DCA Certificate in the SMKI Repository.

(B) The DCA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The DCA shall ensure that the Device CPS incorporates a business continuity plan which shall be designed to ensure continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the DCA Systems or major failure in the DCA processes.

(B) The DCA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) In the event of the Compromise of any DCA Private Key, the DCA shall:

(i) not revoke the related Issuing DCA Certificate;

(ii) not revoke any Device Certificates Issued using the Issuing DCA Private Key;

(iii) not issue any further Device Certificates using the Issuing DCA Private Key;

(iv) treat the event in the same manner as if it were a Major Security Incident in accordance with Section G2 of the Code (System Security: Obligations on the DCC); and

(v) immediately notify the SMKI PMA.

(D) The DCA shall ensure that the Device CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any Issuing DCA Private Key or any part of the DCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The DCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The DCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery

of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[*Not applicable in this Policy*]

6 TECHNICAL SECURITY CONTROLS

The DCA shall ensure that the Device CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root DCA, the Issuing DCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The DCA shall ensure that all Key Pairs which it uses for the purposes of this Policy are generated:

(i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);

(ii) using multi-person control, such that no single Privileged Person is capable of generating any DCA Key; and

(iii) using random numbers which are such as to make it computationally infeasible to regenerate those Key Pairs even with knowledge of when and by means of what equipment they were generated.

(B) The DCA shall not generate any Private Key or Public Key other than a DCA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the DCA shall not generate any Private

Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root DCA and Issuing DCA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 DCA Public Key Delivery to Relying Parties

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the manner by which each DCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the DCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The DCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the size and characteristics set out in the GB Companion Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The DCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known

attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 `keyUsage` Field)

(A) The DCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The DCA shall ensure that each Device Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The DCA shall ensure that each DCA Certificate that is Issued by it has a `keyUsage` of `keyCertSign`.

(D) The DCA shall ensure that no `keyUsage` values may be set in a Device Certificate or DCA Certificate other than in accordance with this Part 6.1.7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The DCA shall ensure that all DCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The DCA shall ensure that all DCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information

Processing Standard which updates or replaces it from time to time).

(C) The DCA shall ensure that no DCA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The DCA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Device CPS; and

(ii) require to be unblocked by an authorised member of DCA Personnel who has been Authenticated as such following a process which shall be set out in the Device CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The DCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The DCA may Back-Up DCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up

within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing DCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The DCA shall ensure that no DCA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The DCA shall ensure that no DCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services;

(ii) in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The DCA shall ensure that the Cryptographic Module in which any DCA Private Key is stored may be accessed only by an authorised member of DCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The DCA shall ensure that any DCA Private Key shall be capable of being de-activated by means of the DCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the Device CPS.

6.2.10 Method of Destroying Private Key

(A) The DCA shall ensure that the Device CPS incorporates provisions for the exercise of strict controls in relation to the destruction of DCA Keys.

(B) The DCA shall ensure that no DCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the DCA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The DCA shall ensure that it archives DCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The DCA shall ensure that:

(i) the Validity Period of each Certificate shall be an indefinite period;

and

(ii) for this purpose, it uses the `notAfter` value specified in Annex B.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The DCA shall ensure that any Cryptographic Module within which a DCA Key is held has Activation Data that are unique and unpredictable.

(B) The DCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the DCA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the DCA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The DCA shall ensure that the Device CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the

DCA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in DCA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the DCA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for DCA Keys.

6.5.2 Computer Security Rating

(A) The DCA shall ensure that the Device CPS incorporates provisions relating to the appropriate security rating of the DCA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The DCA shall ensure that any software which is developed for the purpose of establishing a functionality of the DCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The DCA shall ensure that the Device CPS incorporates provisions which are designed to ensure that the DCA Systems satisfy the requirements of

Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root DCA

(A) The DCA shall ensure that its functions as the Root DCA are carried out on a part of the DCA Systems that is neither directly nor indirectly connected to any System which is not a part of the DCA Systems.

6.7.2 Protection Against Attack

(A) The DCA shall use its best endeavours to ensure that the DCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event;

(ii) any unauthorised attempt to connect to them.

(B) The DCA shall ~~use its reasonable endeavours~~take reasonable steps to ensure that the DCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing DCA

(A) The DCC shall ensure that, where its functions as the Issuing DCA are carried out on a part of the DCA Systems that is connected to an external network, they are carried out on a System that is Separated from all other DCA Systems.

6.7.4 Health Check of DCA Systems

(A) The DCA shall ensure that, in relation to the DCA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

(A) The DCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other DCA activities which require an accurate record of time.

(B) The DCA shall ensure that the Device CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the DCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

The DCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

[*Not applicable in this Policy*]

7.2.2 CRL and CRL Entry Extensions

[*Not applicable in this Policy*]

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 Device Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of Device Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 Device Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Device Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy.
Authentication	means the process of establishing that an individual, organisation, System or Device is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).
Authorised Subscriber	means a Party or RDP which has successfully completed the procedures set out in the SMKI RAPP and has been authorised by the DCA to submit a Certificate Signing Request.

Certificate	means either a Device Certificate or a DCA Certificate.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.
Certificate Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.
DCA Key	means any Private Key or a Public Key generated by the DCA for the purposes of complying with its obligations under the Code.
DCA Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCA.
DCA Private Key	means a DCA Key which is a Private Key.
DCA Systems	means the Systems used by the DCA in relation to the SMKI Services.
DCA Certificate	means either a Root DCA Certificate or an Issuing DCA Certificate.
Device Certificate	means a certificate in the form set out in the Device Certificate Profile in accordance with Annex B, and Issued by the Issuing DCA in accordance with this Policy.
Device Certification Authority (or **DCA**)	means the DCC, acting in the capacity and exercising the functions of one or more of: (a) the Root DCA; (b) the Issuing DCA; and (c) the Registration Authority.

Eligible Subscriber	means: (a) in relation to a Device Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.16 of the Code (Device Certificates); and (b) in relation to a DCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.17 of the Code (DCA Certificates).
Issue	means the act of the DCA, in its capacity as the Root DCA or Issuing DCA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "**Issued**" and "**Issuing**" shall be interpreted accordingly).
Issuing Device Certification Authority (or **Issuing DCA**)	means the DCC exercising the function of Issuing Device Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.
Issuing DCA Certificate	means a certificate in the form set out in the Issuing DCA Certificate Profile in accordance with Annex B, and Issued by the Root DCA to the Issuing DCA in accordance with this Policy.
Issuing DCA Private Key	means a Private Key which is stored and managed by the DCA acting in its capacity as the Issuing DCA.
Issuing DCA Public Key	means the Public Key which is part of a Key Pair with an Issuing DCA Private Key.
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.

Object Identifier (or **OID**)	means an Object Identifier assigned by the Internet Address Naming Authority.
OCA	has the meaning given to that expression in Appendix B of the Code (Organisation Certificate Policy).
OCA Systems	has the meaning given to that expression in Appendix B of the Code (Organisation Certificate Policy).
Policy	means this Device Certificate Policy.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Registration Authority	means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.
Registration Authority Manager	means either a director of the DCC or any other person who may be identified as such in accordance with the SMKI RAPP.
Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.
Relying Party	means a person who, pursuant to the Code, receives and relies upon a Certificate.
Root Device Certification Authority (or **Root DCA**)	means the DCC exercising the function of Issuing DCA Certificates to the Issuing DCA and storing and managing Private Keys associated with that function.
Root DCA Certificate	means a certificate in the form set out in the Root DCA Certificate Profile in accordance with Annex B and self-signed by the Root DCA in accordance with this Policy.

Root DCA Private Key	means a Private Key which is stored and managed by the DCA acting in its capacity as the Root DCA.
Security Related Functionality	means the functionality of the DCA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.
Subject	means: (a) in relation to a Device Certificate, the Device identified by the Device ID in the `hwSerialNum` field of the Device Certificate Profile in Annex B; and (b) in relation to a DCA Certificate, the Root DCA or Issuing DCA as identified by the `subject` field of the relevant Certificate Profile in Annex B.
Subscriber	means, in relation to any Certificate, a Party or RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.
Time-Stamping	means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.
Time-Stamping Authority	means that part of the DCA that: (a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and (b) relies on a time source that is: (i) accurate;

(ii) determined in a manner that is independent of any other part of the DCA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: DCA Certificate and Device Certificate Profiles

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which DCA Certificates and Device Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5759 or IETF RFC5280.

Common requirements applicable to DCA Certificates and Device Certificates

All DCA Certificates and Device Certificates that are validly authorised within the SMKI for use within the scope of the GB Companion Specification and GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all DCA Certificates and Device Certificates shall:
    - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root DCA Certificate;
    - contain the `keyUsage` extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- only contain Public Keys of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
- contain a `certificatePolicies` extension containing at least one `CertPolicyID` which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Devices shall interpret this extension;
- contain a `serialNumber` of no more than 16 octets in length;
- contain a `subjectKeyIdentifier` which shall be marked as non-critical;

- contain an `authorityKeyIdentifier` in the form `[0] KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the Root DCA Certificate;
- only contain `KeyIdentifiers` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
- contain an `issuer` field whose contents MUST be identical to the contents of the signer's `subject` field in the signer's Certificate;
- have a valid `notBefore` field consisting of the time of issue encoded and a valid `notAfter` field for a not well-defined expiraton date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Device Certificates only

All Device Certificates that are issued by the DCA shall:

- not have a well-defined expiration date and so the `notAfter` shall be assigned the `GeneralizedTime` value of 99991231235959Z;
- have an empty `subject` field;
- contain `subjectAltName` extension which contains a single `GeneralName` of type `otherName` that is further sub-typed as a `hardwareModuleName` (id-on-`hardwareModuleName`) as defined in RFC 4108. The `hwSerialNum` field shall be set to the Device's Entity Identifier. In adherence to IETF RFC 5280, the `subjectAltName` shall be marked as critical;
- contain a single Public Key;
- contain a keyUsage extension marked as critical, with a value of only one of:
  - `digitalSignature`; or
  - `keyAgreement`.
- contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID applicable to the version of this Device Certificate Policy applicable at the time that the Device Certificate was issued.

Requirements applicable to the Root DCA and Issuing DCA

All DCA Certificates issued by the DCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the `GeneralizedTime` value of 99991231235959Z;
- must have a Valid `notBefore` field consisting of the time of issue encoded as per RFC5280;
- Per RFC5280, the IssuerName of any certificates MUST be identical to the signer's `subject`;
- have a globally unique `subject`;
- contain a single Public Key;
- contain a `keyUsage` extension marked as critical and defined as `keyCertSign;`
- For Issuing DCA Certificates contain at least one `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of the version of this Device Certificate Policy prevailing at the time.
- For the Root DCA Certificate contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID for `anyPolicy`.
- For Issuing DCA Certificates, contain the `basicConstraints` extension, with values `cA`=True, and `pathLen`=0. This extension shall be marked as critical.
- For the Root DCA Certificate, contain the `basicConstraints` extension, with the value `cA=True` and `pathLen absent` (unlimited). This extension shall be marked as critical.

Device Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to	

		16 Octets	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the Device Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAnd	UTF8String	EMPTY	

`Value` structure within the `subject` field whose `type` is `id-at-commonName` (the "Subject X520 Common Name")			
`subjectAltName`	`OtherName`	contains a single `GeneralName` of type `OtherName` that is further sub-typed as a `HardwareModuleName` (`id-on-hardwareModuleName`) as defined in RFC 4108. The `hwSerialNum` field shall be set to the Device's Entity Identifier	
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The Subject's Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject Device Certificate signature	

Interpretation

`version`

The version of the X.509 Device Certificate. Valid Device Certificates shall identify themselves as version 3.

`serialNumber`

Device Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Device Certificate, and shall be created by the Issuing DCA that signs the Device Certificate. The `serialNumber` shall be unique in the scope of Device Certificate signed by the Issuing DCA.

`signature`

The identity of the signature algorithm used to sign the Device Certificate. The field is identical to the value of the Device Certificate `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading below.

Issuer X520 Common Name

The name of the signer of the Device Certificate. This will be the gloablly unique name of the Issuing DCA of up to 4 Octets (as defined in the Issuing DCA Certificate Profile).

Authority Key Identifier

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all Device Certificates.

Subject Key Identifier

The Subject Key Identifier extension should be included and marked as non-critical in the Device Certificate.

`validity`

The time period over which the Issuing DCA expects the Device Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Device Certificate may be used. This shall be the time the Device Certificate is created.

`notAfter`

The latest time a Device Certificate is expected to be used. Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be EMPTY.

`subjectAltName`

The non-critical `subjectAltName` extension shall contain a single `GeneralName` of type `OtherName` that is further sub-typed as a `HardwareModuleName` (`id-on-hardwareModuleName`) as defined in RFC 4108. The `hwSerialNum` field shall be set to the Device ID.

`subjectPublicKeyInfo`

The Device Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Device Certificate extension (explained further under the next **`extensions`** heading below).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
  }
```

Only the following field in ECParameters shall be used:

- `o namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in Device Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Issuing DCA signature algorithm used to sign this Device Certificate is as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Issuing DCA's signature of the Device Certificate shall be computed using the Issuing DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Device Certificates shall contain the extensions described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `subjectAltName`
- `keyUsage`
- `authorityKeyIdentifier`
- `subjectKeyIdentifier`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root DCA Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to 16 Octets	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Issuer X520 Common Name")	`UTF8String`	Globally unique common name of Root DCA of up to 4 Octets	
`keyIdentifier` in `subjectKeyIdentifier` (the "Subject Key Identifider")	`keyIdentifier`	A unique value that matches the `subjectKeyIdentifier` of the issuer's credential	

notBefore	Time	Creation time of the Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Root DCA of up to 4 Octets (same as Issuer name)	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the Devices SMKI.

version

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Certificate, and shall be created by the DCA that signs the Certificate (self-signed by Root DCA). The `serialNumber` shall be unique in the scope of Certificates signed by the DCA.

signature

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root DCA Certificate's `signatureAlgorithm` field explained further under the next signatureAlgorithm heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root DCA of up to 4 Octets. This will be the same as the `subject` as it is self-signed by the Root DCA.

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

validity

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

Root DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Root DCA certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field must be populated with the globally unique name of the Root DCA of up to 4 Octets.

subjectPublicKeyInfo

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the Key Usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
     namedCurve         OBJECT IDENTIFIER
     -- implicitCurve   NULL
     -- specifiedCurve  SpecifiedECDomain
```

```
}
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular

  set of elliptic curve domain parameters to be represented by an

  `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in DCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root DCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root DCA's signature of the Certificate shall be computed using the Root DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading .

The structure for ECDSA signatures shall be as per RFC 5480.

extensions

Certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

Extensions:

- certificatePolicy
- keyUsage
- basicConstraints
- subjectKeyIdentifer

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference

version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique name of Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile)	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
notBefore	Time	Creation time of the certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of	

		99991231235959Z	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Subject X520 Common Name")	`UTF8String`	Globally unique name of Issuing DCA of up to 4 Octets	
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The Subject's Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject certificate signature	

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Certificate, and shall be created by the Issuing DCA that signs the Certificate. The `serialNumber` shall be unique in the scope of Certificates signed by the Root DCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing DCA Certificate's `signatureAlgorithm` field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root DCA of up to 4 Octets (as defined in the Root DCA Certificate Profile).

Subject Key Identifier

The `subjectKeyIdentifier` extension should be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `authorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all device Certificates.

`validity`

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

Issuing DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Issuing DCA certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

Subject X520 Common Name

This field shall be populated with the globally unique name of the Issuing DCA of up to 4 Octets.

subjectPublicKeyInfo

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next **extensions** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
```

```
}
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular

  set of elliptic curve domain parameters to be represented by an

  `OBJECT IDENTIFIER`.

The object identifier for the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root DCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root DCA's signature of the Certificate shall be computed using the Root DCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Issuing-CA certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`
- `authorityKeyIdentifier`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-
sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

APPENDIX B – ORGANISATION CERTIFICATE POLICY

CONTENTS

Part	Heading	Page
1	INTRODUCTION	8
1.1	OVERVIEW	8
1.2	DOCUMENT NAME AND IDENTIFICATION	8
1.3	SMKI PARTICIPANTS	8
1.3.1	The Organisation Certification Authority	8
1.3.2	Registration Authorities	9
1.3.3	Subscribers	9
1.3.4	Subjects	9
1.3.5	Relying Parties	10
1.3.6	SMKI Policy Management Authority	10
1.3.7	SMKI Repository Provider	10
1.4	USAGE OF ORGANISATION CERTIFICATES AND OCA CERTIFICATES	10
1.4.1	Appropriate Certificate Uses	10
1.4.2	Prohibited Certificate Uses	11
1.5	POLICY ADMINISTRATION	11
1.5.1	Organisation Administering the Document	11
1.5.2	Contact Person	11
1.5.3	Person Determining Organisation CPS Suitability for the Policy	11
1.5.4	Organisation CPS Approval Procedures	11
1.5.5	Registration Authority Policies and Procedures	11
1.6	DEFINITIONS AND ACRONYMS	12
1.6.1	Definitions	12
1.6.2	Acronyms	12
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	13
2.1	REPOSITORIES	13
2.2	PUBLICATION OF CERTIFICATION INFORMATION	13
2.3	TIME OR FREQUENCY OF PUBLICATION	13
2.4	ACCESS CONTROLS ON REPOSITORIES	14
3	IDENTIFICATION AND AUTHENTICATION	15
3.1	NAMING	15
3.1.1	Types of Names	15
3.1.2	Need for Names to be Meaningful	15
3.1.3	Anonymity or Pseudonymity of Subscribers	15
3.1.4	Rules for Interpreting Various Name Forms	15
3.1.5	Uniqueness of Names	15
3.1.6	Recognition, Authentication, and Role of Trademarks	15
3.2	INITIAL IDENTITY VALIDATION	15
3.2.1	Method to Prove Possession of Private Key	15
3.2.2	Authentication of Organisation Identity	16
3.2.3	Authentication of Individual Identity	16
3.2.4	Non-verified Subscriber Information	17

3.2.5 Validation of Authority 17
3.2.6 Criteria for Interoperation 17
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 17
3.3.1 Identification and Authentication for Routine Re-Key 17
3.3.2 Identification and Authentication for Re-Key after Revocation 17
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 17
3.4.1 Authentication for Certificate Revocation Requests 17
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 18
4.1 CERTIFICATE APPLICATION 18
4.1.1 Submission of Certificate Applications 18
4.1.2 Enrolment Process and Responsibilities 18
4.1.3 Enrolment Process for the Registration Authority and its Representatives 18
4.2 CERTIFICATE APPLICATION PROCESSING 19
4.2.1 Performing Identification and Authentication Functions 19
4.2.2 Approval or Rejection of Certificate Applications 19
4.2.3 Time to Process Certificate Applications 19
4.3 CERTIFICATE ISSUANCE 20
4.3.1 OCA Actions during Certificate Issuance 20
4.3.2 Notification to Eligible Subscriber by the OCA of Issuance of Certificate 21
4.4 CERTIFICATE ACCEPTANCE 21
4.4.1 Conduct Constituting Certificate Acceptance 21
4.4.2 Publication of Certificates by the OCA 21
4.4.3 Notification of Certificate Issuance by the OCA to Other Entities 22
4.5 KEY PAIR AND CERTIFICATE USAGE 22
4.5.1 Subscriber Private Key and Certificate Usage 22
4.5.2 Relying Party Public Key and Certificate Usage 22
4.6 CERTIFICATE RENEWAL 22
4.6.1 Circumstances of Certificate Renewal 22
4.6.2 Circumstances of Certificate Replacement 22
4.6.3 Who May Request a Replacement Certificate 23
4.6.4 Processing Replacement Certificate Requests 23
4.6.5 Notification of Replacement Certificate Issuance to a Subscriber 23
4.6.6 Conduct Constituting Acceptance of a Replacement Certificate 24
4.6.7 Publication of a Replacement Certificate by the OCA 24
4.6.8 Notification of Certificate Issuance by the OCA to Other Entities 24
4.7 CERTIFICATE RE-KEY 24
4.7.1 Circumstances for Certificate Re-Key 24
4.7.2 Who may Request Certification of a New Public Key 24
4.7.3 Processing Certificate Re-Keying Requests 24
4.7.4 Notification of New Certificate Issuance to Subscriber 24
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 24
4.7.6 Publication of the Re-Keyed Certificate by the OCA 24
4.7.7 Notification of Certificate Issuance by the OCA to Other Entities 25
4.8 CERTIFICATE MODIFICATION 25
4.8.1 Circumstances for Certificate Modification 25
4.8.2 Who may request Certificate Modification 25
4.8.3 Processing Certificate Modification Requests 25
4.8.4 Notification of New Certificate Issuance to Subscriber 25
4.8.5 Conduct Constituting Acceptance of Modified Certificate 25

4.8.6 Publication of the Modified Certificate by the OCA 25
4.8.7 Notification of Certificate Issuance by the OCA to Other Entities 25
4.9 CERTIFICATE REVOCATION AND SUSPENSION 26
4.9.1 Circumstances for Revocation 26
4.9.2 Who can Request Revocation 27
4.9.3 Procedure for Revocation Request 27
4.9.4 Revocation Request Grace Period 28
4.9.5 Time within which OCA must process the Revocation Request 28
4.9.6 Revocation Checking Requirements for Relying Parties 28
4.9.7 CRL Issuance Frequency (if applicable) 28
4.9.8 Maximum Latency for CRLs (if applicable) 29
4.9.9 On-line Revocation/Status Checking Availability 30
4.9.10 On-line Revocation Checking Requirements 30
4.9.11 Other Forms of Revocation Advertisements Available 30
4.9.12 Special Requirements in the Event of Key Compromise 30
4.9.13 Circumstances for Suspension 30
4.9.14 Who can Request Suspension 30
4.9.15 Procedure for Suspension Request 30
4.9.16 Limits on Suspension Period 30
4.10 CERTIFICATE STATUS SERVICES 30
4.10.1 Operational Characteristics 30
4.10.2 Service Availability 30
4.10.3 Optional Features 31
4.11 END OF SUBSCRIPTION 31
4.12 KEY ESCROW AND RECOVERY 31
4.12.1 Key Escrow and Recovery Policies and Practices 31
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 32
5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 33
5.1 PHYSICAL CONTROLS 33
5.1.1 Site Location and Construction 33
5.1.2 Physical Access 34
5.1.3 Power and Air Conditioning 34
5.1.4 Water Exposure 34
5.1.5 Fire Prevention and Protection 34
5.1.6 Media Storage 35
5.1.7 Waste Disposal 35
5.1.8 Off-Site Back-Up 35
5.2 PROCEDURAL CONTROLS 36
5.2.1 Trusted Roles 36
5.2.2 Number of Persons Required per Task 37
5.2.3 Identification and Authentication for Each Role 37
5.2.4 Roles Requiring Separation of Duties 37
5.3 PERSONNEL CONTROLS 38
5.3.1 Qualification, Experience and Clearance Requirements 38
5.3.2 Background Check Procedures 38
5.3.3 Training Requirements 38
5.3.4 Retraining Frequency and Requirements 38
5.3.5 Job Rotation Frequency and Sequence 38
5.3.6 Sanctions for Unauthorised Actions 39
5.3.7 Independent Contractor Requirements 39

5.3.8 Documentation Supplied to Personnel 39
5.4 AUDIT LOGGING PROCEDURES 39
5.4.1 Types of Events Recorded 39
5.4.2 Frequency of Processing Log 40
5.4.3 Retention Period for Audit Log 41
5.4.4 Protection of Audit Log 41
5.4.5 Audit Log Back-Up Procedures 42
5.4.6 Audit Collection System (Internal or External) 42
5.4.7 Notification to Event-Causing Subject 42
5.4.8 Vulnerability Assessments 43
5.5 RECORDS ARCHIVAL 43
5.5.1 Types of Records Archived 43
5.5.2 Retention Period for Archive 43
5.5.3 Protection of Archive 43
5.5.4 Archive Back-Up Procedures 43
5.5.5 Requirements for Time-Stamping of Records 43
5.5.6 Archive Collection System (Internal or External) 44
5.5.7 Procedures to Obtain and Verify Archive Information 44
5.6 KEY CHANGEOVER 44
5.6.1 Organisation Certificate Key Changeover 44
5.6.2 OCA Key Changeover 44
5.6.3 Subscriber Key Changeover 45
5.7 COMPROMISE AND DISASTER RECOVERY 46
5.7.1 Incident and Compromise Handling Procedures 46
5.7.2 Computing Resources, Software and/or Data are Corrupted 46
5.7.3 Entity Private Key Compromise Procedures 47
5.7.4 Business Continuity Capabilities after a Disaster 47
5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION 47
6 TECHNICAL SECURITY CONTROLS 48
6.1 KEY PAIR GENERATION AND INSTALLATION 48
6.1.1 Key Pair Generation 48
6.1.2 Private Key Delivery to Subscriber 48
6.1.3 Public Key Delivery to Certificate Issuer 48
6.1.4 OCA Public Key Delivery to Relying Parties 49
6.1.5 Key Sizes 49
6.1.6 Public Key Parameters Generation and Quality Checking 49
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 49
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 50
6.2.1 Cryptographic Module Standards and Controls 50
6.2.2 Private Key (m out of n) Multi-Person Control 51
6.2.3 Private Key Escrow 51
6.2.4 Private Key Back-Up 51
6.2.5 Private Key Archival 51
6.2.6 Private Key Transfer into or from a Cryptographic Module 52
6.2.7 Private Key Storage on Cryptographic Module 52
6.2.8 Method of Activating Private Key 52
6.2.9 Method of Deactivating Private Key 52
6.2.10 Method of Destroying Private Key 53

6.2.11 Cryptographic Module Rating 53
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 53
6.3.1 Public Key Archival 53
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 53
6.4 ACTIVATION DATA 54
6.4.1 Activation Data Generation and Installation 54
6.4.2 Activation Data Protection 54
6.4.3 Other Aspects of Activation Data 54
6.5 COMPUTER SECURITY CONTROLS 54
6.5.1 Specific Computer Security Technical Requirements 54
6.5.2 Computer Security Rating 55
6.6 LIFE-CYCLE TECHNICAL CONTROLS 55
6.6.1 System Development Controls 55
6.6.2 Security Management Controls 55
6.6.3 Life-Cycle Security Controls 56
6.7 NETWORK SECURITY CONTROLS 56
6.7.1 Use of Offline Root OCA 56
6.7.2 Protection Against Attack 56
6.7.3 Separation of Issuing OCA 56
6.7.4 Health Check of OCA Systems 56
6.8 TIME-STAMPING 57
6.8.1 Use of Time-Stamping 57
7 CERTIFICATE, CRL AND OCSP PROFILES 57
7.1 CERTIFICATE PROFILES 57
7.1.1 Version Number(s) 57
7.1.2 Certificate Extensions 57
7.1.3 Algorithm Object Identifiers 57
7.1.4 Name Forms 57
7.1.5 Name Constraints 57
7.1.6 Certificate Policy Object Identifier 58
7.1.7 Usage of Policy Constraints Extension 58
7.1.8 Policy Qualifiers Syntax and Semantics 58
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 58
7.2 CRL PROFILE 58
7.2.1 Version Number(s) 58
7.2.2 CRL and CRL Entry Extensions 58
7.3 OCSP PROFILE 58
7.3.1 Version Number(s) 58
7.3.2 OCSP Extensions 58
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 59
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 59
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 59
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 59
8.4 TOPICS COVERED BY ASSESSMENT 59
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 59
8.6 COMMUNICATION OF RESULTS 59
9 OTHER BUSINESS AND LEGAL MATTERS 60
9.1 FEES 60
9.1.1 Certificate Issuance or Renewal Fees 60
9.1.2 Organisation Certificate Access Fees 60

9.1.3 Revocation or Status Information Access Fees 60
9.1.4 Fees for Other Services 60
9.1.5 Refund Policy 60
9.2 FINANCIAL RESPONSIBILITY 60
9.2.1 Insurance Coverage 60
9.2.2 Other Assets 60
9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects 60
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 61
9.3.1 Scope of Confidential Information 61
9.3.2 Information not within the Scope of Confidential Information 61
9.3.3 Responsibility to Protect Confidential Information 61
9.4 PRIVACY OF PERSONAL INFORMATION 61
9.4.1 Privacy Plan 61
9.4.2 Information Treated as Private 61
9.4.3 Information not Deemed Private 61
9.4.4 Responsibility to Protect Private Information 61
9.4.5 Notice and Consent to Use Private Information 61
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 61
9.4.7 Other Information Disclosure Circumstances 61
9.5 INTELLECTUAL PROPERTY RIGHTS 62
9.6 REPRESENTATIONS AND WARRANTIES 62
9.6.1 Certification Authority Representations and Warranties 62
9.6.2 Registration Authority Representations and Warranties 62
9.6.3 Subscriber Representations and Warranties 62
9.6.4 Relying Party Representations and Warranties 62
9.6.5 Representations and Warranties of Other Participants 62
9.7 DISCLAIMERS OF WARRANTIES 62
9.8 LIMITATIONS OF LIABILITY 62
9.9 INDEMNITIES 62
9.10 TERM AND TERMINATION 62
9.10.1 Term 62
9.10.2 Termination of Organisation Certificate Policy 63
9.10.3 Effect of Termination and Survival 63
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 63
9.11.1 Subscribers 63
9.11.2 Organisation Certification Authority 63
9.11.3 Notification 63
9.12 AMENDMENTS 63
9.12.1 Procedure for Amendment 63
9.12.2 Notification Mechanism and Period 63
9.12.3 Circumstances under which OID Must be Changed 63
9.13 DISPUTE RESOLUTION PROVISIONS 63
9.14 GOVERNING LAW 64
9.15 COMPLIANCE WITH APPLICABLE LAW 64
9.16 MISCELLANEOUS PROVISIONS 64
9.16.1 Entire Agreement 64
9.16.2 Assignment 64
9.16.3 Severability 64
9.16.4 Enforcement (Attorney's Fees and Waiver of Rights) 64

9.16.5 Force Majeure 64
9.17 OTHER PROVISIONS 64
9.17.1 Organisation Certificate Policy Content 64
9.17.2 Third Party Rights 64
Annex A: DEFINITIONS AND INTERPRETATION 65
Annex B: OCA CERTIFICATE AND ORGANISATION CERTIFICATE PROFILES 71

1 INTRODUCTION

The document comprising this Appendix B (together with its Annexes A and B):

- shall be known as the "**Organisation Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) Organisation Certificates; and

(ii) OCA Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

(C) Except where the context otherwise requires, words or expressions used in this Policy shall have the meanings ascribed to them in IETF RFC 5280 where they:

(i) appear in `Courier New` font;

(ii) are accompanied by the descriptor 'field', 'type' or 'extension'; and/or

(D) take the form of a conjoined string of two or more words, such as '`digitalSignature`'.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been assigned an OID of 1.2.826.0.1. 8641679.1.2.1.1.

1.3 SMKI PARTICIPANTS

1.3.1 The Organisation Certification Authority

(A) The definition of Organisation Certification Authority is set out in Annex

A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The SMKI RAPP sets out the procedure to be followed by an Eligible Subscriber in order to become a Subscriber for one or more Certificates.

(D) Eligible Subscribers are subject to the applicable requirements of the SMKI RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code (Subscriber Obligations).

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of an Organisation Certificate must be an Organisation and be identified in the `subject` field of the Organisation Certificate Profile in accordance with Annex B.

(B) The Subject of an OCA Certificate must be the entity identified by the

`subject` field of the Root OCA Certificate Profile or Issuing OCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code (Relying Party Obligations).

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF ORGANISATION CERTIFICATES AND OCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The OCA shall ensure that Organisation Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Organisations in accordance with or pursuant to the Code.

(B) The OCA shall ensure that OCA Certificates are Issued only to the OCA:

(i) in its capacity as, and for the purposes of exercising the functions of, the Root OCA; and

(ii) in its capacity as, and for the purposes of exercising the functions of, the Issuing OCA.

(C) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(A) No Party or RDP shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the OCA or the SMKI PMA.

1.5.3 Person Determining Organisation CPS Suitability for the Policy

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the SMKI PMA to approve the Organisation CPS.

1.5.4 Organisation CPS Approval Procedures

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the procedure by which the SMKI PMA may approve the Organisation CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The Registration Authority Policies and Procedures (the **SMKI RAPP**) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

(A) Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The OCA shall lodge copies of the following in the SMKI Repository:

(i) each Organisation Certificate that has been accepted by a Subscriber;

(ii) each OCA Certificate;

(iii) each version of the SMKI RAPP;

(iv) each version of the SMKI Recovery Procedure;

(v) the latest version of the Organisation CRL;

(vi) the latest version of the Organisation ARL; and

(vii) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

(B) The OCA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The OCA shall ensure that:

(i) each Organisation Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each OCA Certificate is lodged to the SMKI Repository promptly on

being Issued;

(iii) the SMKI RAPP is lodged in the SMKI Repository, and a revised version of the SMKI RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) the SMKI Recovery Procedure is lodged in the SMKI Repository, and a revised version of the SMKI Recovery Procedure is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(v) the Organisation CRL is lodged in the SMKI Repository, and a revised version of the Organisation CRL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy;

(vi) the Organisation ARL is lodged in the SMKI Repository, and a revised version of the Organisation ARL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy; and

(vii) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the SMKI RAPP to ensure that the name of the entity that is the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the SMKI RAPP to ensure that the name of the Subject of each OCA Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Provision is made in the SMKI RAPP to:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) permit the OCA to Authenticate each Eligible Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

(A) Provision is made in the SMKI RAPP in relation to:

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of Organisation Identity

(A) Provision is made in the SMKI RAPP in relation to the:

(i) procedure to be followed by a Party or RDP in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the OCA will determine whether a Party or RDP is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party or RDP shall be Authenticated by the OCA for that purpose.

(B) Provision is made in the SMKI RAPP to ensure that each Eligible Subscriber has one or more DCC ID, User ID or RDP ID that is EUI-64 Compliant and has been allocated to that Eligible Subscriber in accordance with Section B2 (DCC, User and RDP Identifiers).

(C) Provision is made in the SMKI RAPP for the purpose of ensuring that the criteria in accordance with which the OCA shall Authenticate a Party or RDP shall be set to Level 3 pursuant to GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the SMKI RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to Level 3

(Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.4 Non-verified Subscriber Information

(A) The OCA shall verify all information in relation to Certificates.

(B) Further provision on the content of OCA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The OCA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 Authentication for Certificate Revocation Requests

(A) Provision is made in the SMKI RAPP in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation Request and verify that they are authorised to submit that request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

(A) Provision is made in the SMKI RAPP in relation to:

(i) in respect of an Organisation Certificate:

(a) the circumstances in which an Eligible Subscriber may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System; and

(ii) in respect of an OCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain an OCA Certificate.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made, where applicable, in the SMKI RAPP in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals, Systems and Devices in order to Authenticate them and verify that they are authorised to act on behalf of an Authorised Subscriber or Eligible Subscriber in its capacity as such; and

(ii) maintenance by the OCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the SMKI RAPP in relation to the establishment of an enrolment process in respect of OCA Personnel and OCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the OCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the SMKI RAPP in relation to the Authentication by the OCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the OCA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) may give notice to the Party or RDP which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the SMKI RAPP, this Policy or any other provision of the Code, the OCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the OCA is made in Section L8 of the Code (SMKI Performance Standards and Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 OCA Actions during Certificate Issuance

(A) The OCA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy and the SMKI RAPP; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with the SMKI RAPP.

(B) The OCA shall ensure that:

(i) each OCA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each Organisation Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) An OCA Certificate may only be:

(i) Issued by the OCA; and

(ii) for that purpose, signed using the Root OCA Private Key.

(D) An Organisation Certificate may only be:

(i) Issued by the OCA; and

(ii) for that purpose, signed using an Issuing OCA Private Key.

(E) The OCA shall not Issue:

(i) an Issuing OCA Certificate using a Root OCA Private Key after the expiry of the Validity Period of a Root OCA Certificate containing the Public Key associated with that Private Key;

(ii) an Organisation Certificate using an Issuing OCA Private Key after the expiry of the Validity Period of an Issuing OCA Certificate containing the Public Key associated with that Private Key; or

(iii) any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously Issued by it (except that the OCA may Issue an OCA Root Certificate containing the same Public Key in so far as it contains a different, or differently encrypted, Contingency Public Key).

4.3.2 Notification to Eligible Subscriber by the OCA of Issuance of Certificate

(A) Provision is made in the SMKI RAPP for the OCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the SMKI RAPP to:

(i) specify a means by which an Eligible Subscriber may clearly indicate to the OCA its rejection of a Certificate which has been Issued to it; and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued, and which has not rejected it, is treated as having accepted that Certificate.

(B) A Certificate which has been Issued by the OCA shall not be treated as valid for any purposes of this Policy or the Code until it is treated as having been accepted by the Eligible Subscriber to which it was Issued.

(C) The OCA shall maintain a record of all Certificates which have been Issued by it and are treated as accepted by a Subscriber.

(D) Further provision in relation to the rejection and acceptance of Certificates is made in Section L11 of the Code (Subscriber Obligations).

4.4.2 Publication of Certificates by the OCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy (Publication and Repository Responsibilities) and Section L5 of the Code (The SMKI Repository Service).

4.4.3 Notification of Certificate Issuance by the OCA to Other Entities

(A) The OCA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11 of the Code (Subscriber Obligations); and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates

(B) The OCA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where any OCA System or any OCA Private Key is (or is suspected by the OCA of being) Compromised, the OCA shall:

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in

relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to an OCA Private Key (but subject to the provisions of the SMKI Recovery Procedure):

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any Organisation Certificates Issued using that Private Key; and

(c) promptly both notify the SMKI PMA and, subject to the provisions of the SMKI Recovery Procedure, verifiably destroy the OCA Private Key Material.

(B) Where the OCA Root Private Key is Compromised (or is suspected by the OCA of being Compromised), the OCA:

(i) may issue a replacement for any OCA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that OCA Certificate applies for the Issue of a new Certificate in accordance with this Policy.

(C) A Subscriber for an Organisation Certificate may request a replacement for that Certificate at any time by applying for the Issue of a new Organisation Certificate in accordance with this Policy.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the OCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the OCA to Other Entities

See Part 4.4.3 of this Policy

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The OCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated for use by the Subject of an Organisation Certificate, the Subscriber for a Certificate which is associated with the previous Key Pair shall apply for the Issue of a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

4.7.6 Publication of the Re-Keyed Certificate by the OCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification (except to the extent to which it permits the OCA to Issue an OCA Root Certificate containing the same Public Key as a Certificate previously Issued by it, where the Certificates contain different, or differently encrypted, Contingency Public Keys).

(B) Subject to paragraph (A), neither the OCA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the OCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate:

(i) (subject to the provisions of the SMKI Recovery Procedure) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; or

(ii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate.

(B) The OCA must revoke a Certificate upon:

(i) (subject to the provisions of the SMKI Recovery Procedure) receiving a Certificate Revocation Request if the Certificate to which that request relates has been Authenticated in accordance with Part 3.4.1 of this Policy; or

(ii) being directed to do so by the SMKI PMA.

(C) The OCA must revoke a Certificate in relation to which it has not received a Certificate Revocation Request:

(i) (subject to the provisions of the SMKI Recovery Procedure) where it becomes aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate;

(ii) where it has determined that the Subscriber for that Certificate does not continue to satisfy the criteria set out in this Policy and the SMKI RAPP for being an Authorised Subscriber;

(iii) where it becomes aware that the Subscriber for that Certificate has

ceased to be an Eligible Subscriber in respect of the Certificate.

(D) In an extreme case, where it considers it necessary to do so for the purpose of preserving the integrity of the SMKI Services, the OCA may, on the receipt of a Certificate Revocation Request in relation to a Certificate which has not been Authenticated in accordance with Part 3.4.1 of this Policy, revoke that Certificate.

(E) Where the OCA revokes a Certificate in accordance with paragraph (D) it shall notify the SMKI PMA and provide a statement of its reasons for the revocation.

4.9.2 Who can Request Revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Subscriber, and shall on doing so:

(i) provide all the information specified in the SMKI RAPP (including all the information necessary for the Authentication of the Certificate); and

(ii) specify its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1(A) of this Policy).

(B) The SMKI PMA may direct the OCA to revoke a Certificate.

(C) The OCA may elect to revoke a Certificate in accordance with Part 4.9.1(D) of this Policy.

4.9.3 Procedure for Revocation Request

(A) Provision is made in the SMKI RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request.

(B) On receiving a Certificate Revocation Request, the OCA shall take reasonable steps~~use its reasonable endeavours~~ to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(C) Where the OCA, in accordance with Part 4.9.1(C) of this Policy, intends to revoke a Certificate in relation to which it has not received a Certificate Revocation Request, it shall use its best endeavours prior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation.

(D) The OCA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which OCA must process the Revocation Request

(A) The OCA shall ensure that it processes all Certificate Revocation Requests promptly, and in any event in accordance with such time as is specified in the SMKI RAPP.

4.9.6 Revocation Checking Requirements for Relying Parties

(A) Provision in relation to the revocation checking requirements for Relying Parties is made in Section L12 of the Code (Relying Party Obligations).

4.9.7 CRL Issuance Frequency (if applicable)

(A) The OCA shall ensure that an up to date version of the Organisation ARL is lodged in the SMKI Repository:

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of an OCA Certificate.

(B) Each version of the Organisation ARL shall be valid until the date which is 12 months after the date on which that version of the Organisation ARL is lodged in the SMKI Repository.

(C) Further provision in relation to the reliance that may be placed on the Organisation ARL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(D) The OCA shall ensure that an up to date version of the Organisation CRL is lodged in the SMKI Repository:

(i) at least once in every period of twelve hours; and

(ii) within one hour on the revocation of an Organisation Certificate.

(E) Each version of the Organisation CRL shall be valid until 48 hours from the time at which it is lodged in the SMKI Repository.

(F) Further provision in relation to the reliance that may be placed on the Organisation CRL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(G) The OCA shall ensure that each up to date version of the Organisation ARL and Organisation CRL:

(i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and

(ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The OCA shall ensure that the Organisation CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280 (section 5.3.1).

(I) The OCA shall retain a copy of the information contained in all versions of the Organisation CRL and Organisation ARL, together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the Panel, the SMKI PMA, any Subscriber or any Relying Party.

4.9.8 Maximum Latency for CRLs (if applicable)

See Part 4.9.7 of this Policy.

4.9.9 On-line Revocation/Status Checking Availability

(A) This Policy does not support on-line revocation status checking.

(B) The OCA shall not provide any on-line revocation status checking service.

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

(A) In circumstances in which:

(i) an up to date version of the Organisation ARL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(A) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the Organisation ARL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(B) of this Policy, but thereafter shall not rely on any Certificate.

(B) In circumstances in which:

(i) an up to date version of the Organisation CRL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(C) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the Organisation CRL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(D) of this Policy, but thereafter shall not rely on any Organisation Certificate.

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The OCA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[*Not applicable in this Policy*]

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The OCA shall ensure that the OCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The OCA shall ensure that:

(i) all of the physical locations in which the OCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The OCA shall ensure that the OCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with:

(i) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(ii) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

(E) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the OCA are stored in secure

containers accessible only to appropriately authorised individuals.

(F) The OCA shall ensure that the OCA Systems are Separated from any DCA Systems, save that any Systems used for the purposes of the Registration Authority functions of the OCA and DCA shall not require to be Separated.

5.1.2 Physical Access

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to OCA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the OCA Systems are situated.

5.1.4 Water Exposure

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to water exposure at all physical locations in which the OCA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in

relation to fire prevention and protection at all physical locations in which the OCA Systems are situated.

5.1.6 Media Storage

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the OCA.

5.1.7 Waste Disposal

(A) The OCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the OCA are disposed of only using secure methods of disposal in accordance with:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time.

5.1.8 Off-Site Back-Up

(A) The OCA shall regularly carry out a Back-Up of:

(i) all Data held on the OCA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the OCA shall ensure that the Organisation CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The OCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are

ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the Organisation CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise OCA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The OCA shall ensure that, where any elements of the OCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of OCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The OCA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the OCA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of OCA Personnel has a clearly defined level of access to the OCA Systems and the premises in which they are located;

(iii) no individual member of OCA Personnel is capable, by acting alone, of engaging in any action by means of which the OCA Systems may be Compromised to a material extent; and

(iv) the Organisation CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the OCA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of OCA Personnel; and

(ii) the application of controls to the actions of all members of OCA Personnel who are Privileged Persons, in particular:

(a) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and

(b) providing that the revocation of any OCA Certificate is one such function.

(B) The OCA shall ensure that the Organisation CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) OCA Systems administration;

(ii) OCA Systems operations;

(iii) OCA Systems security; and

(iv) OCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The OCA shall ensure that all OCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the OCA, not have been previously relieved of any past assignment (whether for the OCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The OCA shall ensure that all OCA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of OCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of OCA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of OCA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the OCA in this Policy include references to persons with whom the OCA contracts in order to secure performance of its obligations as the OCA.

5.3.8 Documentation Supplied to Personnel

(A) The OCA shall ensure that all OCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the Organisation CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The OCA shall ensure that:

(i) the OCA Systems record all systems activity in an audit log;

(ii) the Organisation CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of OCA Personnel;

(b) the use of OCA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the OCA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the OCA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The OCA shall ensure that:

(i) the audit logging functionality in the OCA Systems is fully enabled at all times;

(ii) all OCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the OCA Systems in compliance with:

(a) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(b) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time;

(B) The OCA shall ensure that the Organisation CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be

reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of OCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The OCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The OCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or

replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The OCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the OCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The OCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the Organisation CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the OCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The OCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The OCA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The OCA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The OCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the OCA's operations.

(B) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to the periodic verification by the OCA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 Organisation Certificate Key Changeover

(A) The OCA shall Issue a new Organisation Certificate in relation to an Organisation where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the SMKI RAPP and this Policy.

5.6.2 OCA Key Changeover

(A) Where the OCA ceases to use an OCA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) either:

(a) verifiably destroy the OCA Private Key Material; or

(b) retain the OCA Private Key Material in such a manner that it is adequately protected against being put back into use;

(ii) not revoke the related OCA Public Key (which may continue to be used for the purpose of validating Digital Signatures generated using the OCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any relevant Certificate subsequently Issued by it is Issued using the OCA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(v) in its capacity as the Root OCA:

(a) Issue a new relevant OCA Certificate; and

(b) promptly lodge that OCA Certificate in the SMKI Repository.

(B) The OCA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.6.3 Subscriber Key Changeover

(A) Where:

(i) a Certificate has been revoked in accordance with Part 4.9 of this Policy; and

(ii) the Subscriber for that Certificate submits to the OCA a Certificate Signing Request for the Issue of a replacement Certificate,

the OCA shall verify that the reasons for the revocation and replacement of the previous Certificate have been satisfactorily addressed, and may Issue a Certificate in accordance with the Certificate Signing Request only after it

has done so.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The OCA shall ensure that the Organisation CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the OCA Systems or major failure in the OCA processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date Organisation ARL and Organisation CRL.

(B) The OCA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any OCA Private Key or any part of the OCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The OCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The OCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[*Not applicable in this Policy*]

6 TECHNICAL SECURITY CONTROLS

The OCA shall ensure that the Organisation CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root OCA, the Issuing OCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The OCA shall ensure that all Key Pairs which it uses for the purposes of this Policy are generated:

(i) in a protected environment compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time);

(ii) using multi-person control, such that no single Privileged Person is capable of generating any such Key Pair; and

(iii) using random numbers which are such as to make it computationally infeasible to regenerate those Key Pairs even with knowledge of when and by means of what equipment they were generated.

(B) The OCA shall not generate any Private Key or Public Key other than an OCA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the OCA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root OCA and Issuing OCA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 OCA Public Key Delivery to Relying Parties

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

(i) in relation to the manner by which each OCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the OCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The OCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the size and characteristics set out in the GB Companion Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The OCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 `keyUsage` Field)

(A) The OCA shall ensure that each Certificate that is Issued by it has a `keyUsage` field in accordance with RFC5759 and RFC5280.

(B) The OCA shall ensure that each Organisation Certificate that is Issued by it has a `keyUsage` of either:

(i) `digitalSignature`; or

(ii) `keyAgreement`.

(C) The OCA shall ensure that each OCA Certificate that is Issued by it has a `keyUsage` of either:

(i) `keyCertSign`; or

(ii) `CRLSign`.

(D) The OCA shall ensure that no `keyUsage` values may be set in an Organisation Certificate or OCA Certificate other than in accordance with this Part 6.1.7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The OCA shall ensure that all OCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The OCA shall ensure that all OCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(C) The OCA shall ensure that no OCA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from

time to time).

(D) The OCA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Organisation CPS; and

(ii) require to be unblocked by an authorised member of OCA Personnel who has been Authenticated as such following a process which shall be set out in the Organisation CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The OCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The OCA may Back-Up OCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing OCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The OCA shall ensure that no OCA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The OCA shall ensure that no OCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services;

(ii) in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The OCA shall ensure that the Cryptographic Module in which any OCA Private Key is stored may be accessed only by an authorised member of OCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The OCA shall ensure that any OCA Private Key shall be capable of being de-activated by means of the OCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the Organisation CPS.

6.2.10 Method of Destroying Private Key

(A) The OCA shall ensure that the Organisation CPS incorporates provisions for the exercise of strict controls in relation to the destruction of OCA Keys.

(B) The OCA shall ensure that no OCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the OCA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The OCA shall ensure that it archives OCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The OCA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an Organisation Certificate, 10 years;

(ii) in the case of an Issuing OCA Certificate, 25 years; and

(iii) in the case of a Root OCA Certificate, 50 years.

(B) For the purposes of paragraph (A), the OCA shall set the `notAfter` value specified in Annex B in accordance with that paragraph.

(C) The OCA shall ensure that no OCA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The OCA shall ensure that any Cryptographic Module within which an OCA Key is held has Activation Data that are unique and unpredictable.

(B) The OCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the OCA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the OCA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The OCA shall ensure that the Organisation CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the

OCA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in OCA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the OCA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for OCA Keys.

6.5.2 Computer Security Rating

(A) The OCA shall ensure that the Organisation CPS incorporates provisions relating to the appropriate security rating of the OCA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The OCA shall ensure that any software which is developed for the purpose of establishing a functionality of the OCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The OCA shall ensure that the Organisation CPS incorporates provisions which are designed to ensure that the OCA Systems satisfy the

requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root OCA

(A) The OCA shall ensure that its functions as the Root OCA are carried out on a part of the OCA Systems that is neither directly nor indirectly connected to any System which is not a part of the OCA Systems.

6.7.2 Protection Against Attack

(A) The OCA shall use its best endeavours to ensure that the OCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event; and

(ii) any unauthorised attempt to connect to them.

(B) The OCA shall take reasonable steps~~use its reasonable endeavours~~ to ensure that the OCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing OCA

(A) The DCC shall ensure that, where its functions as the Issuing OCA are carried out on a part of the OCA Systems that is connected to an external network, they are carried out on a System that is Separated from all other OCA Systems.

6.7.4 Health Check of OCA Systems

(A) The OCA shall ensure that, in relation to the OCA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

(A) The OCA shall ensure that Time-Stamping takes place in relation to all Certificates and all other OCA activities which require an accurate record of time.

(B) The OCA shall ensure that the Organisation CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the OCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

The OCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

(A) The OCA shall ensure that the Organisation ARL and Organisation CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL Entry Extensions

(A) The OCA shall notify Parties of the profile of the Organisation CRL and of any Organisation CRL extensions.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 Organisation Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of Organisation Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 Organisation Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Organisation Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy,
- the rule of interpretation set out at Part 1.1 of this Policy shall apply.

Activation Data	means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.
Archive	means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).
Audit Log	means the audit log created in accordance with Part 5.4.1 of this Policy.
Authentication	means the process of establishing that an individual, Certificate, System or Organisation is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).
Authorised Subscriber	means a Party or RDP which has successfully completed the procedures set out in the SMKI RAPP and has been authorised by the OCA to submit a Certificate Signing Request.
Certificate	means either an Organisation Certificate or an OCA

	Certificate.
Certificate Profile	means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.
Certificate Re-Key	means a change to the Public Key contained within a Certificate bearing a particular serial number.
Certificate Revocation Request	means a request for the revocation of a Certificate by the OCA, submitted by the Subscriber for that Certificate to the OCA in accordance with the SMKI RAPP and this Policy.
Certificate Signing Request	means a request for a Certificate submitted by an Eligible Subscriber in accordance with the SMKI RAPP.
DCA	has the meaning given to that expression in Appendix A of the Code (Device Certificate Policy).
DCA Systems	has the meaning given to that expression in Appendix A of the Code (Device Certificate Policy).
Eligible Subscriber	means: (a) in relation to an Organisation Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.18 of the Code (Organisation Certificates); and (b) in relation to an OCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.19 of the Code (OCA Certificates).
Issue	means the act of the OCA, in its capacity as the Root OCA or Issuing OCA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "**Issued**" and "**Issuing**"

	shall be interpreted accordingly).
Issuing Organisation Certification Authority (or **Issuing OCA**)	means the DCC exercising the function of Issuing Organisation Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.
Issuing OCA Certificate	means a certificate in the form set out in the Issuing OCA Certificate Profile in accordance with Annex B, and Issued by the Root OCA to the Issuing OCA in accordance with this Policy.
Issuing OCA Private Key	means a Private Key which is stored and managed by the OCA acting in its capacity as the Issuing OCA.
Issuing OCA Public Key	means the Public Key which is part of a Key Pair with an Issuing OCA Private Key.
Key Escrow	means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.
Object Identifier (or **OID**)	means an Object Identifier assigned by the Internet Address Naming Authority.
OCA Certificate	means either a Root OCA Certificate or an Issuing OCA Certificate.
OCA Key	means any Private Key or a Public Key generated by the OCA for the purposes of complying with its obligations under the Code.
OCA Private Key	means either a Root OCA Private Key or an Issuing OCA Private Key.
OCA Systems	means the Systems used by the OCA in relation to the SMKI Services.

Organisation Authority Revocation List (or **ARL**)	means a list, produced by the OCA, of all OCA Certificates that have been revoked in accordance with this Policy.
Organisation Certificate	means a certificate in the form set out in the Organisation Certificate Profile in accordance with Annex B, and Issued by the Issuing OCA in accordance with this Policy.
Organisation Certificate Revocation List (or **CRL**)	means a list, produced by the OCA, of all Organisation Certificates that have been revoked in accordance with this Policy.
Organisation Certification Authority (or **OCA**)	means the DCC, acting in the capacity and exercising the functions of one or more of: (a) the Root OCA; (b) the Issuing OCA; and (c) the Registration Authority.
Private Key Material	in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.
Registration Authority	means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the SMKI RAPP.
Registration Authority Manager	means either a director of the DCC or any other person who may be identified as such in accordance with the SMKI RAPP.
Registration Authority Personnel	means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.
Relying Party	means a person who, pursuant to the Code, receives and relies upon a Certificate.

Root Organisation Certification Authority (or **Root OCA**)	means the DCC exercising the function of Issuing OCA Certificates to the Issuing OCA and storing and managing Private Keys associated with that function.
Root OCA Certificate	means a certificate in the form set out in the Root OCA Certificate Profile in accordance with Annex B and self-signed by the Root OCA in accordance with this Policy.
Root OCA Private Key	means a Private Key which is stored and managed by the OCA acting in its capacity as the Root OCA.
Security Related Functionality	means the functionality of the OCA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.
Subject	means: (a) in relation to an Organisation Certificate, the Organisation identified by the `subject` field of the Organisation Certificate Profile in Annex B; and (b) in relation to an OCA Certificate, the globally unique name of the Root OCA or Issuing OCA as identified by the `subject` field of the relevant Certificate Profile in Annex B.
Subscriber	means, in relation to any Certificate, a Party or RDP which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.
Time-Stamping	means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the OCA that:

(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(b) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the OCA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the Independent Time Source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: OCA Certificate and Organisation Certificate Profiles

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which OCA Certificates and Organisation Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5759 and IETF RFC5280.

Common requirements applicable to OCA Certificates and Organisation Certificates

All OCA Certificates and Organisation Certificates that are validly authorised within the SMKI for use within the scope of GB Companion Specification and GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all OCA Certificates and Organisation Certificates shall:
    - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root OCA Certificate;
    - contain the `keyUsage` extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- shall, in relation to communications with devices, contain a non-empty subject field which contains an `X520OrganizationalUnitName` whose value is to be expressed as the human-readable two octet hexadecimal representation of the integer `RemotePartyRole` that the Certificate allows the Subject of the Certificate to perform;
- only contain Public Keys of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;

- contain a `certificatePolicies` extension containing at least one `CertPolicyID` which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Parties and Devices shall interpret this extension;
- contain a `serialNumber` of no more than 16 octets in length;
- contain a `subjectKeyIdentifier` which shall be marked as non-critical;
- contain an `authorityKeyIdentifier` in the form `[0] KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the Root OCA Certificate. Note this exception only applies where `RemotePartyRole` as specified in the `X520OrganizationalUnitName` part of the `subject` field = root;
- only contain `KeyIdentifiers` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
- contain an `issuer` field whose contents MUST be identical to the contents of the signer's `subject` field in the signer's Certificate;
- have a valid `notBefore` field consisting of the time of issue encoded and a valid `notAfter` field expiration date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Organisation Certificates only

All Organisation Certificates that are issued by the OCA shall:

- within the `subject` field, in addition to other attributes, contain an `AttributeTypeAndValue` structure whose type shall be `id-at-uniqueIdentifier {joint-iso-itu-t(2) ds(5) attributeType(4) uniqueIdentifier(45)}` and whose value shall be the 8 octet Entity Identifier of the subject of the Certificate;
- contain a single Public Key;
- contain a `keyUsage` extension marked as critical, with a value of only one of:
  - `digitalSignature`; or
  - `keyAgreement`.

- contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of this Policy under which the Certificate is issued.

Requirements applicable to the Root OCA and Issuing OCA

All OCA Certificates issued by the OCA shall:

- have globally unique `subject` field contents;
- contain a single public key except for the Root-CA where there shall be two public keys. The second public key shall be referred to as the Contingency Key and shall be present in the `WrappedApexContingencyKey` extension with the meaning of IETF RFC5934. The Contingency Key shall be encrypted as per the requirements of the GBCS;
- contain a `keyUsage` extension marked as critical and defined as:
  - `keyCertSign`; and
  - `cRLSign`;
- for Issuing OCA Certificates, contain at least one `CertPolicyID` in the `certificatePolicies` extension that refers to the OID of this Policy under which the Certificate is issued;
- for the Root OCA Certificate, contain a single `CertPolicyID` in the `certificatePolicies` extension that refers to the OID for `anyPolicy`;
- for Issuing OCA Certificates, contain the `basicConstraints` extension, with values `cA=True`, and `pathLen=0`. This extension shall be marked as critical;
- for the Root OCA Certificate, contain the basicConstraints extension, with the value `cA=True` and `pathLen absent` (unlimited). This extension shall be marked as critical.

Organisation Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference

version	INTEGER	v3	
serialNumber	INTEGER	Positive Integer of up to 16 Octets	
signature	AlgorithmIdentifier	SHA256 with ECDSA	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Issuer X520 Common Name")	UTF8String	Globally unique common name of Issuing OCA of up to 4 Octets (as defined in the Issuing OCA Certificate Profile)	
keyIdentifier in Authoritykeyidentifier (the "Subject Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
notBefore	Time	Creation time of the Organisation Certificate	

notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Name of the Subject of up to 16 Octets	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-organizationalUnitName (the "Subject X520 Organizational Unit Name")	UTF8String	Remote Party Role of the subject of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-uniqueIdentifier (the "Subject's Unique Identifier")	UniqueIdentifier	The 64 bit Entity Identifier of the subject of the Certificate	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	

extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Organisation Certificate signature	

Interpretation

version

The version of the X.509 Organisation Certificate. Valid Organisation Certificates shall identify themselves as version 3.

serialNumber

Organisation Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Organisation Certificate, and shall be created by the Issuing OCA that signs the Organisation Certificate. The serialNumber shall be unique in the scope of Organisation Certificate signed by the Issuing OCA.

signature

The identity of the signature algorithm used to sign the Organisation Certificate. The field is identical to the value of the Organisation Certificate signatureAlgorithm field explained further under the next **signatureAlgorithm** heading.

Issuer X520 Common Name

The name of the signer of the Organisation Certificate. This will be the gloablly unique name of the Issuing OCA of up to 4 Octets (as defined in the Issuing OCA Certificate Profile).

Authority Key Identifier

To optimize building the correct credential chain, the non-critical Authority Key Identifier extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all Organisation Certificates.

Subject Key Identifier

The Subject Key Identifier extension shall be included and marked as non-critical in the Organisation Certificate.

`validity`

The time period over which the Issuing OCA expects the Organisation Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time an Organisation Certificate may be used. This shall be the time the Organisation Certificate is created.

`notAfter`

The latest time an Organisation Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

Subject X520 Common Name

This field shall contain a unique X.500 Distinguished Name (DN). This should be the unique trading name of the Organisation of up to 16 Octets.

Subject X520 Organizational Unit Name

The Subject X520 Organizational Unit Name attribute of `subject` shall be populated with the RemotePartyRole code that the Certificate allows the subject of the Certificate to perform. See the GB Companion Specification for details of RemotePartyRole codes.

Subject's Unique Identifier

This shall be populated with the 64 bit Entity Identifier (compliant with EUI-64 standard – see Great Britain Companion Specification) of the subject of the Certificate

`subjectPublicKeyInfo`

The Organisation Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Organisation Certificate extension (explained further under the next **`extensions`** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
  }
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The `OBJECT IDENTIFIER` for the curve choice to be used in Organisation Certificate is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Issuing OCA signature algorithm used to sign this Organisation Certificate is as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Issuing OCA's signature of the Organisation Certificate shall be computed using the Issuing OCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Organisation Certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `keyUsage`
- `authorityKeyIdentifier`
- `subjectKeyIdentifier`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to 16 Octets	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The value field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-commonName` (the "Issuer X520 Common	`UTF8String`	Globally unique common name of Root OCA of up to 4 Octets	

Name")			
keyIdentifier in SubjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Root OCA of up to 4 Octets (same as Issuer name)	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-organizationalUnitName (the "Subject X520 Organizational Unit Name")	UTF8String	Remote Party Role of the subject of the Certificate	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The Subject's Public Key	

The `extnValue` in the `extension` whose `extnID` is `id-pe-WrappedApexContingencyKey`	`ApexContingencyKey`	The Subject's protected (encrypted) Public Key used for recovery purposes	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject Certificate signature	

These certificates are the root of trust for the Organisations SMKI.

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the Certificate, and shall be created by the OCA that signs the Certificate (self-signed by Root OCA). The `serialNumber` shall be unique in the scope of Certificates signed by the OCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root OCA Certificate's signatureAlgorithm field explained further under the next **`signatureAlgorithm`** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root OCA of up to 4 Octets. This will be the same as the `subject` as it is self-signed by the Root OCA.

Subject Key Identifier

The `SubjectKeyIdentifier` extension shall be included and marked as non-critical in the Certificate.

`validity`

The time period over which the issuer expects the Certificate to be valid. The validity period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

Subject X520 Common Name

This field must be populated with the globally unique name of the Root OCA of up to 4 Octets.

Subject X520 Organizational Unit Name

The Subject X520 `OrganizationalUnitName` attribute of `subject` shall be populated with the RemotePartyRole code that the Certificate allows the subject of the Certificate to perform. See the GB Companion Specification for details of RemotePartyRole codes for the purposes of communications with Devices.

`subjectPublicKeyInfo`

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Certificate extension (explained further under the next **`extensions`** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
  }
```

Only the following field in ECParameters shall be used:

o `namedCurve` - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an `OBJECT IDENTIFIER`.

The object identifier fo the curve choice to be used in OCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key shall be rejected if any value other than 0x04 is in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root OCA signature algorithm used to sign this Certificate as defined in section under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root OCA's signature of the Certificate shall be computed using the Root OCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional `extensions`:

- `certificatePolicy`
- `keyUsage`
- `basicConstraints`
- `subjectKeyIdentifer`

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing OCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference
`version`	`INTEGER`	v3	
`serialNumber`	`INTEGER`	Positive Integer of up to 16 Octets	
`signature`	`AlgorithmIdentifier`	SHA256 with ECDSA	
The `value` field of the `AttributeTypeAndValue` structure within the `subject` field whose `type` is `id-at-`	`UTF8String`	Globally unique name of Root OCA of up to 4 Octets (as defined in the Root OCA Certificate Profile)	

commonName (the "Issuer X520 Common Name")			
keyIdentifier in subjectKeyIdentifier (the "Subject Key Identifier")	keyIdentifier	Provides a means for identifying certificates containing the particular Public Key used in an application	
keyIdentifier in authorityKeyIdentifier (the "Authority Key Identifier")	keyIdentifier	A unique value that matches the subjectKeyIdentifier value of the issuer's credential	
notBefore	Time	Creation time of the certificate	
notAfter	Time	Expiry time of the Certificate	
The value field of the AttributeTypeAndValue structure within the subject field whose type is id-at-commonName (the "Subject X520 Common Name")	UTF8String	Globally unique name of Issuing OCA of up to 4 Octets	
The value field of the AttributeTypeAndValue structure within the subject field	UTF8String	Remote Party Role of the Subject of the Certificate	

whose `type` is `id-at-organizationalUnitName` (the "Subject X520 Organizational Unit Name")			
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The Subject's Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	SHA256 with ECDSA	
`signatureValue`	`BIT STRING`	Subject certificate signature	

`version`

The version of the X.509 Certificate. Valid Certificates shall identify themselves as version 3.

`serialNumber`

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the Root OCA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root OCA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing OCA Certificate's `signatureAlgorithm` field explained further under the next **`signatureAlgorithm`** heading.

Issuer X520 Common Name

The name of the signer of the Certificate. This will be the gloablly unique name of the Root OCA of up to 4 Octets (as defined in the Root OCA Certificate Profile).

Subject Key Identifier

The `SubjectKeyIdentifier` extension shall be included and marked as non-critical in the Certificate.

Authority Key Identifier

To optimize building the correct credential chain, the non-critical `AuthorityKeyIdentifier` extension shall be populated with a unique value as recommended by RFC 5280 and shall be included in all Organisation Certificates.

`validity`

The time period over which the issuer expects the Certificate to be valid. The `validity` period is the period of time from `notBefore` through `notAfter`, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as `UTCTime` as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as `GeneralizedTime` as YYYYMMDDHHmmssZ.

`notBefore`

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

`notAfter`

The latest time a Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

Subject X520 Common Name

This field shall be populated with the globally unique name of the Issuing OCA of up to 4 Octets.

Subject X520 Organizational Unit Name

The Subject X520 Organizational Unit Name attribute of subject shall be populated with the RemotePartyRole code that the Certificate allows the subject of the Certificate to perform. See the GB Companion Specification for details of RemotePartyRole codes.

`subjectPublicKeyInfo`

The Certificate's `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the `subjectPublicKeyInfo` structure shall contain the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2)
us(840) ansi-X9-62(10045) keyType(2) 1 }
```

`id-ecPublicKey` indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the `KeyUsage` Certificate extension (explained further under the next **`extensions`** heading).

The parameter for `id-ecPublicKey` is as follows and shall always be present:

```
ECParameters ::= CHOICE {
    namedCurve         OBJECT IDENTIFIER
    -- implicitCurve   NULL
    -- specifiedCurve  SpecifiedECDomain
  }
```

Only the following field in ECParameters shall be used:

- `namedCurve` - identifies all the required values for a particular

  set of elliptic curve domain parameters to be represented by an

  `OBJECT IDENTIFIER`.

The object identifier fo the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2)
us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }
```

The `subjectPublicKey` from `SubjectPublicKeyInfo` is the ECC Public Key.

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The first octet of the `subjectPublicKey` indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root OCA signature algorithm used to sign this Certificate as defined under the next **Signature Method (ECDSA)** heading.

`signatureValue`

The Root OCA's signature of the Certificate shall be computed using the Root OCA's private signing key using the algorithm identified under the next **Signature Method (ECDSA)** heading.

The structure for ECDSA signatures shall be as per RFC 5480.

`extensions`

Issuing-CA Certificates shall contain the `extensions` described below. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`

- keyUsage
- basicConstraints
- subjectKeyIdentifer
- authorityKeyIdentifier

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be `ecdsa-with-SHA256` as specified in RFC 5759 and 6318. The algorithm identifier is:

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-

62(10045) signatures(4) ecdsa-with-sha2(3) 2 }
```

SHA-256 hash algorithm

The hash algorithm used shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

APPENDIX C – SMKI COMPLIANCE POLICY

1 INTRODUCTION

1.1 The document comprising this Appendix C:

(a) shall be known as the "**SMKI Compliance Policy**" (and in this document is referred to simply as the "**Policy**"),

(b) is a SEC Subsidiary Document related to Section L2 of the Code (SMKI Assurance).

2 SMKI INDEPENDENT ASSURANCE SCHEME

DCC: Duty to Submit to an SMKI Independent Assurance Scheme

2.1 The DCC shall subject the SMKI Services to assessment against an assurance scheme which satisfies:

(a) the quality requirements specified in Part 2.2 of this Policy;

(b) the independence requirements specified in Part 2.3 of this Policy; and

(c) the approval requirements specified in Part 2.5 of this Policy,

and that scheme is referred to in this Policy as the "**SMKI Independent Assurance Scheme**".

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the SMKI Independent Assurance Scheme must be a scheme:

(a) which is recognised as an accreditation scheme for the purposes of Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures;

(b) which is based on ISO 27001; and

(c) the provider of which:

(i) is used by the United Kingdom Government to provide assurance in

relation to electronic trust services; and

(ii) requires all its scheme assessors to be UKAS certified.

Independence Requirements

2.3 The independence requirements specified in this Part 2.3 are that the provider of the SMKI Independent Assurance Scheme must be independent of the DCC and of each DCC Service Provider from which the DCC acquires capability for the purposes of the provision of the SMKI Services (referred to in this Policy as a "**Relevant DCC Service Provider**").

2.4 For the purposes of Part 2.3 of this Policy, the provider of the SMKI Independent Assurance Scheme is to be treated as independent of the DCC (and of Relevant DCC Service Providers) only if:

(a) neither the DCC nor any of its subsidiaries (or any Relevant DCC Service Provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the provider of the scheme;

(b) either:

(i) no director or employee of the DCC (or of any Relevant DCC Service Provider) is or becomes a director or employee of the provider of the scheme; or

(ii) where any person is or becomes both a director or employee of the DCC (or of any Relevant DCC Service Provider) and a director or employee of the provider of the scheme, appropriate arrangements are in place to ensure that that person is able to have no influence on any decisions made by the provider of the scheme in respect of the approval of any person or the accreditation of any thing in accordance with the scheme;

(c) no person who is a director or employee of the DCC (or of any Relevant DCC Service Provider) holds or acquires any investment by way of shares, securities or other financial rights or interests in the provider of the scheme,

except where sub-paragraph (b)(ii) applies and that investment is acquired by that person by way of reasonable compensation for his or her performance as a director or employee of the provider of the scheme; and

(d) the provider of the scheme does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC (or in any Relevant DCC Service Provider).

Approval Requirements

2.5 Before entering into any agreement with the provider of the SMKI Independent Assurance Scheme, in accordance with its obligation under Section L2.2 of the Code (SMKI Compliance Policy), the DCC shall submit to the SMKI PMA for approval:

(a) its proposed choice of scheme; and

(b) the proposed terms and conditions of its agreement with the provider of that scheme,

and shall not enter into any such agreement unless the SMKI PMA has first approved the proposed SMKI Independent Assurance Scheme and the proposed terms and conditions of that agreement.

2.6 If the SMKI PMA does not approve either the proposed SMKI Independent Assurance Scheme or the proposed terms and conditions of the DCC's agreement with the provider of that scheme:

(a) the SMKI PMA shall provide the DCC with a statement of its reasons for not doing so; and

(b) the DCC shall submit to the SMKI PMA for approval, as soon as is reasonably practicable, a revised proposal in relation to the scheme.

3 INDEPENDENT ASSURANCE SERVICE PROVIDER

DCC: Duty to Procure Independent Assurance Services

3.1 For the purposes of complying with its obligation under Section L2.2 of the Code

(SMKI Compliance Policy), the DCC shall procure the provision of assurance services:

(a) of the scope specified in Part 3.2 of this Policy;

(b) from a person who:

(i) is suitably qualified in accordance with Part 3.3 of this Policy; and

(ii) satisfies the independence requirements specified in Part 3.4 of this Policy,

and that person is referred to in this Policy as the "**Independent SMKI Assurance Service Provider**".

Scope of Independent Assurance Services

3.2 The assurance services specified in this Part 3.2 are services in accordance with which the Independent SMKI Assurance Service Provider shall:

(a) undertake an initial assessment of the SMKI Services against the SMKI Independent Assurance Scheme in accordance with Part 4 of this Policy;

(b) subsequently undertake further assessments of the SMKI Services against the SMKI Independent Assurance Scheme:

(i) at a frequency recommended by the provider of that scheme; or

(ii) where there is no such recommended frequency, or where the SMKI PMA otherwise determines, at a frequency specified by the SMKI PMA;

(c) at the request of, and to an extent determined by, the SMKI PMA, carry out an assessment of the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set;

(d) at the request of the SMKI PMA, provide to it advice in relation to the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set;

(e) at the request of the SMKI PMA, provide to it advice in relation to a review of this Policy, which shall include in particular:

(i) recommendations as to the scope and frequency of assessments carried out in accordance with this Policy; and

(ii) advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default), including where the Defaulting Party is the DCC in accordance with Section L2.6 of the Code (Events of Default); and

(f) at the request of the SMKI PMA Chair, provide a representative to attend and contribute to the discussion at any meeting of the SMKI PMA.

Suitably Qualified Service Provider

3.3 The Independent SMKI Assurance Service Provider shall be treated as suitably qualified in accordance with this Part 3.3 only if it is recognised by the provider of the SMKI Independent Assurance Scheme as being qualified to carry out assessments against that scheme.

Independence Requirements

3.4 The independence requirements specified in this Part 3.4 are that the Independent SMKI Assurance Service Provider must be independent of each SMKI Participant and of each service provider from whom that SMKI Participant acquires capability for any purpose related to its compliance with its obligations under the Code (but excluding any provider of corporate assurance services to that SMKI Participant).

3.5 For the purposes of Part 3.4 of this Policy, the Independent SMKI Assurance Service Provider is to be treated as independent of an SMKI Participant (and of a relevant service provider of that SMKI Participant) only if:

(a) neither that SMKI Participant nor any of its subsidiaries (or such a service provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent SMKI Assurance Service Provider;

(b) no director of that SMKI Participant (or of any such service provider) is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent SMKI Assurance Service Provider; and

(c) the Independent SMKI Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in that SMKI Participant (or in any such service provider).

4 INITIAL ASSURANCE ASSESSMENT

DCC: Duty to Procure Initial Assessment

4.1 The DCC shall ensure that an initial assurance assessment of the SMKI Services:

(a) against the SMKI Independent Assurance Scheme; and

(b) in respect of compliance by the DCC with the applicable requirements of the SMKI Document Set,

is undertaken by the Independent SMKI Assurance Service Provider in accordance with Part 4.2 of this Policy.

Nature of the Initial Assessment

4.2 The initial assessment referred to in Part 4.1 of this Policy shall be undertaken in two stages, as described in Parts 4.3 and 4.5 of this Policy.

4.3 The first stage of the initial assessment shall:

(a) be undertaken ~~prior to the commencement of Interface Testing~~by no later than such date as is necessary in order to ensure that an assessment report may be produced in accordance with paragraph (b); and

(b) result in an assessment report to be known as the "**Stage 1 Assurance Report**" in relation to the SMKI Services being produced by the Independent SMKI Assurance Service Provider by no later than such date as the SMKI PMA shall determine~~at least one month prior to the anticipated start date of Interface~~

~~Testing~~.

4.4 The Stage 1 Assurance Report shall:

(a) clearly identify any failure of the DCC to comply with the applicable requirements of the SMKI Document Set;

(b) recommend that the assurance status of the DCC in relation to the SMKI Services should be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved; and

(c) be provided to both the DCC and the SMKI PMA promptly upon completion.

4.5 The second stage of the initial assessment shall:

(a) be undertaken by no later than such date as is necessary in order to ensure that an assessment report may be produced in accordance with paragraph (b)~~12 weeks after the commencement of Interface Testing~~; and

(b) result in an assessment report to be known as the "**Stage 2 Assurance Report**" in relation to the SMKI Services being produced by the Independent SMKI Assurance Service Provider by no later than such date as the SMKI PMA shall determine~~as soon as reasonably practicable following the completion of that second stage of the initial assessment~~.

4.6 The Stage 2 Assurance Report shall:

(a) clearly identify any failure of the DCC to comply with the applicable requirements of the SMKI Document Set;

(b) recommend that the assurance status of the DCC in relation to the SMKI Services should be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved; and

(c) be provided to both the DCC and the SMKI PMA promptly upon completion.

PMA: Response to the Initial Assessment

4.7 On receiving either the Stage 1 Assurance Report or Stage 2 Assurance Report, the SMKI PMA shall:

(a) promptly consider that report;

(b) determine that the assurance status of the DCC in relation to the SMKI Services is to be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved;

(c) where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at 'approved with caveats', state in writing its reasons for considering that it is acceptable for the DCC to:

(i) in the case of the Stage 1 Assurance Report, commence the provision of the SMKI Services; or

(ii) in the case of the Stage 2 Assurance Report, continue to provide the SMKI Services; and

(d) provide a copy of the report (being redacted only in so far as necessary for the purposes of security) and a statement of its determination (and of any reasons accompanying that determination) to all Parties.

4.8 Where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at 'approved with caveats' or 'not approved' it shall:

(a) require that the DCC submit to it as soon as reasonably practicable a remedial action plan; and

(b) within one month of the submission of that plan, require the DCC to make any changes to it that the SMKI PMA may specify.

DCC: Duty in relation to Remedial Action Plan

4.9 Where the DCC is required to do so in accordance with Part 4.8(a) of this Policy, it shall as soon as reasonably practicable submit to the SMKI PMA a remedial action plan.

4.10 Where the DCC is required by the SMKI PMA in accordance with Part 4.8(b) of this Policy to make changes to the remedial action plan, it may appeal that decision to the Authority and:

(a) the Authority shall determine what changes (if any) shall be made to the remedial action plan; and

(b) the determination of the Authority shall be final and binding for the purposes of the Code.

4.11 The DCC shall implement any remedial action plan subject to any required changes to it specified by:

(a) the SMKI PMA in accordance with Part 4.8(b) of this Policy; or

(b) the Authority in accordance with Part 4.10 of this Policy.

5 PMA: DUTY TO PROVIDE INFORMATION

Initial Assurance Assessment

5.1 The SMKI PMA shall, on request, provide to the Secretary of State and the Authority a copy of:

(a) the Stage 1 Assurance Report received by it in accordance with Part 4.4 of this Policy;

(b) the Stage 2 Assurance Report received by it in accordance with Part 4.6 of this Policy; and

(c) any remedial action plan that the DCC is required to implement in accordance with Part 4.11 of this Policy.

Subsequent Assurance Assessments

5.2 Following any assessment carried out by the Independent SMKI Assurance Service Provider of the compliance of the DCC with the applicable requirements of the SMKI Document Set, the SMKI PMA's determination as to the extent to which the DCC is compliant with those requirements shall be made available by it to:

(a) all Parties;

(b) the Panel;

(c) the Authority; and

(d) on request, the Secretary of State.

Version D1.0

APPENDIX D

SMKI Registration Authority Policies and Procedures (SMKI RAPP)

Contents

1 Introduction 4

1.1 Purpose 4

2 SMKI Registration Authority obligations to support DCCKI identity verification 5

3 SMKI Roles 6

3.1 Party, RDP, SMKI PMA, Panel and DCC representatives 6

3.2 SMKI Registration Authority representatives 7

4 Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures 9

4.1 General registration obligations 9

4.1.1 Organisation, individual, and RA obligations 9

4.1.2 High level overview of SMKI Registration Authority procedures 10

4.1.3 Change of details 12

4.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party or RDP 13

4.1.5 SROs ceasing to be eligible to act on behalf of a Party or RDP 13

5 Detailed Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures and processes 14

5.1 Procedure and processes to verify organisational identity 14

5.3 Procedure for becoming a Senior Responsible Officer 17

5.4 Procedure for becoming an Authorised Responsible Officer 20

5.5 Procedure for provision of credentials to AROs for accessing SMKI Services and SMKI Repository Services 23

5.6 Procedure for becoming an Authorised Subscriber 32

6 SMKI Registration Authority registration procedures 35

6.1 General registration obligations 35

6.2 Procedure for becoming a SMKI Registration Authority Manager 36

6.3 Procedure for becoming a member of SMKI Registration Authority Personnel 37

6.4 Procedure for provision of credentials to a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel 38

7 Submission of CSRs and Issuance of Certificates 40

7.1 Submission of Certificate Signing Requests 40

7.2 Issuance of Certificates 40

8 Revocation 41

8.1 Revocation of Device Certificates 41

8.2 Revocation of Organisation Certificates 41

8.2.1 General Organisation Certificate revocation obligations 41

8.2.2 Procedure for Organisation Certificate Revocation 42

8.3 Revocation of SMKI Services and/or SMKI Repository Services access credentials 44

8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and/or SMKI Repository Services and / or File Signing Certifcates 44

8.3.2 Procedure for revocation of SMKI Services and/or SMKI Repository Services access credentials for AROs 45

8.3.3 General obligations relating to revocation of SMKI Registration Authority Manager or SMKI Registration Authority Personnel credentials for accessing SMKI Services and/or SMKI Repository Services 47

8.3.4 Procedure for revocation of SMKI Services access credentials for SMKI Registration Authority Managers and SMKI Registration Authority Personnel 48

Appendix A – Form Templates…….47

Appendix B – Definitions 50

1 Introduction

1.1 Purpose

Section L9.6 of the Code sets out the process for the DCC to develop the SMKI Registration Authority Policies and Procedures (SMKI RAPP) as a SMKI SEC Document as defined in Section L 9.4 (a) (v).

The SMKI RAPP sets out the principle obligations and activities undertaken by the DCC in its capacity as the SMKI Registration Authority in accordance with Section L of the Code, and Appendices A, B [and the IKI Certificate Policy] to the Code. The SMKI RAPP also sets out the activities undertaken by the SMKI Registration Authority in support of the procedures set out in the DCCKI RAPP, as set out in Section 2 of this document.

2 SMKI Registration Authority obligations to support DCCKI identity verification

The DCCKI RAPP sets out the procedures by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP, the Panel or a DCC Service Provider in respect of DCCKI Services and DCCKI Repository Services. The DCCKI RAPP also sets out the activities undertaken by the DCC as DCCKI Registration Authority.

Upon request from the DCCKI Registration Authority to verify the identity of an individual nominated to be a DCCKI SRO or DCCKI ARO, the SMKI Registration Authority shall:

a) arrange a verification meeting with the nominated individual, at a date and time that is mutually agreed;

b) at the verification meeting, verify the individual identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG 45 (Identity Proofing and Verification of an Individual), or except to the extent that the DCC otherwise notifies the SMKI Registration Authority, to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA for the purposes of verification of individuals to become an SMKI SRO or SMKI ARO;

c) following the verification meeting, notify the nominated individual whether the process to verify their individual identity has been successful; and

d) following the verification meeting, confirm in writing to the DCCKI Registration Authority whether the identity of the individual has been successfully verified.

All other procedural steps required by which nominated individuals may become DCCKI Senior Responsible Officers and/or DCCKI Authorised Responsible Officers in order to act on behalf of a Party, RDP, the Panel or DCC Service Provider (acting on behalf of the DCC) in respect of DCCKI Services and DCCKI Repository Services are as set out in the DCCKI RAPP.

Provided that the DCC need not repeat these processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming a DCCKI SRO and/or DCCKI ARO where the required verification processes have already been carried out for the purposes of identifying them as being an SMKI SRO and/or SMKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a DCCKI ARO or DCCKI SRO, be treated as if it had taken place after that date.

3 SMKI Roles

This SMKI RAPP details the roles of Parties, RDPs, the SMKI PMA, the Panel and DCC in the context of access to SMKI Services and/or SMKI Repository Services as set out in the Code, this SMKI RAPP and the SMKI Interface documents. The SMKI RAPP sets out the procedures by which nominated individuals may become Senior Responsible Officers and/or Authorised Responsible Officers in order to act on behalf of a Party, RDP, the SMKI PMA, the Panel or the DCC (acting in its role as DCC Service Provider) in respect of SMKI Services and SMKI Repository Services.

This SMKI RAPP also details the obligations in respect of the SMKI Registration Authority and the individuals acting on its behalf as SMKI Registration Authority Managers or SMKI Registration Authority Personnel.

From time to time, the SMKI PMA may require documents or information to be lodged in the SMKI Repository. In such instances, it shall submit a request via the DCC Service Desk and provide such documents and/or information to be lodged in the SMKI Repository. The DCC shall lodge documents and/or information provided to the SMKI Repository, as soon as reasonably practicable following receipt.

3.1 Party, RDP, SMKI PMA, Panel and DCC representatives

Individuals permitted to act as representatives of a Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) are as set out immediately below:

- **Senior Responsible Officer (SRO**). The process by which an individual is nominated and their authorisation is checked and their identity verified, so as to be an SRO and act on behalf of an organisation is set out in SMKI RAPP Section 5.2. An individual is nominated to become an SRO by a Director or Company Secretary for a Party, RDP or the DCC (for DCC Service Provider personnel), the SMKI PMA Chair for the SMKI PMA or the Panel Chair for the Panel. Once an individual has become an SRO, the SRO may at any time nominate individuals to undertake to become Authorised Responsible Officers (AROs) and to access SMKI Services and/or SMKI Repository Services. An SRO may also nominate themselves to become an ARO as described below.
- **Authorised Responsible Officer (ARO)**. The process by which an individual is nominated, verified and authorised to be an ARO is set out in SMKI RAPP Section 5.4. The means by which AROs are provided with credentials to authenticate access to SMKI Services and/or SMKI Repository Services is set out in Section 5.5. The DCC shall permit only AROs to act on behalf of a Party, RDP, SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) for the purposes of accessing SMKI Services and/or SMKI Repository Services. Depending upon the processes followed, an ARO may also be authorised to act on behalf of a Party or the DCC (in its role as DCC Service Provider) to be an Authorised Subscriber for Organisation Certificates, Device Certificates or both, following successful completion of SMKI and Repository Entry Process Tests. All AROs are also permitted to access SMKI Repository Services on behalf of the organisation that they represent, as set out in the SMKI Repository Interface Design Specification.

Each Party, RDP or the DCC (in its role as DCC Service Provider) that wishes to:

a) become an Authorised Subscriber for Organisation Certificates and/or Device Certificates;

b) become an Authorised Subscriber for an IKI Certificate for the purposes of Digitally Signing of files; or

c) have access only to the SMKI Repository,

shall have at least one ARO successfully appointed (and therefore one SRO).

The DCC shall not be required to repeat processes in relation to an individual for the purposes of verifying their identity for the purposes of becoming an SRO and/or ARO in respect of SMKI Services or SMKI Repository Services, where the required verification processes have already been carried out for the purposes of identifying them as being a DCCKI SRO and/or DCCKI ARO respectively.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing an ARO or SRO or the Party or RDP becoming an Authorised Subscriber, be treated as if it had taken place after that date.

3.2 SMKI Registration Authority representatives

Individuals acting as representatives of the DCC in its role as SMKI Registration Authority are:

- **SMKI Registration Authority Manager**. The process by which a SMKI Registration Authority Manager is nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or SMKI Repository Services is set out in SMKI RAPP Sections 6.2 and 6.4.
- **SMKI Registration Authority Personnel.** The process by which SMKI Registration Authority Personnel are nominated, verified, authorised and provided with the means to authenticate their access to SMKI Services and/or SMKI Repository is set out in SMKI RAPP Sections 6.3 and 6.4.

The DCC shall ensure that only a SMKI Registration Authority Manager or SMKI Registration Authority Personnel may act on behalf of the DCC in respect of matters relating to the SMKI Registration Authority. Each Party, RDP, the SMKI PMA, the Panel and the DCC (in its role of DCC Service Provider) shall refrain from dealing with DCC personnel (including Registration Authority Managers and Registration Authority Personnel) other than as directed by the DCC Service Desk for the purposes of submitting CSRs and CRRs.

The DCC, in order to perform its role as SMKI Registration Authority, shall nominate at least two individuals to become a SMKI Registration Authority Manager, each of which will have responsibility for:

a) management of the SMKI Registration Authority function and SMKI Registration Authority Personnel;

b) nomination of individuals to become SMKI Registration Authority Personnel;

c) authentication and verification of SMKI Registration Authority Personnel, as set out in Section 6.3 of this document; and

d) provision of the means to authenticate access to SMKI Services and/or SMKI Repository for authorised Party or RDP representatives, SMKI PMA members, Panel Members, and DCC personnel (including SMKI Registration Authority Personnel);

e) managing the process by which documents and information are lodged in the SMKI Repository; and

f) approval of CRRs.

A SMKI Registration Authority Manager may nominate individuals to become SMKI Registration Authority Personnel and to act on behalf of the SMKI Registration Authority as set out in this SMKI RAPP and the Code. The primary responsibilities of SMKI Registration Authority Personnel are:

a) to conduct registration processes as set out in SMKI RAPP Sections 5 to 5.6, incorporating:
   i. verification of organisational identity;
   ii. verification and authorisation of individuals nominated to become SROs of AROs, as set out in Section 5.2 and 5.4 of this document;
   iii. provision of the means to authenticate access to SMKI Services and/or SMKI Repository Services for authorised Party or RDP representatives, SMKI PMA members, Panel Members and DCC personnel ; and
   iv. assessment of whether an organisation qualifies to become an Authorised Subscriber for Organisation Certificates and/or Device Certificates.

b) processing and approval (where required) of Certification Signing Requests and Certificate Revocation Requests; and

c) processing of requests for revocation of credentials used to access SMKI Services and/or SMKI Repository Services.

The DCC shall ensure that SMKI Registration Authority Managers and SMKI Registration Authority Personnel, where required, are available to undertake the obligations in respect of procedures set out in this SMKI RAPP:

a) in respect of the verification, processing and approval of Certificate Revocation Requests (CRRs), on a 24*7 basis; and

b) in respect of all other procedures as set out in this SMKI RAPP, on a Working Day basis and during standard working hours in England.

The DCC and any Party or RDP may agree that any action taken by either of them prior to the date of the designation of this SMKI RAPP shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI RAPP for the purposes of appointing a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, be treated as if it had taken place after that date.

4 Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures

4.1 General registration obligations

4.1.1 Organisation, individual, and RA obligations

Each Party, RDP, the SMKI PMA, the Panel and the DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or SMKI Repository Services shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.6, as appropriate.

To facilitate this, the SMKI Registration Authority shall:

a) make the forms as set out in SMKI RAPP Appendices A to E, available via the internet facing DCC Website;

b) provide reasonable support and advice to each Party, the SMKI PMA, the Panel and DCC Service Providers in relation to the procedures as set out in SMKI RAPP sections 5.1 to 5.6;

c) place no restriction on the number of individuals that can be nominated as SROs or AROs in respect of any Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider);

d) permit an individual to become an ARO to represent multiple parties, by successfully completing the procedures in SMKI RAPP section 4 as are necessary;

e) store and maintain records relating to the nomination, verification and authorisation of individuals and organisations (but not the personal details of individuals) as set out Sections 5.1 to 5.6, and in accordance with the Code and the DCC's data retention policy and data protection policy;

f) not permit any nominated individual to access the SMKI Services or relevant SMKI Repository Services on behalf of a Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) until they have become an ARO;

g) ensure that credentials issued under the IKI Certificate Policy to AROs have a lifetime of ten years following and that such credentials and shall cease to be valid after ten years following issuance;

h) for authentication and file signing credentials issued under the IKI Certificate Policy and where the Key Pair and Certificate Signing Request are both generated by the ARO on a Cryptographic Credential Token during the ARO verification meeting, that the ARO has an opportunity to validate and agree information (e.g. Role and other organisation and individual identity) against which the Certificate is Issued is accurate and that it reflects the identity of the ARO or system that is the subject of the Certificate;

i) for authentication and file signing credentials issued under the IKI Certificate Policy and which are delivered to the SMKI Registration Authority in the form of a Certificate Signing Request generated by the ARO's organisation and provided by the ARO during the ARO verification meeting , that the ARO has an opportunity to validate the information in the resulting Certificate reflects that provided in the Certificate Signing Request and that it is accurate and reflects the identity of the ARO or system that is the subject of the Certificate;

j) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked; and

k) produce, each month, and make available to each Party, RDP, the SMKI PMA and the Panel, a report for that organisation which details the list of SROs, AROs, the credentials that have been issued to each ARO and those AROs for which credentials will expire in the following month.

4.1.2 High level overview of SMKI Registration Authority procedures

Figure 1 as set out immediately below provides a high level view of the procedures required in order for a Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider) to:

- verify their organisational identity;
- become a SRO;
- become an ARO;
- gain credentials for accessing SMKI Services and/or SMKI Repository;
- become an Authorised Subscriber for:
    - Organisation Certificates or Device Certificates, or both;
    - a File Signing Certificate (issued under the IKI Certificate Policy) for the purposes of Digitally Signing of files in accordance with the Code;
- gain access to Organisation Certificates and/or Device Certificates and other material via the SMKI Repository; and
- gain access to the File Signing Certificate to be used for the purposes of Digitally Signing of files.

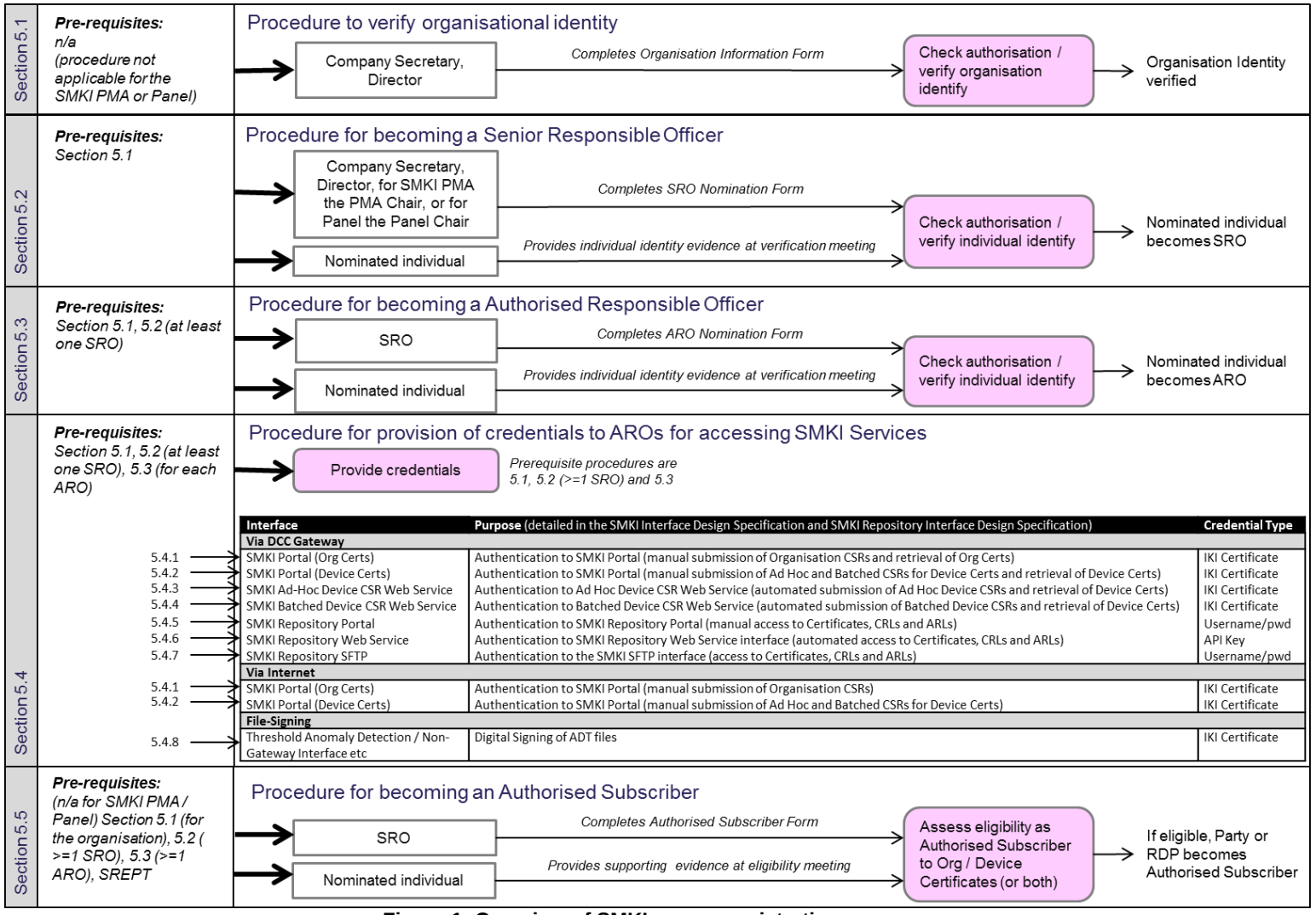

Figure 1: Overview of SMKI access registration processes

- SMKI RAPP Section 5.1 sets out the procedure and detailed processes for confirming the role of the nominating individual and verifying the organisational identity of the Party, RDP or DCC Service Provider, which shall be conducted where its identity has not previously been established. DCC shall not conduct the procedure in the case that the applicant is the SMKI PMA or the Panel.
- SMKI RAPP Section 5.2 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an SRO. The DCC shall ensure that an individual cannot become an SRO until the organisational identity of the applicant has been verified, unless (as set out immediately above) the applicant is the SMKI PMA or the Panel.
- SMKI RAPP Section 5.4 sets out the procedure and detailed processes for verifying the identity of an individual nominated to become an ARO. The DCC shall ensure that an individual cannot become an ARO until the organisation has at least one SRO and the organisational identity of the applicant has been verified, unless the applicant is the SMKI PMA or the Panel.
- Once an individual has become an ARO, SMKI RAPP Section 5.5 sets out the procedure and detailed processes by which the appropriate credentials used to access SMKI Services and/or SMKI Repository Services are provided to AROs.
- Where an applicant wishes to be an Authorised Subscriber for Organisation Certificates or Device Certificates or both, Section 5.6 of the SMKI RAPP sets out the procedure and detailed processes by which the DCC determines if the applicant is eligible to become an Authorised Subscriber for such Organisation Certificates or Device Certificates or both.

In respect of the procedures and detailed processes set out in SMKI RAPP Sections 5.1 to 5.6, the DCC shall place no restriction on the number of forms that can be submitted by an individual Party, RDP, the SMKI PMA, the Panel or the DCC. Where reasonably practicable, the DCC shall conduct the procedures as set out in SMKI RAPP Sections 5.1 to 5.6 such that where multiple forms are submitted at the same time, multiple procedures can be conducted within a single visit to the DCC's offices by the applicant's nominated individuals.

4.1.3 Change of details

If there is a change to any of the information used to verify the organisational identity of any Party, RDP or a DCC Service Provider (acting on behalf of the DCC), an SRO shall advise the DCC Service Desk of the change and shall ensure that the procedure and detailed processes as set out in SMKI RAPP Section 5.1 is undertaken in respect of the revised evidence of identity, as soon as is reasonably practicable after the change occurs.

If there is a change to any of the information used to verify the identity of any SRO or ARO, an SRO shall:

a) advise the DCC Service Desk of the change;

b) ensure that its SRO or ARO undertakes the procedures as set out in SMKI RAPP Sections 5.2 or 5.4 in respect of the revised evidence of identity, as soon as is reasonably practicable after the change occurs ; and

c) for an ARO ensure that credentials used to access SMKI Services and/or SMKI Repository Services are revoked as set out in SMKI RAPP Section 8.3.

No Party, RDP, the SMKI PMA, Panel or the DCC (acting as DCC Service Provider) shall unreasonably withhold information that is required by the SMKI Registration Authority in order to perform the procedures as set out in SMKI RAPP Sections 5.1 to 5.6.

4.1.4 Director or Company Secretary ceasing to be eligible to act on behalf of a Party or RDP

Where Director or Company Secretary ceases to be eligible to act on behalf of a Party or RDP in respect of the procedures set out in the SMKI RAPP:

a) the Director or Company Secretary themselves, or another Director or Company Secretary whose identity has previously been verified by the DCC, shall advise the DCC Service Desk of the change;
b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from a Director or Company Secretary; and
c) if b) is successful, the DCC shall update the DCC's records of authorised individuals for the Party or RDP and shall no longer consider the individual to be able to act on behalf of that Party or RDP.

4.1.5 SROs ceasing to be eligible to act on behalf of a Party or RDP

Where an SRO ceases to be eligible to act on behalf of a Party or RDP in respect of the procedures set out in the SMKI RAPP:

a) the SRO themselves, or a Director or Company Secretary whose identity has previously been verified by the DCC, shall advise the DCC Service Desk of the change;
b) the DCC shall confirm such information from the relevant Nominee Details Form, in order to provide confidence that the request is from the SRO, an authorised Director or Company Secretary; and
c) if b) is successful, update the DCC's records of authorised individuals for the Party or RDP and shall no longer consider the individual to be able to act on behalf of that Party or RDP.

5 Detailed Party, RDP, SMKI PMA, Panel and DCC (as DCC Service Provider) registration procedures and processes

Each Party, RDP, the SMKI PMA, the Panel and DCC (in its role as DCC Service Provider) shall ensure that its nominated representatives wishing to access SMKI Services and/or SMKI Repository Services shall undertake the procedures and processes as set out in SMKI RAPP Sections 5.1 to 5.5, as appropriate.

5.1 Procedure and processes to verify organisational identity

The processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to verify the organisational identity of a Party, RDP or DCC Service Provider (acting on behalf of the DCC). As set out in section 4.1.2 of this document, the SMKI Registration Authority shall not complete this procedure in respect of the SMKI PMA or the Panel.

Step	When	Obligation	Responsibility	Next Step
5.1.1	As required	The applicant organisation shall complete the Organisation Information Form, as set out in SMKI RAPP Appendix A (A1). In doing so, the applicant organisation shall ensure that: a) the information entered on the form is complete and accurate; b) the EUI64 Identifier range for any particular User Role is defined by the applicant organisation such that the range is continuous and does not overlap with the EUI64 Identifier range for any other User Role, other than where a particular EUI64 Identifier is allowed to be used for more than one User Role in accordance with H1.5; and c) the Organisation Information Form is authorised by a Director or Company Secretary on behalf of the applicant organisation. The applicant organisation shall also complete the Nominee Details Form, as set out in SMKI RAPP Appendix A (A5), for the Director or Company Secretary that has authorised the Organisation Information Form. In doing so, the applicant organisation shall ensure that the information entered on the form is complete and accurate.	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC Service Provider	5.1.2
5.1.2	As required, following 5.1.1	Submit the completed Organisation Information Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC Service Provider	5.1.3

Step	When	Obligation	Responsibility	Next Step
5.1.3	As soon as reasonably practicable following receipt of completed Organisation Information Form	Acknowledge receipt by email to the Director or Company Secretary that has authorised the Organisation Information Form	SMKI Registration Authority	5.1.4
5.1.4	As soon as reasonably practicable following 5.1.3	Confirm that the nominating Director or Company Secretary holds such a position within the application organisation, via a public information source. Analyse the information entered on the Organisation Information Form and Nominee Details Form, to determine completeness, discrepancies and whether the submitted EUI64 Identifier ranges are consistent with the restriction set out in step 5.1.1. Where there are omissions/discrepancies or the submitted EUI64 Identifier ranges are not consistent with the restriction set out in step 5.1.1, the SMKI Registration Authority shall agree actions and/or amendments, via email or in writing, with the Director or Company Secretary that has authorised the Organisation Information Form	SMKI Registration Authority	If complete, accurate and no discrepancies, 5.1.6; if not complete and accurate or any discrepancies, 5.1.5
5.1.5	Once omissions / discrepancies addressed	Submit a revised Organisation Information Form and/or Nominee Details Form to the SMKI Registration Authority, or in writing as directed on the DCC Website	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC Service Provider	5.1.3
5.1.6	As soon as reasonably practicable, following 5.1.4	Agree with the applicant organisation and confirm, by email, the date and time of a meeting to verify the organisation identity to the Director, or Company Secretary that has signed the Organisation Information Form. The meeting shall be held at DCC's offices unless otherwise agreed by the DCC Chief Information Security Officer, where such DCC agreement shall not unreasonably be withheld.	SMKI Registration Authority	5.1.7
5.1.7	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the applicant Director, Company Secretary, SMKI PMA Chair or Panel Chair, by email and telephone, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, an SRO shall inform the SMKI Registration	SMKI Registration Authority or applicant organisation, as appropriate	5.1.8

Step	When	Obligation	Responsibility	Next Step
		Authority, by email and telephone, and shall agree and confirm an alternative date and time.		
5.1.8	In meeting to verify organisational identity	Verify: a) the organisational identity of the applicant organisation to Level 3 (Verified) pursuant to the CESG GPG46 (Organisation Identity) , or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA; b) via information held by SECCo, that the applicant organisation has the User Role or User Roles as specified in Organisation Information Form; c) proof of individual identity provided for the nominating individual against the information listed on the Organisation Information Form and the Nominee Details Form; and d) individual identity of the nominating individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.	SMKI Registration Authority	If not successful, 5.1.9; if successful, 5.1.10
5.1.9	As soon as reasonably practicable, following 5.1.8	Notify the nominating Director or Company Secretary that verification of the organisational identity has been unsuccessful, in writing	SMKI Registration Authority	5.1.5 once issues addressed
5.1.10	As soon as reasonably practicable, following 5.1.8	Inform the nominating Director or Company Secretary that the organisational identity has been successfully verified, in writing	SMKI Registration Authority	5.1.11
5.1.11	As soon as reasonably practicable, following 5.1.10	Add the verified organisation to the DCC's list of such organisations, in accordance with Section 4.1.2 of Appendix A to the Code and Section 4.1.2 of Appendix B to the Code	SMKI Registration Authority	End of procedure

5.3 Procedure for becoming a Senior Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become a Senior Responsible Officer in respect of that Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.2.1	As required	Complete the SRO Nomination Form and Nominee Details Form, as set out in SMKI RAPP Appendix A (A3) and Appendix A (A5). In doing so, the individual completing the SRO Nomination Form and Nominee Details Form shall ensure that the information entered on the forms is complete and accurate, and that: a) the nominating individual is: i. for a Party, RDP or the DCC (as DCC Service Provider), a Director of, or Company Secretary of and an employee of, the applicant organisation or its parent organisation; ii. for the SMKI PMA, the SMKI PMA Chair; or iii. for the Panel, the Panel Chair; and b) the SRO Nomination Form and Nominee Details Form are both authorised, where applicable, by a Director or Company Secretary, SMKI PMA Chair or Panel Chair on behalf of the applicant organisation	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC (as DCC Service Provider). If nominated on behalf of the SMKI PMA, the SMKI PMA Chair. If nominated on behalf of the Panel, the Panel Chair.	5.2.2
5.2.2	As required, following 5.2.1	Submit the completed SRO Nomination Form and Nominee Details Form to the SMKI Registration Authority, in writing, as directed on the DCC Website	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC (as DCC Service Provider). If nominated on behalf of the SMKI PMA, the SMKI PMA Chair. If nominated on behalf of the Panel, the Panel Chair.	5.2.3
5.2.3	As soon as reasonably practicable following receipt of completed SRO Nomination Form	Acknowledge receipt by email to the Director, Company Secretary, SMKI PMA Chair or Panel Chair that has authorised the SRO Nomination Form	SMKI Registration Authority	5.2.4

Step	When	Obligation	Responsibility	Next Step
5.2.4	As soon as reasonably practicable following 5.2.3	Analyse the information entered on the SRO Nomination Form and Nominee Details Form, to: a) determine completeness and any discrepancies; and b) confirm, using the DCC's records or using publicly available information, that the Director, Company Secretary, SMKI PMA Chair or Panel Chair that has authorised the SRO Nomination Form has the role indicated on the SRO Nomination Form. Where there are omissions/discrepancies, agree actions with the nominating individual, via email or in writing	SMKI Registration Authority	If complete, 5.2.6; if not complete, 5.2.5
5.2.5	Once omissions / discrepancies addressed	Submit a revised SRO Nomination Form and/or Nominee Details Form to the SMKI Registration Authority, in writing as directed on the DCC Website	Director or Company Secretary, on behalf of the applicant organisation, which shall be a Party, RDP or DCC (as DCC Service Provider). If nominated on behalf of the SMKI PMA, the SMKI PMA Chair. If nominated on behalf of the Panel, the Panel Chair	5.2.3
5.2.6	As soon as reasonably practicable, following 5.2.4	Contact the Director, Company Secretary, SMKI PMA Chair or Panel Chair that nominated the individual, via telephone, using the telephone number provided previously in the Organisation Nomination Form, to confirm whether each nominated individual on the SRO Nomination Form is authorised to act on behalf of the organisation as SRO and seek confirmation of information provided on the SRO Nomination Form in order to provide confidence that the correct person has been contacted	SMKI Registration Authority	If confirmed as authorised, 5.2.8; if not confirmed as authorised, 5.2.7
5.2.7	As soon as reasonably practicable following rejection	Inform the applicant organisation that the application to become a Senior Responsible Officer has not been successful, in writing to the Director, Company Secretary, SMKI PMA Chair or Panel Chair that has authorised the SRO Nomination Form	SMKI Registration Authority	5.2.6 once issues resolved
5.2.8	As soon as reasonably practicable, following 5.2.6	Agree, via email with the Director, Company Secretary, SMKI PMA Chair or Panel Chair of the applicant organisation who nominated the individual to become a Senior Responsible Officer, a date and time for the nominated individual(s) to attend a verification meeting	SMKI Registration Authority	5.2.9

Step	When	Obligation	Responsibility	Next Step
5.2.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI Registration Authority Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform the nominated individual and the applicant Director, Company Secretary, SMKI PMA Chair or Panel Chair, by email and telephone, and shall agree and confirm an alternative date and time. If it is identified that the individual(s) nominated to act on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, the nominated individual shall inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.2.10
5.2.10	In SRO verification meeting	At the face-to-face SRO verification meeting, the SMKI Registration Authority shall, in person: a) check proof of individual identity provided for each nominated individual against the information listed on the SRO Nomination Form and the Nominee Details Form; and b) verify the individual identity for each nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	SMKI Registration Authority	If not successfully verified, 5.2.11; if successfully verified, 5.2.12
5.2.11	As soon as reasonably practicable, following verification meeting	Notify the Director, Company Secretary, SMKI PMA Chair or Panel Chair, in writing, that the nominated individual(s) has not been verified successfully and has not become a Senior Responsible Officer on behalf of the applicant organisation	SMKI Registration Authority	5.2.5 once issues addressed
5.2.12	As soon as reasonably practicable, following verification meeting	Notify the Director, Company Secretary, SMKI PMA Chair or Panel Chair, in writing, that the nominated individual(s) has become a Senior Responsible Officer on behalf of the applicant organisation	SMKI Registration Authority	5.2.13
5.2.13	As soon as reasonably practicable, 5.2.12	Add the relevant SRO to the DCC's list of SROs, in accordance with Section 4.1.2 of Appendix A to the Code and Section 4.1.2 of Appendix B to the Code	SMKI Registration Authority	End of Procedure

5.4 Procedure for becoming an Authorised Responsible Officer

The procedure as detailed immediately below shall be conducted by the SMKI Registration Authority in order to check the authorisation and verify the identity of any individual that has been nominated to become an Authorised Responsible Officer in respect of that Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider).

Step	When	Obligation	Responsibility	Next Step
5.3.1	As required	Complete the ARO Nomination Form and Nominee Details Form as set out in SMKI RAPP Appendix A (A4) and Appendix A (A5), ensuring that; a) the information entered on the forms is complete and accurate; and b) the ARO Nomination Form and Nominee Details Form are authorised by an SRO on behalf of the applicant organisation	SRO on behalf of the applicant organisation, which shall be a Party, RDP, the SMKI PMA, the Panel or DCC (as DCC Service Provider)	5.3.2
5.3.2	As required, following 5.3.1	Submit the completed ARO Nomination Form and Nominee Details Form to the SMKI Registration Authority in writing, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party, RDP, the SMKI PMA, the Panel or DCC (as DCC Service Provider)	5.3.3
5.3.3	As soon as reasonably practicable following receipt of completed ARO Nomination Form and Nominee Details Form	Acknowledge receipt by email to the SRO as identified on the ARO Nomination Form	SMKI Registration Authority	5.3.4
5.3.4	As soon as reasonably practicable following 5.3.3	Analyse the information entered on the ARO Nomination Form and Nominee Details Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	SMKI Registration Authority	If complete, 5.3.6; if not complete, 5.3.5
5.3.5	Once omissions / discrepancies are addressed	Submit a revised ARO Nomination Form and/or Nominee Details Form to the Registration Authority in writing as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party, RDP, the SMKI PMA, the Panel or DCC (as DCC Service Provider)	5.3.3

Step	When	Obligation	Responsibility	Next Step
5.3.6	As soon as reasonably practicable, following 5.3.4	Contact an SRO of the applicant organisation via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm whether the nominated individual is authorised to become an ARO	SMKI Registration Authority	If confirmed as authorised, 5.3.8; if not authorised, 5.3.7
5.3.7	As soon as reasonably practicable following rejection	Notify an SRO that the procedure for becoming an ARO has not been successful for relevant nominated individual, in writing	SMKI Registration Authority	5.3.5 once issues addressed
5.3.8	As soon as reasonably practicable, following 5.3.6	Agree with the applicant organisation and confirm the date and time for the ARO verification meeting, via email to an SRO for the applicant organisation and the nominated individual	SMKI Registration Authority	5.3.9
5.3.9	As soon as reasonably practicable on becoming aware of unavailability	If it is identified that SMKI RA Personnel will be unavailable to conduct the verification meeting on the agreed date and time, the SMKI Registration Authority shall inform an SRO and the nominated individual, by email and telephone, and shall agree and confirm an alternative date and time. If it is identified that the nominated individual(s) acting on behalf of the applicant organisation will be unavailable to attend the verification meeting on the agreed date and time, an SRO shall inform the SMKI Registration Authority, by email and telephone, and shall agree and confirm an alternative date and time.	SMKI Registration Authority or applicant organisation, as appropriate	5.3.10
5.3.10	In ARO verification meeting	At the ARO face-to-face verification meeting, the SMKI Registration Authority shall, in person, for the nominated individual: a) check proof of individual identity provided against the information listed on the ARO Nomination Form and Nominee Details Form; and b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	SMKI Registration Authority	If verified, 5.3.12; if not verified, 5.3.11

Step	When	Obligation	Responsibility	Next Step
5.3.11	As soon as reasonably practicable, following ARO verification meeting	Notify: a) the nominated individual that they have become an ARO, verbally; or b) in writing to the SRO, that the verification has not been successful for the nominated individual, that the nominated individual has not become an ARO, and provide reasons for the rejection and request that the nominated individual is required to attend a further ARO verification meeting once the issues have been remedied	SMKI Registration Authority	If successful, 5.3.12; otherwise 5.3.5 once issues are addressed
5.3.12	As soon as reasonably practicable, following ARO verification meeting	Notify the applicant organisation, to the SRO on behalf of the applicant organisation, in writing of the individuals whose identify has been verified and have become AROs	SMKI Registration Authority	5.3.13
5.3.13	As soon as reasonably practicable, following 5.3.12	Add the relevant individual to the DCC's list of AROs	SMKI Registration Authority	Procedure as set out in SMKI RAPP section 5.5

5.5 Procedure for provision of credentials to AROs for accessing SMKI Services and SMKI Repository Services

The procedure and processes as detailed immediately below shall be conducted by the SMKI Registration Authority in order to provide credentials for accessing SMKI Services and/or SMKI Repository Services to Authorised Responsible Officers in respect of a Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider). The SMKI Registration Authority shall not provide such credentials to an individual on behalf of a Party, RDP, the SMKI PMA, the Panel or the DCC (in its role as DCC Service Provider), other than where the organisation has completed SMKI and Repository Entry Process Tests and such individuals have become Authorised Responsible Officers.

Step	When	Obligation	Responsibility	Next Step
5.4.1	During ARO verification meeting and after becoming an ARO	**IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Organisation Certificates and/or Device Certificates, and where the Party, RDP or DCC Service Provider has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: a) If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of Organisation CSRs and retrieval of corresponding Organisation Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet. b) If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of Organisation CSRs and retrieval of corresponding Organisation Certificates. The DCC shall ensure that the	SMKI Registration Authority	5.4.2

Step	When	Obligation	Responsibility	Next Step
		Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via a DCC Gateway Connection. Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		
5.4.2	During ARO verification meeting and after becoming an ARO	**IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection or SMKI Portal via the Internet** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates, the Registration Authority shall determine, in accordance with the steps set out in Section 5.6 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall, if the ARO wishes to access the SMKI Portal Interface, provide the ARO with: a) If the applicant organisation has access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface for the purposes of submission of Device CSRs and retrieval of corresponding Device Certificates via a DCC Gateway Connection. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via the Internet.	SMKI Registration Authority	5.4.3

Step	When	Obligation	Responsibility	Next Step
		b) If the applicant organisation does not have access to a DCC Gateway Connection, one Cryptographic Credential Token containing credentials issued under the applicable IKI Certification Authority that authenticate the ARO to access the SMKI Portal Interface via the Internet for the purposes of submission of Device CSRs and retrieval of corresponding Device Certificates. The DCC shall ensure that the Cryptographic Credential Token enables the ARO to set a PIN code which shall be used each time the Cryptographic Credential Token is used, to render the Cryptographic Credential Token operative. Such credentials shall not allow the ARO to access the SMKI Portal Interface via a DCC Gateway Connection. Where the Party, RDP or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests, the DCC shall retain such Cryptographic Credential Token until such time as the Party, RDP or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, at which point the DCC shall send such Cryptographic Credential Token to the ARO via secure courier.		

Step	When	Obligation	Responsibility	Next Step
5.4.3	During ARO verification meeting and after becoming an ARO	**IKI credentials for Ad Hoc Device CSR Web Service** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Ad Hoc Device CSR Web Service, the SMKI Registration Authority shall, if the applicant organisation has access to a DCC Gateway Connection and is a Supplier Party or the DCC, and where the Supplier Party or DCC (in its role as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via USB token or optical media, with: a) Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided, via USB token or optical media, by the applicant organisation in accordance with the SMKI Interface Design Specification; and b) a CA/Browser Forum recognised certificate which enables verification of the Ad Hoc Device CSR Web Service interface server identity, and that will be used as part of mutual authentication to the Ad Hoc Device CSR Web Service interface If the Supplier Party or DCC (in its role as DCC Service Provider) has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the Supplier Party or DCC (as DCC Service Provider) has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Ad Hoc Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.	SMKI Registration Authority	5.4.4

Step	When	Obligation	Responsibility	Next Step
5.4.4	During ARO verification meeting and after becoming an ARO	**IKI credentials for Batched Device CSR Web Service** If the applicant has indicated on the Authorised Subscriber application form that it wishes to be an Authorised Subscriber for Device Certificates and it wishes to use the Batched Device CSR Web Service, the SMKI Registration Authority shall determine, if the applicant is not a Supplier Party or the DCC, in accordance with the steps set out in Section 5.6 of the SMKI RAPP, whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises. Where there is such reasonable evidence, and where the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the appointed ARO, via USB token or optical media, with: a) Batched Device CSR Web Service access credentials for Device Certificates, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification; and b) a CA/Browser Forum recognised certificate which enables verification of the Batched Device CSR Web Service interface server identity, and that will be used as part of mutual authentication to the Batched Device CSR Web Service interface. If the applicant organisation has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on a USB token or optical media via secure courier or by secured electronic means, the appointed ARO with Batched Device CSR Web Service access credentials for Device Certificates, which corresponds with a CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.	SMKI Registration Authority	5.4.5

Step	When	Obligation	Responsibility	Next Step
5.4.5	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository Portal** If the applicant organisation has access to a DCC Gateway Connection, and it wishes to access the SMKI Repository via the SMKI Repository Portal and has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password, to be accessed via the SMKI Repository Portal, that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification. If the applicant organisation has access to a DCC Gateway Connection, it wishes to access the SMKI Repository via the SMKI Repository Portal but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting: a) DCC shall, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, provide the appointed ARO with a username and password via secured electronic means that is specific to the Authorised Responsible Officer, for the purposes of authenticating to the SMKI Repository Portal via DCC Gateway Connection, as set out in the SMKI Repository Interface Design Specification.	SMKI Registration Authority	5.4.6

Step	When	Obligation	Responsibility	Next Step
5.4.6	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository Web Service** If the applicant organisation has access to a DCC Gateway Connection, and wishes to access the SMKI Repository Web Service interface and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification, along with a certificate which enables verification of the SMKI Repository Web Service server identity. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository Web Service interface but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide, on electronic media as set out in the SMKI Repository User Guide, the ARO with: a) the credentials required to authenticate to the SMKI Repository Web Service interface, as set out in the SMKI Repository Interface Specification; and b) a CA/Browser Forum recognised certificate which enables verification of the SMKI Repository Web Service interface server identity, and that will be used as part of mutual authentication to the SMKI Repository Web Service interface.	SMKI Registration Authority	5.4.7

Step	When	Obligation	Responsibility	Next Step
5.4.7	During ARO verification meeting and after becoming an ARO	**Credentials for SMKI Repository Portal SFTP** If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials and has successfully completed SMKI and Repository Entry Process Tests, provide the ARO with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface. If the applicant organisation has access to a DCC Gateway Connection, wishes to access the SMKI Repository using SSH File Transfer Protocol (SFTP) access credentials but has not successfully completed SMKI and Repository Entry Process Tests at the time of the verification meeting, once the applicant organisation has successfully completed SMKI and Repository Entry Process Tests, the SMKI Registration Authority shall provide the ARO, via the SMKI Repository Portal profile page, with credentials, in the form of a username and password, used to access the SSH File Transfer Protocol (SFTP) interface.	SMKI Registration Authority	5.4.8
5.4.8	During ARO verification meeting and after becoming an ARO	**IKI credentials for file signing** If the applicant organisation wishes the ARO to be Issued with a File Signing Certificate for the purposes as set out in the Code, the SMKI Registration Authority shall either a) provide the ARO with a Cryptographic Credential Token enabling the ARO to submit a CSR for a File Signing Certificate; in which case, the ARO shall use the software on the Cryptographic Credential Token to generate a Private Key for a File Signing Certificate to submit a CSR for a File Signing Certificate; and if the CSR is valid, the ICA shall Issue a File Signing Certificate under the IKI Certificate Policy, to be used for the purposes as set out in the Code; or b) provide the appointed ARO, via USB token or optical media, with an IKI File Signing Certificate, which shall be Issued by the DCC in response to a valid CSR that shall be provided by the applicant organisation in accordance with the SMKI Interface Design Specification.	SMKI Registration Authority	5.4.9

Step	When	Obligation	Responsibility	Next Step
5.4.9	During ARO verification meeting and after issuance of credentials	**Acceptance of credentials issued in steps 5.4.1 to 5.4.8** The SMKI Registration Authority shall complete the relevant sections of the Nominee Details Form in Appendix A (A5) accordingly. The ARO shall confirm receipt of and acceptance of the credentials issued by completing the relevant sections of the Nominee Details Form in Appendix A (A5). Should the ARO not wish to accept these credentials, the ARO shall notify the SMKI Registration Authority immediately and not sign for the Certificate and / or Cryptographic Credential.	SMKI Registration Authority ARO	End of procedure

5.6 Procedure for becoming an Authorised Subscriber

The procedure detailed immediately below shall be conducted by the DCC, in order to determine whether a Party or RDP has become an Authorised Subscriber for Organisation Certificates, an Authorised Subscriber for Device Certificates, or both.

Step	When	Obligation	Responsibility	Next Step
5.5.1	As required	Complete the Authorised Subscriber Application Form as set out in SMKI RAPP Appendix A (A2), ensuring that the information entered on the form is complete and accurate, and the Authorised Subscriber Application Form is authorised by an SRO on behalf of the applicant organisation	Nominating officer or SRO on behalf of the applicant organisation, which shall be a Party or RDP	5.5.2
5.5.2	As required, following 5.5.1	Submit the completed Authorised Subscriber Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website	Applicant organisation, which shall be a Party or RDP	5.5.3
5.5.3	As soon as reasonably practicable following 5.5.2	Acknowledge receipt by email to the SRO or nominating officer as identified on the Authorised Subscriber Application Form	SMKI Registration Authority	5.5.4
5.5.4	As soon as reasonably practicable following 5.5.3	Analyse the information entered on the Authorised Subscriber Application Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	SMKI Registration Authority	If complete, 5.5.6; if not complete, 5.5.5
5.5.5	Once omissions / discrepancies are addressed	Submit a revised Authorised Subscriber Application Form to the SMKI Registration Authority in writing, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party or RDP	5.5.3
5.5.6	As soon as reasonably practicable, following 5.5.4	Contact the SRO as identified on the Authorised Subscriber Application Form via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority. The SMKI Registration Authority shall verbally confirm details for the SRO as held by the DCC to verify that the correct individual has been contacted. The SMKI Registration Authority shall confirm the applications indicated on the Authorised Subscriber Application Form are authorised	SMKI Registration Authority	If confirmed as authorised, 5.5.8; if not authorised, 5.5.7
5.5.7	As soon as reasonably practicable following rejection	Notify the SRO as identified on the Authorised Subscriber Application Form that the procedure in respect of the application has not been successful, in writing	SMKI Registration Authority	5.5.5 once issues addressed

Step	When	Obligation	Responsibility	Next Step
5.5.8	As requested	Where the application organisation is not a DCC Service Provider, conduct the SMKI and Repository Entry Process Tests if SMKI and Repository Entry Process Tests have not been completed previously, in accordance with Sections H14.22 to H14.31 of the Code	Applicant organisation, in respect of the corresponding Authorised Subscriber Application Form	If successful or the applicant organisation is a DCC Service Provider (acting on behalf of the DCC), 5.5.10; if not successful, 5.5.9
5.5.9	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing, to SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the SMKI and Repository Entry Process Tests were not completed successfully	DCC	5.5.8 once issues addressed
5.5.10	As soon as reasonably practicable, following 5.5.8	The DCC shall confirm in writing to the relevant Party that the SMKI and Repository Entry Process Tests have been completed successfully	DCC	5.5.11
5.5.11	As soon as reasonably practicable, following 5.5.10	If the applicant organisation has indicated on its Authorised Subscriber Application Form that it wishes to become an Authorised Subscriber in respect of the Organisation Certificate Policy, the SMKI Registration Authority shall confirm in writing to the SRO as identified on the Authorised Subscriber Application Form that it the applicant organisation has become an Authorised Subscriber for Organisation Certificates Where appropriate, the DCC shall issue credentials enabling the applicant to act as an Authorised Subscriber for Organisation Certificates, in accordance with the procedural steps as set out in section 5.5 of this document.	SMKI Registration Authority	If the applicant organisation has indicated that it wishes to become an Authorised Subscriber for Organisation Certificates, 5.5.12; otherwise, 5.5.13
5.5.12	As soon as possible, following 5.5.11	Other than in the case of a Party who is a Supplier Party or a DCC Service Provider, if the applicant organisation has indicated on the Authorised Subscriber Application Form that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy, the SMKI Registration Authority shall assess whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become such an Authorised Subscriber in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises.	SMKI Registration Authority	If determined to be an Authorised Subscriber for Device Certificates, 5.5.16; otherwise 5.5.14

Step	When	Obligation	Responsibility	Next Step
5.5.13	As soon as possible, following 5.5.12	Confirm in writing, to the SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the DCC has determined that applicant organisation is not eligible to become an Authorised Subscriber for Device Certificates.	SMKI Registration Authority	If the applicant organisation wishes to refer the matter to the SMKI PMA or Panel, 5.5.14, otherwise End of procedure
5.5.14	As soon as possible, following 5.5.13	Determine whether there is reasonable evidence to suggest that it is necessary for the applicant organisation to become such an Authorised Subscriber in order for them to carry out business process that will, or are likely to, lead to the installation of Devices in premises. The SMKI PMA or Panel shall confirm the outcome to the DCC, in writing.	SMKI PMA or Panel	If determined to be an Authorised Subscriber for Device Certificates, 5.5.15; otherwise End of procedure
5.5.15	As soon as reasonably practicable, following 5.5.14, or, where a Supplier Party or the DCC (in its role as DCC Service Provider) has indicated that it wishes to become an Authorised Subscriber in respect of the Device Certificate Policy	The SMKI Registration Authority shall confirm in writing, to the SRO or nominating officer as identified on the Authorised Subscriber Application Form, that the applicant organisation has become an Authorised Subscriber for Device Certificates.	SMKI Registration Authority	5.5.16
5.5.16	As soon as reasonably practicable, following 5.5.15	The SMKI Registration Authority shall arrange and conduct a meeting, as soon as reasonably practicable, at which the credentials as set out in steps 5.4.2, 5.4.3 and 5.4.5 (as set out in Section 5.4 of this document) shall be provided, as appropriate.	SMKI Registration Authority	5.5.17
5.5.17	As soon as reasonably practicable, following 5.5.15 or 5.5.16	Update the DCC's list of Authorised Subscribers for Organisation Certificates and/or Device Certificates, for audit purposes.	SMKI Registration Authority	End of procedure

6 SMKI Registration Authority registration procedures

The procedures as set out in SMKI RAPP Sections 6.2 to 6.4 shall be undertaken in order for nominated individuals to act on behalf of the SMKI Registration Authority as a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel.

6.1 General registration obligations

The SMKI Registration Authority shall:

a) not permit any nominated individual to access Systems used to provide SMKI Services and/or SMKI Repository Services as a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel until the procedures in SMKI RAPP Sections 6.2 or 6.3 have been successfully completed;

b) in performing the procedures as set out in SMKI RAPP Sections 6.2 and 6.3, store and maintain records relating to individuals becoming SMKI Registration Authority Managers and SMKI Registration Authority Personnel, in accordance with the Code and the DCC's data retention policy;

c) ensure that, at all times, there are at least two SMKI Registration Authority Managers; and

d) if there is a change to any of the information used to verify the identity of any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, ensure that its SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel undertakes the procedures as set out in SMKI RAPP Sections 6.2 or 6.3 in respect of the revised evidence of identity.

The DCC shall ensure that:

a) for authentication credentials issued under the IKI Certificate Policy to Authorised Responsible Officers, ensure that such authentication credentials have a lifetime of ten years following issuance of such authentication credentials and shall cease to function upon after ten years following issuance; and

b) for authentication credentials not issued under the IKI Certificate Policy, shall ensure that such authentication credentials remain valid until revoked.

6.2 Procedure for becoming a SMKI Registration Authority Manager

The procedure for becoming a SMKI Registration Authority Manager as detailed immediately below shall be conducted by DCC's Chief Information Security Officer (CISO) on behalf of the DCC, in order to nominate, authorise and verify a SMKI Registration Authority Manager.

Step	When	Obligation	Responsibility	Next Step
6.2.1	As required	Nominate an individual to become a SMKI Registration Authority Manager, who shall be an employee of the DCC or be contracted to the DCC, and advise the nominated individual of the evidence to be provided in order to verify their identity	DCC Chief Information Security Officer, on behalf of the DCC	6.2.2
6.2.2	As soon as reasonably practicable following 6.2.1	Confirm verification meeting date/time with nominated individual	DCC Chief Information Security Officer, on behalf of the DCC	6.2.3
6.2.3	In verification meeting	The DCC shall, in accordance with the provisions of Sections G4.4 to G4.8: a) check proof of identity provided against the information provided by the nominated individual; and b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	DCC Chief Information Security Officer, on behalf of the DCC	If verified, 6.2.5. If not verified, 6.2.4
6.2.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the failure to the individual and notify the individual that a further verification meeting is required to remedy the unsuccessful elements of the verification	DCC Chief Information Security Officer, on behalf of the DCC	6.2.5
6.2.5	In verification meeting	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a SMKI Registration Authority Manager and notify the SMKI PMA that the nominated individual has become a SMKI Registration Authority Manager	DCC Chief Information Security Officer, on behalf of the DCC	6.2.6
6.2.6	As soon as reasonably practicable following 6.2.5	Record the details of the individual that has become a SMKI Registration Authority Manager, in a manner which is auditable	SMKI Registration Authority	Procedure as set out in SMKI RAPP Section 6.4

6.3 Procedure for becoming a member of SMKI Registration Authority Personnel

The procedure for becoming a member of SMKI Registration Authority Personnel as detailed immediately below shall be conducted by a SMKI Registration Authority Manager on behalf of the SMKI Registration Authority, in order to nominate, verify, authorise and provide means for authenticating access to Systems used to provide SMKI Services and/or SMKI Repository Services in respect of a member of SMKI Registration Authority Personnel.

Step	When	Obligation	Responsibility	Next Step
6.3.1	As required	Nominate an individual to become a member of SMKI Registration Authority Personnel, who shall be an employee of the DCC or be contracted to the DCC	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.2
6.3.2	As soon as reasonably practicable following 6.3.1	Confirm verification meeting date/time with nominated individual	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.3
6.3.3	In verification meeting	In the verification meeting, the DCC shall, in accordance with the provisions of Sections G4.4 to G4.8: a) check proof of identity provided against the information provided by the nominated individual; and b) verify the identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 (Identity Proofing and Verification of an Individual), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	If successful, 6.3.5. If not successful, 6.3.4
6.3.4	In verification meeting	If the identity of the nominated individual is not successfully verified, provide reasons for the rejection to the individual and notify the individual that a further meeting is required to remedy the affected elements of the verification	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.2
6.3.5	As soon as reasonably practicable, following 6.3.3	If the identity of the nominated individual is successfully verified, notify the individual verbally and subsequently in writing that they have become a member of SMKI Registration Authority Personnel.	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	6.3.6
6.3.6	As soon as reasonably practicable following 6.3.5	Record the details of the individual that has become a member of SMKI Registration Authority Personnel in respect of the SMKI Registration Authority, in a manner which is auditable	SMKI Registration Authority	Procedure as set out in SMKI RAPP Section 6.4

6.4 Procedure for provision of credentials to a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel

The procedure for provision of credentials to a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, as detailed immediately below, shall be conducted by the DCC's CISO in respect of a SMKI Registration Authority Manager or a SMKI Registration Authority Manager in respect of a member of SMKI Registration Authority Personnel.

Step	When	Obligation	Responsibility	Next Step
6.4.1	In verification meeting, following confirmation of becoming a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel	Provide credentials in accordance with step 6.4.2 or 6.4.3 below, depending on whether the individual has become a SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel	DCC	If providing to a SMKI Registration Authority Manager, 6.4.2; if providing to a member of SMKI Registration Authority Personnel, 6.4.3
6.4.2	In verification meeting, following confirmation of becoming a SMKI Registration Authority Manager	Provide the SMKI Registration Authority Manager with credentials as listed immediately below, to be used to perform activities on behalf of the SMKI Registration Authority: a) one Cryptographic Credential Token containing authentication credentials issued under the IKI Certificate Policy which can be used to authenticate the individual to the SMKI RA Portal; and b) usernames and passwords enabling for the purposes of authentication to the SMKI Repository Portal.	DCC's CISO	6.4.4
6.4.3	In verification meeting, following confirmation of becoming a member of SMKI Registration Authority Personnel	Provide the member of SMKI Registration Authority Personnel with credentials as listed immediately below, to be used to perform activities on behalf of the SMKI Registration Authority: a) one Cryptographic Credential Token containing authentication credentials issued under the IKI Certificate Policy which can be used to authenticate the individual to the SMKI RA Portal; and b) usernames and passwords enabling for the purposes of authentication to the SMKI Repository Portal.	SMKI Registration Authority Manager	6.4.4

Step	When	Obligation	Responsibility	Next Step
6.4.4	In verification meeting, following issuance of credentials	The SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel shall sign that they accept the credentials issued to them on the Cryptographic Credential Token. Where the SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel does not accept the credentials they shall notify the DCC's CISO (in the case of the SMKI Registration Authority Manager) or otherwise the SMKI Registration Authority Manager) and shall not sign for the Cryptographic Credential Token.	SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel	End of Procedure

7 Submission of CSRs and Issuance of Certificates

7.1 Submission of Certificate Signing Requests

The SMKI Interface Design Specification and the Code sets out the provisions in respect of:

a) the mechanism established for this purpose is in accordance with the procedure in PKCS#10;

b) naming restrictions in respect of the Subject of each Certificate in accordance with the relevant Certificate Profile;

c) the circumstances in which an Authorised Subscriber may submit a Certificate Signing Request (CSR) in respect of a Device Certificate and the means by which it may do so;

d) the circumstances in which an Authorised Subscriber may submit a CSR in respect of an Organisation Certificate and the means by which it may do so;

e) the circumstances in which an Authorised Subscriber for an IKI Certificate may submit a CSR in respect of an IKI Certificate and the means by which it may do so; and

f) requirements in respect of validation of the format of a CSR, checking that the submitting organisation is an Eligible Subscriber for the Certificate and rejection if such requirements are not met.

The SMKI Registration Authority shall validate the Subject of each Certificate to ensure that each CSR corresponds with an EUI64 Identifier range that is applicable to the relevant User Role, as provided in the Organisation Information Form.

Subject to the provisions of the Code and this SMKI RAPP, the DCC shall accept requests for copies of Organisation Certificates and/or Device Certificates from non DCC Users by phone via the DCC Service Desk or via the SMKI Portal via the Internet. The DCC shall, following such a request, provide the relevant information as soon as is reasonably practicable, via a secured electronic means.

7.2 Issuance of Certificates

The SMKI Interface Design Specification sets out the provisions in respect of:

a) the circumstances in which the DCA shall issue Device Certificates;

b) the circumstances in which the OCA shall issue Organisation Certificates;

c) the circumstances in which the ICA shall issue IKI Certificates; and

d) the obligations in respect of lodging Certificates in the SMKI Repository.

8 Revocation

8.1 Revocation of Device Certificates

In line with the SMKI Device Certificate Policy, Device Certificates cannot be revoked. As a result:

a) no organisation shall submit a Certificate Revocation Request (CRR) in respect of a Device Certificate; and

b) the DCC shall not be obliged to maintain a Device Certificate Revocation List (CRL) Device Authority Revocation List (ARL).

8.2 Revocation of Organisation Certificates

8.2.1 General Organisation Certificate revocation obligations

The DCC shall permit each of the following individuals to request the revocation of an Organisation Certificate, where the reasons for such revocation request must be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9 in Appendix B of the Code:

a) Any SMKI PMA member, on behalf of the SMKI PMA;

b) Any Senior Responsible Officer for a Subscriber for an Organisation Certificate; or

c) Any SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel, on behalf of the DCC.

The DCC, in its role as SMKI Registration Authority, shall only accept CRRs through the following mechanisms (or a combination of such mechanisms):

a) in writing, via registered post;

b) via a secured electronic means; or

c) in Person, at the offices of the SMKI Registration Authority, where the address of such offices shall be as set out on the DCC Website.

The revocation of an Organisation Certificate shall be permanent and the SMKI Registration Authority shall ensure that no revoked Organisation Certificate may be reinstated.

The DCC shall, each month, prepare and submit a report to the SMKI PMA regarding the number and nature of Organisation Certificate revocations.

8.2.2 Procedure for Organisation Certificate Revocation

The procedure for authorisation, verification and, where verified, revocation of Certificates is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.2.2.1	As soon as reasonably practicable when Certificate revocation is required	An SRO on behalf of a Subscriber, the DCC or the SMKI PMA shall submit, using the mechanisms set out in SMKI RAPP Section 8.2.1, a CRR to the SMKI Registration Authority. The reason for such CRR shall be one of the permitted reasons for Organisation Certificate revocation as set out in Section 4.9 in Appendix B of the Code. Each CRR shall contain the following information, as set out in SMKI RAPP **Error! Reference source not found.**: a) Identify the Subscriber; b) Identify the Subscriber's SRO who is submitting the CRR; c) Unambiguously (i.e. by specifying the serial number of the Certificate) identify the Certificate to be revoked; and d) State the reason for the Certificate revocation.	Subscriber requiring Organisation Certificate revocation	8.2.2.2
8.2.2.2	As soon as reasonably practicable, following 8.2.2.1	On receipt of a CRR, notify the SMKI Registration Authority Manager for verification, processing and/or approval. The SMKI Registration Authority shall treat each CRR and any associated circumstances as confidential.	SMKI Registration Authority Personnel	8.2.2.3
8.2.2.3	As soon as reasonably practicable following receipt	Validate the Certificate Revocation Request, by contacting a Senior Responsible Officer and confirming details for the SRO as provided in the original application to become an SRO: a) Where submitted in writing, the SMKI Registration Authority shall telephone a Senior Responsible Officer. The SMKI Registration Authority shall 1) confirm such information from the relevant SRO Nomination Form, in order to provide confidence that the request is from an authorised SRO; and 2) confirm the details of the Organisation Certificate to which the revocation request received relates (as provided in the submitted letter) b) Where submitted in person, the SMKI Registration Authority shall 1) verify the handwritten signature of the Senior Responsible Officer against that held by the SMKI Registration Authority; 2) confirm details provided in the relevant SRO Nomination Form, in order determine that the request is authentic; and 3) confirm the details of the Organisation Certificate to which the CRR received relates	SMKI Registration Authority Manager	If validated, 8.2.2.5; if invalid (considered malicious and/or inauthentic) or incomplete, 8.2.2.4

Step	When	Obligation	Responsibility	Next Step
8.2.2.4	As soon as reasonably practicable following unsuccessful validation	Reject the revocation request and notify the Senior Responsible Officer in respect of the Party that was contacted in step 7.2.2.3 to validate the revocation request, in writing, including the reasons for rejection and identify resulting steps to be taken	SMKI Registration Authority Manager	End of procedure
8.2.2.5	As soon as reasonably practicable following successful validation	Notify the Senior Responsible Officer that was contacted in step 7.2.2.3 to validate the revocation request and the DCC's CISO by phone that the revocation request has been accepted	SMKI Registration Authority Manager	8.2.2.6
8.2.2.6	As soon as reasonably practicable following 8.2.2.5	Revoke the identified Organisation Certificate that is the subject of the CRR	SMKI Registration Authority Manager	8.2.2.7
8.2.2.7	As soon as reasonably practicable following notification, or every hour (whichever is sooner)	Update the relevant Certificate Revocation List (CRL) and publish such CRL to the SMKI Repository, as set out in the SMKI Interface Design Specification and the Appendix B of the Code.	SMKI Registration Authority	8.2.2.8
8.2.2.8	Following revocation	Notify the SRO submitting the CRR of the successful revocation of the Organisation Certificate in the CRR, in writing	SMKI Registration Authority Manager	End of procedure

8.3 Revocation of SMKI Services and/or SMKI Repository Services access credentials

8.3.1 General obligations relating to revocation of ARO credentials for accessing SMKI Services and/or SMKI Repository Services and / or File Signing Certificates

A Senior Responsible Officer on behalf of a Party, RDP, the SMKI PMA or the DCC (in its role as DCC Service Provider) may request the revocation of access credentials in respect of an Authorised Responsible Officer acting on behalf of that Party, RDP, the SMKI PMA or the DCC (as DCC Service Provider), using the form as set out in **Error! Reference source not found.**and clearly identifying the credentials to be revoked.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

a) An applicant wishes the credentials of an ARO to be revoked.

b) A Party, RDP, SMKI PMA, SEC Panel or the DCC (as DCC Service Provider), of which the ARO is a representative, becomes ineligible to access SMKI Services and/or SMKI Repository Services or ceases to become an Authorised Subscriber for Device Certificates or Organisation Certificates, or both, as appropriate.

c) If there is a change to any of the information that was used to verify the identity of an ARO (but where the renewal or replacement of documents used to verify such identity, where the identity information remains the same, shall not constitute a change).

d) A Party, RDP, DCC (as DCC Service Provider), SEC Panel or the SMKI PMA notifies the SMKI Registration Authority that it reasonably believes that the ARO is a threat to the security, integrity, or stability of the SMKI Services and/or SMKI Repository Services.

e) The information on which the identity of an ARO was established is known, or is reasonably suspected, to be inaccurate.

f) The authentication credentials issued to the ARO are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to an ARO is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

Where access credentials have been revoked and the Party, RDP, SMKI PMA or DCC (as DCC Service Provider) wishes to receive new access credentials, that Party, RDP, SMKI PMA, SEC Panel or DCC (as DCC Service Provider) shall submit a new ARO Nomination Form.

8.3.2 Procedure for revocation of SMKI Services and/or SMKI Repository Services access credentials for AROs

The procedure for verification and, where verified, revocation of authentication credentials is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.2.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Appendix A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised by an SRO on behalf of the applicant organisation	SRO on behalf of the applicant organisation, which shall be a Party, SEC Panel, RDP, DCC (as DCC Service Provider) or member of the SMKI PMA	8.3.2.2
8.3.2.2	As required, following 8.3.2.1	Submit the completed Credential Revocation Request Form to the SMKI Registration Authority in writing or via a secured electronic means, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party, SEC Panel, RDP, DCC (as DCC Service Provider) or member of the SMKI PMA	8.3.2.3
8.3.2.3	As soon as reasonably practicable following 8.3.2.2	Acknowledge receipt by email to the SRO as identified on the Credential Revocation Request Form	SMKI Registration Authority	8.3.2.4
8.3.2.4	As soon as reasonably practicable following 8.3.2.3	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree actions with the SRO via email or in writing	SMKI Registration Authority	If complete, 8.3.2.6; if not complete, 8.3.2.5
8.3.2.5	Once omissions / discrepancies are addressed	Submit a revised Credential Revocation Request Form to the SMKI Registration Authority in writing or via a secured electronic means, as directed on the DCC Website	SRO on behalf of the applicant organisation, which shall be a Party, SEC Panel, RDP, DCC (as DCC Service Provider) or member of the SMKI PMA	8.3.2.6
8.3.2.6	As soon as reasonably practicable, following 8.3.2.4	Contact the SRO as identified on the Credential Revocation Request Form via telephone, using the registered contact information for the SRO as held by the SMKI Registration Authority, to confirm the application identified by the Credential Revocation Request Form is authorised	SMKI Registration Authority	If confirmed as authorised, 8.3.2.8; if not authorised, 8.3.2.7

Step	When	Obligation	Responsibility	Next Step
8.3.2.7	As soon as reasonably practicable following rejection	Notify the SRO that was contacted in step 7.3.2.3, that the procedure in respect of the application has not been successful, in writing	SMKI Registration Authority	End of procedure
8.3.2.8	As soon as reasonably practicable following 8.3.2.6	Notify the SRO that was contacted in step 7.3.2.3, and the DCC's CISO in writing that the revocation request has been accepted	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.9
8.3.2.9	As soon as reasonably practicable following 8.3.2.8	Revoke the credentials for the relevant service, for the identified ARO as indicated by the SRO on the Credential Revocation Request Form. In doing so, the DCC shall, where required to revoke the credentials, revoke all associated IKI Certificates. DCC shall ensure that access to the relevant service is prevented from the point of revocation.	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.10
8.3.2.10	As soon as reasonably practicable following 8.3.2.9	Notify the SRO that was contacted in step 7.3.2.3 of the successful revocation of credentials for the ARO. Where such revocation results in the individual that is the subject of the Credential Revocation Request no longer having any valid credentials issued to them in accordance with the SMKI RAPP, the SMKI Registration Authority shall notify the SRO that was contacted in step 7.3.2.3 that the individual is no longer an ARO, in writing	SMKI Registration Authority Personnel, on behalf of the SMKI Registration Authority	8.3.2.11
8.3.2.11	As soon as reasonably practicable following 8.3.2.10	Where the revoked credentials were issued on a Cryptographic Credential Token or Cryptographic Credential Tokens, the Party or DCC Service Provider shall, where such Cryptographic Credential Tokens are in the possession of the applicant organisation, send the Cryptographic Credential Token or Cryptographic Credential Tokens to the DCC, via secure courier	SRO on behalf of the applicant organisation	8.3.2.12
8.3.2.12	As soon as reasonably practicable following 8.3.2.11	The DCC shall verifiably destroy all Secret Key Material or Certificates contained on the returned Cryptographic Credential Token	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.2.13
8.3.2.13	As soon as reasonably practicable following 8.3.2.12	Record the details of the credentials that have been revoked in respect of the ARO as identified on the Credential Revocation Request Form, plus update the DCC's list of AROs, in a manner which is auditable	SMKI Registration Authority	End of procedure

8.3.3 General obligations relating to revocation of SMKI Registration Authority Manager or SMKI Registration Authority Personnel credentials for accessing SMKI Services and/or SMKI Repository Services

The following parties may request the revocation of authentication credentials in respect of SMKI Registration Authority Personnel, using the form as set out in **Error! Reference source not found.**:

a) Any SMKI PMA member, on behalf of the SMKI PMA; and

b) Any member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority.

The permitted reasons for revocation of authentication credentials shall be as listed immediately below:

a) A SMKI Registration Authority Manager wishes the credentials of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel to be revoked

b) A member of SMKI Registration Authority Personnel becomes ineligible to access SMKI Services and/or SMKI Repository Services.

c) A member of SMKI Registration Authority Personnel fails to comply with Appendix A and Appendix B of the Code, or this SMKI RAPP.

d) Any information used to verify the identity of a member of SMKI Registration Authority Personnel changes, the individual leaves the employment of the DCC, or moves within DCC to a role in which they are not entitled to access SMKI Services and/or SMKI Repository Services.

e) A SMKI Registration Authority Manager becomes aware that the member of SMKI Registration Authority Personnel or a SMKI Registration Authority Manager is a potential threat to the security, integrity, or stability of the SMKI Services and/or SMKI Repository Services.

f) The information on which the identity of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel was established is known, or is suspected, to be inaccurate.

g) The authentication credentials issued to the member of SMKI Registration Authority Personnel are lost, stolen, inoperative, or destroyed. The DCC shall ensure that the Cryptographic Credential Token issued to a member of SMKI Registration Authority Personnel is automatically rendered inoperative where the PIN code on the Cryptographic Credential Token used to access SMKI Services has been entered incorrectly 15 consecutive times.

8.3.4 Procedure for revocation of SMKI Services access credentials for SMKI Registration Authority Managers and SMKI Registration Authority Personnel

The procedure for verification and, where verified, revocation of credentials in respect of a SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel is as set out immediately below.

Step	When	Obligation	Responsibility	Next Step
8.3.4.1	As required	Complete the Credential Revocation Request Form as set out in SMKI RAPP Appendix A (A7), ensuring that the information entered on the form is complete and accurate, and the Credential Revocation Request Form is authorised: a) for a member of SMKI Registration Authority Personnel, by a SMKI Registration Authority Manager; or b) for a SMKI Registration Authority Manager, by the DCC's CISO.	SMKI Registration Authority Personnel or SMKI Registration Authority Manager	8.3.4.2
8.3.4.2	As required, following 8.3.4.1	Submit the completed Credential Revocation Request Form to a SMKI Registration Authority Manager, by hand in person	SMKI Registration Authority Personnel or SMKI Registration Authority Manager	8.3.4.3
8.3.4.3	As soon as reasonably practicable following 8.3.4.2	Analyse the information entered on the Credential Revocation Request Form; determine completeness and any discrepancies. Where there are omissions/discrepancies, agree amendments and adjust form contents	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.4
8.3.4.4	As soon as reasonably practicable following 8.3.4.3	Revoke the credentials of the identified SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel as indicated on the Credential Revocation Request Form	SMKI Registration Authority Manager, as directed by the DCC's CISO	8.3.4.5
8.3.4.5	As soon as reasonably practicable following 8.3.4.4	Where such revoked credentials were issued on a Cryptographic Credential Token, the DCC shall retrieve such Cryptographic Credential Token from the identified SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel and shall verifiably destroy all Secret Key Material or Certificates contained on the Cryptographic Credential Token	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	8.3.4.6
8.3.4.6	As soon as reasonably practicable following 8.3.4.5	Record the details of the credentials that have been revoked in respect of the member of SMKI Registration Authority Personnel or SMKI Registration Authority Manager as identified on the Credential Revocation Request Form	SMKI Registration Authority Manager, on behalf of the SMKI Registration Authority	End of procedure

Appendix A – Form Templates

The Form Templates listed in Appendix A are available from the DCC website at the following location:

https://www.smartdcc.co.u**k**/ [exact link suffix to be inserted prior to designation]

The DCC may, subject to the approval of the PMA, modify the Form templates from time to time.

A1. Organisation Information Form

A2. Authorised Subscriber / Interface Access Application Form

A3. SMKI SRO Nomination Form

A4. SMKI ARO Nomination Form

A5. Nominee Details Form

A6. Organisation Certificate Revocation Request Form

A7. Credential Revocation Request Form

Appendix B – Definitions

Term	Meaning as defined in SEC
Ad Hoc Device CSR Web Service Interface	The system-to-system interface provided to the SMKI for the purposes of SMKI Subscribers refreshing Device Certificates following a Device CSR for the respective Device being approved through a Batch or Ad Hoc CSR to the SMKI Portal
Authorised Responsible Officer (ARO)	Means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, RDP a DCC Service Provider, the SMKI PMA or the Panel in accordance with the SMKI RAPP
Batched Device CSR Web Service Interface	The system-to-system interface provided to the SMKI for the purposes of SMKI Subscribers refreshing Device Certificates following a Device CSR for the respective Device being approved following the submission of a Batched Certificate Signing Request
Cryptographic Credential Token	Means a FIPS 140-2 Level 3 token containing Secret Key Material, as issued in accordance with the SMKI RAPP
SMKI Registration Authority Manager	Means an individual who acts on behalf of the SMKI Registration Authority to perform tasks relating to the management of the SMKI Registration Authority, as set out in the SMKI RAPP
SMKI Registration Authority Personnel	Means those persons who are engaged by DCC, in so far as such persons carry out functions of the SMKI Registration Authority as set out in the SMKI RAPP
Senior Responsible Officer (SRO)	Means an individual that has successfully completed the process for becoming an SRO on behalf of a Party, RDP, a DCC Service Provider, the SMKI PMA or the Panel in accordance with the SMKI RAPP

APPENDIX E – DCC USER GATEWAY SERVICES SCHEDULE

[Intentionally Blank]

APPENDIX F – MINIMUM COMMUNICATION SERVICES FOR SMETS1 METERS

Ref	Description	Eligible Users
1.1	Update Import Tariff (prepayment)	Import Supplier, Gas Supplier
1.1	Update Import Tariff (credit)	Import Supplier, Gas Supplier
1.2	Update Price (prepayment)	Import Supplier, Gas Supplier
1.2	Update Price (credit)	Import Supplier, Gas Supplier
1.5	Update Balance	Import Supplier, Gas Supplier
1.6	Update Payment Mode	Import Supplier, Gas Supplier
2.1	Update Prepay Configuration	Import Supplier, Gas Supplier
2.2	Top Up Device	Import Supplier, Gas Supplier
2.3	Update Debt	Import Supplier, Gas Supplier

2.5	Activate Emergency Credit	Import Supplier, Gas Supplier
3.2	Restrict Access – CoT	Import Supplier, Gas Supplier
3.3	Clear Event Log	Import Supplier, Gas Supplier
4.1	Read Instantaneous Import Register Values	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter
4.2	Read Instantaneous Export Register Values	Export Supplier, Electricity Distributor
4.3	Read Instantaneous Prepayment Register Values	Import Supplier, Gas Supplier
4.4	Retrieve Billing Data Log	Import Supplier, Gas Supplier
4.8	Read Profile Data	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Other User
4.10	Read Network Data	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter

4.11	Read Tariff	Import Supplier, Gas Supplier, Other User
4.16	Read Active Power Import	Import Supplier, Electricity Distributor
6.2	Read Device Configuration	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User
6.4	Update Device Configuration (Load Limiting)	Import Supplier, Gas Supplier
6.5	Update Device Configuration (Voltage)	Electricity Distributor
6.6	Update Device Configuration (Gas Conversion)	Gas Supplier
6.7	Update Device Configuration (Gas Flow)	Gas Supplier
6.8	Update Device Configuration (Billing Calendar)	Import Supplier, Gas Supplier
6.11	Synchronise Clock	Import Supplier, Gas Supplier

6.12	Update Device Configuration (Instantaneous Power Threshold)	Import Supplier, Gas Supplier
6.13	Read Event or Security Log	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Registered Supplier Agent
6.15	Update Security Credentials	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter
6.23	Update Security Credentials (CoS)	Import Supplier, Gas Supplier
7.1	Enable Supply	Import Supplier
7.2	Disable Supply	Import Supplier, Gas Supplier
7.3	Arm Supply	Import Supplier, Gas Supplier
7.4	Read Supply Status	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent
11.1	Update Firmware	Import Supplier, Gas Supplier

11.2	Read Firmware Version	Import Supplier, Gas Supplier, Electricity Distributor, Gas Transporter, Export Supplier, Registered Supplier Agent, Other User

APPENDIX G - DCC GATEWAY CONNECTION CODE OF CONNECTION

Definitions

Connection Period	means the period for which a DCC Gateway Connection is to be provided, as determined in accordance with the provisions of clause 1.6 or pursuant to Section H15.18(c).
Contractual Bandwidth	means, in relation to any particular DCC Gateway HV Connection, the maximum number of megabits of data that are permitted to be transmitted each second over that connection.
Electronic Site Review	means a remote, desk-based assessment of the location at which the DCC Gateway Connection is required to assess whether a physical Site Survey is required.
Enabling Works	means any building or civil works, including laying of cables and gaining the necessary wayleaves or consents, required to be undertaken by a DCC Gateway Party and/or the DCC, to enable the DCC to provide a DCC Gateway Connection.
Maximum Physical Bandwidth	means 100 megabits per second (Mbps) or such increases as may be notified to DCC Gateway Parties by the DCC from time to time.
Site Survey	means a physical assessment of the location at which the DCC Gateway Connection is required, to assess whether any Enabling Works are required inside and/or outside the DCC Gateway Party's premises and to detail preparatory works to be carried out by the DCC Gateway Party to be reflected in the offer made pursuant to Section

H15.12.

1 DCC GATEWAY CONNECTIONS

1.1 Section H15 sets out principal rights and obligations applying to the provision of DCC Gateway Connections which are supplemented by the provisions set out below.

General Obligations

1.2 A DCC Gateway LV Connection will provide a download bandwidth of up to 40Mbps and an upload bandwidth of up to 10Mbps or such increases as may be notified to DCC Gateway Parties by the DCC from time to time.

1.3 A DCC Gateway HV Connection will provide a bandwidth of up to the Maximum Physical Bandwidth, which can be specified in increments of 10Mbps.

1.4 Each Party that wishes to establish a DCC Gateway Connection shall submit a request for a connection, using the application form for such requests as published on the DCC Website. Except in the case of a request made by a Registration Data Provider, such request shall specify the DCC Gateway Bandwidth Option and:

(a) in the case of a request for a DCC Gateway LV Connection, the Connection Period; or

(b) in the case of a request for a DCC Gateway HV Connection;

(i) the required Contractual Bandwidth in relation to that connection, provided that the Contractual Bandwidth for any connection shall be an integer multiple of 10Mbps, and shall not exceed the Maximum Physical Bandwidth;

(ii) and the Connection Period.

1.5 Following a request for a connection being submitted, the DCC and the Party that submitted the request shall inform each other of the contact details of one or more persons working for their respective organisations for the purposes of communications associated with the establishment and management of DCC Gateway Connection(s). The following information shall be provided in relation to each such person (and shall subsequently be kept up to date by the providing Party):

(a) contact name;

(b) contact email;

(c) contact telephone;

(d) contact role(s);

(e) contact address;

and any other contact details as may be reasonably required by the DCC or the other Party from time to time.

Connection Mechanisms and Period of Connection

1.6 Where a DCC Gateway Party wishes to procure a DCC Gateway Connection:

(a) the connection may be requested for an initial period of either one or three years from the point at which the connection becomes capable of operation provided that, in the case of a connection requested by a Registration Data Provider, the period of connection will not be requested but will be provided in accordance with Section E 3.5(b); and

(b) the DCC shall notify the DCC Gateway Party when the connection becomes capable of operation.

1.7 The Electronic Site Review and Site Survey constitute (respectively) the desk-based assessment and physical site assessment referred to in Section H15. Where a DCC Gateway Party requests multiple DCC Gateway Connections for a single location at the same time, the DCC shall ~~use all reasonable endeavours~~take all reasonable steps to conduct any Site Surveys in a single visit to that location.

1.8 Where any Enabling Works are required, the DCC Gateway Party and the DCC shall inform each other of the progress and completion of the Enabling Works.

1.9 In the event that a DCC Gateway Party wishes to decrease the Contractual Bandwidth of its DCC Gateway HV Connection during its Connection Period:

(a) the DCC Gateway Party shall inform the DCC, provided that the requested decrease shall be an integer multiple of 10Mbps;

(b) the DCC shall reduce the Contractual Bandwidth accordingly as soon as is reasonably practicable and in any event within 30 days of being informed of the required adjustment; and

(c) the DCC shall provide the DCC Gateway Party with advance notice of the date from which the adjusted Contractual Bandwidth shall take effect.

1.10 In the event that a DCC Gateway Party wishes to increase the Contractual Bandwidth of its DCC Gateway HV Connection during its Connection Period:

(a) the DCC Gateway Party shall inform the DCC, provided that the requested increase shall be an integer multiple of 10Mbps, and shall not exceed the Maximum Physical Bandwidth of that connection;

(b) the DCC shall confirm to the DCC Gateway Party the applicable charges arising from the increase as soon as reasonably practicable and in any event within 5 Working Days;

(c) following notification of the applicable charges, the DCC Gateway Party shall, within 30 days, confirm to the DCC that the DCC Gateway Party wishes to proceed with the increase (and where no such confirmation is provided within 30 days, the DCC's offer to increase the bandwidth at the notified applicable charge shall lapse);

(d) where the DCC receives confirmation from the DCC Gateway Party within 30 days that it wishes to proceed with the increase, the DCC shall increase the Contractual Bandwidth accordingly as soon as is reasonably practicable and in any event within 30 days of receiving such confirmation; and

(e) the DCC shall provide the DCC Gateway Party with advance notice of the date from which the adjusted Contractual Bandwidth shall take effect.

Installation, Maintenance and Removal of DCC Gateway Equipment

1.11 Sections H15.20 to H15.28 set out principal rights and obligations relating to DCC Gateway Equipment which are supplemented with the provisions set out below.

1.12 Where the DCC is undertaking works at the DCC Gateway Party's premises for the purposes of installation, maintenance or removal of DCC Gateway Equipment, the DCC shall take all reasonable steps to avoid interrupting the DCC Gateway Party's existing telecommunications services at those premises. In the event that it is necessary to interrupt the DCC Gateway Party's existing telecommunications services:

(a) the DCC shall take all reasonable steps to provide the DCC Gateway Party with advance notice of the interruption; and

(b) the DCC Gateway Party shall have the right to request that such interruption be rescheduled, acceptance of such request not to be unreasonably withheld or delayed by the DCC.

1.13 Where the DCC Gateway Party's existing telecommunications services are interrupted as a result of DCC undertaking works as set out in clause 1.12, the DCC shall:

(a) take all reasonable steps to minimise the length and impact of the interruption; and

(b) ensure that the telecommunications services are restored as soon as is reasonably practicable and in any event immediately following the completion of the works.

1.14 Where maintenance undertaken by the DCC requires the replacement of DCC Gateway Equipment, the DCC shall remove that equipment within 30 days of the date of the replacement activity.

1.15 In the event that, pursuant to Section H15.28 or the provisions of clause 1.14, DCC Gateway Equipment is not removed within 30 days, the DCC Gateway Party may dispose of the equipment and shall notify the DCC at least 5 days prior to disposing of the DCC Gateway Equipment, provided that the DCC shall have the right to remove the equipment prior to the end of that 5 day period.

1.16 Subject to the obligations in Sections H15.20, H15.21, and H15.28(b) for the DCC to act in accordance with Good Industry Practice, the DCC shall not be responsible for or liable to the DCC Gateway Party for making good any minor repairs to decoration that have become necessary as a result of the DCC's installation, maintenance or removal of DCC Gateway Equipment.

1.17 Each DCC Gateway Party shall make available to the DCC all information, facilities and services reasonably required by the DCC to carry out installation, maintenance or removal of DCC Gateway Equipment.

1.18 Where reasonably requested by a DCC Gateway Party, the DCC shall provide such information as required by the DCC Gateway Party in order to facilitate the

installation, maintenance or removal of DCC Gateway Equipment. Following receipt of that information, the DCC Gateway Party shall have the right to reschedule the visit by the DCC. The DCC Gateway Party acknowledges that rescheduling of the visit required for installation may give rise to the DCC notifying a revised connection date pursuant to Section H15.15 and that rescheduling the visit for maintenance or removal may give rise to corresponding delays for the completion of that maintenance or removal.

1.19 Subject to Section H15.24, and except where such steps are necessary on security or safety grounds, each DCC Gateway Party shall not take any steps that may affect the operation of the DCC Gateway Connection without prior agreement of the DCC, such agreement not to be unreasonably withheld or delayed, and shall ensure that no person other than the DCC undertakes any maintenance of the DCC Gateway Equipment.

1.20 The DCC Gateway Party shall implement and maintain controls to ensure the physical security of the DCC Gateway Equipment, including that only appropriately authorised persons have access to such equipment, and that this access is recorded in a log maintained for that purpose.

1.21 The DCC shall ~~use its reasonable endeavours~~take reasonable steps to comply with any DCC Gateway Party's reasonable requests in respect of installation or relocation of DCC Gateway Equipment. The DCC Gateway Party shall be entitled to make the final decision on the routing of cables and location of the DCC Gateway Equipment, subject to such decision not impacting on the DCC's ability to provide and maintain the DCC Gateway Connection.

1.22 The DCC may modify or replace the DCC Gateway Equipment where necessary to maintain the operation of the DCC Gateway Connection, provided that such modification or replacement does not materially diminish the performance of the DCC Gateway Connection, and only after giving reasonable notice of the need to modify or replace the DCC Gateway Equipment to the DCC Gateway Party.

1.23 The DCC shall wherever possible carry out maintenance of the DCC Gateway Equipment installed at a DCC Gateway Party's site remotely, using the network connection itself to gain access to the DCC Gateway Equipment:

(a) where reasonably practicable, the DCC shall provide reasonable advance notice to the DCC Gateway Party of such maintenance;

(b) such advance notice shall be provided to a contact nominated to the DCC for that purpose by the DCC Gateway Party, or otherwise the contact provided pursuant to clause 1.5; and

(c) the DCC Gateway Party shall have the right to request that the maintenance is rescheduled, acceptance of such request not to be unreasonably withheld or delayed by the DCC.

1.24 The DCC and each DCC Gateway Party shall provide sufficient information to each other to enable the establishment and maintenance of the network layer connectivity across the DCC Gateway Connection.

1.25 The DCC shall give the DCC Gateway Party reasonable notice of required site visits to perform installation, maintenance or removal of DCC Gateway Equipment and the DCC shall accommodate the DCC Gateway Party's reasonable requests regarding the timing of such visits.

Reporting Obligations

Left intentionally blank.

APPENDIX H – CH HANDOVER SUPPORT MATERIALS

Definitions

Advanced Shipment Notification (or ASN)	means, in relation to a Region, the notification containing the information listed in Annex A of this document under 'Advanced Shipment Notification' identified as being provided in relation to that Region.
Central Region	means the Region which covers the majority of Wales and the majority of central England.
CH Delivery and Returns	means the OMS Account profile which enables the user of an OMS Account with this profile or the DCC on their behalf to carry out the following activities on the OMS: (a) the viewing and amendment of Communication Hub Consignments; (b) the viewing and downloading of Advanced Shipment Notifications; (c) the creation, acceptance and rejection of requests to return Communications Hubs and Communications Hub Auxiliary Equipment to the DCC; and (d) the maintenance of Delivery Location information and Party contact details in relation to Communications Hub Orders.
CH Ordering	means the OMS Account profile which enables the user of an OMS Account with this profile or the DCC on their behalf to carry out the following activities on the OMS: (a) the creation, submission, viewing, and amendment of Communications Hub Forecasts, Communications Hub Orders; (b) the creation of Delivery Location information; and (c) all activities that can be carried out under an OMS Account with the CH Delivery and Returns profile.
CH Supporting Information	means the materials identified as such which: (a) are published by the DCC on the DCC Website; and (b) contain the information required by clause 1.4 of this document.

CH Query	means the OMS Account profile which enables the user of an OMS Account with this profile or the DCC on their behalf to carry out the following activities on the OMS: (a) the viewing of Communication Hub Consignments, Communications Hub Forecasts, Communications Hub Orders; and (b) the viewing and downloading of Advanced Shipment Notifications.
CHF Identifier	has the meaning given to that term in the CHTS.
Coverage Area	means the geographical coverage of the SM WAN at a point in time.
Delivery Issues Report Notification (or DIRN)	means the report provided to a Party by the DCC pursuant to clause 6.23.
Delivery Note	means, in relation to a Region, the documentation containing the information listed in Annex A under 'Delivery Note' identified as being provided in relation to that Region.
GPF Identifier	has the meaning given to that term in the CHTS.
Installation Location	means a the location of the premises at which a Communications Hub is planned to be, or has been, installed.
Mesh Communications Hub	means a WAN Variant in the Central Region and the South Region which is capable of using both mobile cellular radio technology and wireless mesh radio technology to connect to the SM WAN.
North Region	means the Region which covers the majority of Scotland and the majority of northern England.
OMS Account	means an arrangement by which a user is given access to an OMS profile by entering a unique username and password.
OMS Order Reference	means a reference that is unique to a Communications Hub Order and which is first notified as set out in clause 3.19.
Order Management System (or OMS)	means the systems comprising part of the CH Ordering System and which are used for: (a) the submission of information comprising Communications Hub Forecasts and Communications Hub Orders; (b) the management and tracking of Communications Hub Orders and deliveries of Communications Hubs and Communications

	Hub Auxiliary Equipment; and (c) the rejection, return or replacement of Communications Hubs and Communications Hub Auxiliary Equipment; (d) the provision of contact details by DCC and each other Party in respect of the matters in (a), (b) and (c) above (where required).
Significant Metallic Obstruction	has the meaning given to that term in the CH Installation and Maintenance Support Materials.
South Region	means the Region which covers the majority of southern England.
Working Hours	for the purposes of this document, means the period between 07:00 and 17:00 during a Working Day.

1 INTRODUCTION

Document purpose

1.1 This document is the CH Handover Support Materials, and forms Appendix [xxx] of the Code.

General clarifications

1.2 Unless expressly stated otherwise, the obligations in this document are applicable in relation to all Regions.

1.3 Unless expressly stated otherwise, none of the obligations in this document apply to Test Communications Hubs.

1.4 The DCC shall publish the CH Supporting Information on the DCC website, which shall include the following information:

(a) information regarding Communications Hub packaging and labelling;

(b) additional diagrammatical information supporting the definition of Significant Metallic Obstruction; and

(c) a description of the way in which LED indicators depict the operational status of a Communications Hub.

1.5 Prior to first publication of, and any subsequent modification to the CH Supporting Information the DCC shall:

(a) undertake reasonable consultation with Parties regarding its content or any proposed modification thereto;

(b) give due consideration to, and take into account, any consultation responses received; and

(c) publish a statement of its reasons for including or modifying content, as applicable, together with copies of any consultation responses received that are not marked as confidential.

1.6 The DCC shall publish the initial CH Supporting Information and any subsequently modified versions on the DCC Website as soon as reasonably practicable following the completion of the activities set out in clause 1.5.

2 ORDER MANAGEMENT SYSTEM

2.1 Subject to the remaining provisions set out in this clauses 2.1 to 2.7 of this document, the DCC shall provide each Party with access to the Order Management System (OMS) for each Region via:

(a) the Self-Service Interface; and

(b) a public internet link.

Access to the OMS

2.2 A Party other than the DCC shall only access the OMS via an OMS Account.

2.3 Any Party first seeking to access the OMS for a Region shall submit a valid request for one or more OMS Accounts via the Service Desk.

2.4 Each Party may request access for OMS Accounts in relation to each Region. DCC shall provide four OMS Accounts per Region at no additional Charge. A Party may request more than four OMS Accounts per Region, subject to Section F5.23.

2.5 A request for an OMS Account shall be considered valid if it includes:

(a) the Party Signifier for the Party making the request;

(b) a username comprised of an email address for each OMS Account being requested, which shall not be used for any other accounts accessing the OMS for that Region;

(c) the OMS profile(s) to be associated with each OMS Account being requested; and

(d) the Region for which access is being requested.

2.6 The DCC shall provide a password to be associated with each individual OMS Account to the requesting Party no later than four Working Days following the receipt of a valid request for an OMS Account. The requesting Party may then use the combination of username and password to access the relevant instance of the OMS.

2.7 A Party may request a change to the OMS profile(s) that are available via an OMS Account, modify the OMS Account or close the OMS Account by submitting a request to the Service Desk. The DCC shall implement such a change no later than four Working Days following the receipt of such a request and shall notify the Party on the day of completion.

3 FORECASTING AND ORDERING COMMUNICATIONS HUBS

Communications Hub Forecasts

3.1 Following receipt of a Communications Hub Forecast or the deeming of a Communications Hub Forecast by the DCC in accordance with Section F5.6, the DCC shall notify via email to all OMS Accounts associated with that Party that the following information is available via the OMS:

(a) a unique reference for the relevant Communications Hub Forecast; and

(b) the associated date, which shall be:

(i) where a Communication Hub Forecast has been submitted by a Party, the date of submission; or

(ii) where the Communications Hub forecast has not been submitted by a Party, the date at which the DCC has deemed that forecast.

SM WAN coverage information

3.2 The DCC shall provide Parties with information regarding SM WAN coverage at potential Installation Locations and the WAN Variant (and, where applicable, the Communications Hub Auxiliary Equipment) required for each Installation Location via the SM WAN Coverage Database. The DCC shall make the SM WAN Coverage Database information available via:

(a) the Self Service Interface;

(b) responses to Service Request 12.1 (Request WAN matrix); or

(c) a reasonable alternative method, as specified by the DCC, where the methods specified in clauses 3.2(a), 3.2(b) are not available.

3.3 Where a Party requires SM WAN coverage information for an Installation Location where there is no associated postcode, the Party may raise an Incident with the DCC and in so doing shall provide the geographic latitude and longitude, for the Installation Location as part of the initial diagnosis information required by the Incident Management Policy. The DCC shall resolve the Incident by providing SM WAN coverage information for the Installation Location and shall additionally allocate the Installation Location to a Region.

Delivery Locations

3.4 A Party shall provide Delivery Locations on the OMS using the CH Ordering profile and shall provide and maintain the following information for each Delivery Location:

(a) the full delivery address;

(b) operating hours; and

(c) the name, email address, and telephone number for a nominated contact in relation to Communications Hubs Orders.

3.5 The DCC shall ensure that the OMS allows each Party using the CH Ordering profile to select a maximum of two Delivery Locations for each Communications Hub Order.

Deemed Communications Hub Orders

3.6 Where, in accordance with Section F5.13(c), the DCC deems the quantities of Communications Hubs to be included in a Communications Hub Order for a Party, it shall inform via email notification to all OMS Accounts associated with that Party that a deemed order has been made and make available, via the OMS, details of the deemed quantity of each Device Model and of any Communications Hub Auxiliary Equipment.

3.7 Where a Party receives a notification in accordance with clause 3.6, that Party shall specify a Delivery Location or Delivery Locations for the Communications Hub Order within two Working Days and shall comply with, and provide the further information set out in, clauses 3.13 and 3.14.

3.8 Where a Party has not specified a Delivery Location or Delivery Locations, or provided the other information required, in accordance with clause 3.7, the DCC shall specify the Communications Hub Order Delivery Location or Delivery Locations using Delivery Locations provided for any previous orders and, specify the further information set out in, clauses 3.13 and 3.14.

3.9 Where the DCC has determined the Delivery Location(s) pursuant to clause 3.8 and the relevant Party has not notified the DCC within 30 days of the DCC's notification pursuant to clause 3.6, that the extant delivery details are correct, then the relevant Party shall be deemed to have requested cancellation of the Consignment or Consignments (and Section F5.19 shall be deemed to apply). The DCC shall notify that such a request has been deemed, via an email to all OMS Accounts associated with that Party.

Submitting Communications Hub Orders

3.10 When submitting a Communications Hub Order, each Party shall ensure that only such WAN Variants and Communications Hub Auxiliary Equipment are ordered as it may reasonably require to:

(a) complete planned installations using the WAN Variants and Communication Hub Auxiliary Equipment that are indicated as required for the relevant Installation Location(s) on the SM WAN Coverage Database; and

(b) maintain sufficient stock to resolve coverage Incidents and Communication Hub faults as described in the CH Installation and Maintenance Support Materials.

3.11 Where a Party submits a Communications Hub Order for the Central Region or the South Region that results in greater than 7% of the total number of Communications Hubs in the Communications Hub Order being Mesh Communications Hubs, the DCC may request an explanation why the quantity of Mesh Communications Hubs ordered is required and where such an explanation is requested the Party shall provide the explanation via email promptly.

3.12 Each Party shall ensure that its Communications Hubs Order is such that it would not result in a requirement for the DCC to deliver a single Consignment that comprises only Communications Hub Auxiliary Equipment.

3.13 In addition to complying with the requirements set out in Section F5.8, for each Communications Hub Order that it submits, a Party shall:

(a) request delivery to no more than two Delivery Locations per Region;

(b) request delivery to each Delivery Location no more than once in any single week; and

(c) specify a Delivery Date and associated Delivery Window that is within Working Hours.

3.14 A Party submitting a Communications Hub Order shall ensure that for each delivery that will result from that Communications Hub Order and in relation to the Region to which the Order relates:

(a) the number of each WAN Variant is an integer multiple of the quantity of Communications Hubs that are contained in a carton, as specified in Annex B of this document;

(b) the total number of Communications Hubs ordered is such that a pallet layer contains the total number of cartons for that pallet layer as specified in Annex B of this document; and

(c) the total number of Communications Hubs is greater than or equal to the quantity of Communications Hubs contained in a complete standard pallet, as specified in Annex B of this document.

3.15 The DCC shall package and load Communications Hubs as described in Annex D of this document.

3.16 The DCC shall make available to a Party using the CH Ordering profile at least one contact telephone number and email address for the DCC which is relevant to each Communications Hub Order placed by that Party for the purposes of allowing a Party to request amendments to Delivery Locations, Delivery Dates, or Delivery Windows in relation to a Communications Hub Order that it has submitted.

3.17 A Party shall make available to the DCC via the OMS using the CH Ordering profile at least one contact telephone number and email address for that Party which is relevant to each of its Communications Hub Orders, which shall be used by the DCC for any email or telephone communications regarding the order.

3.18 For each Communications Hub Order, where the DCC identifies an opportunity for consolidation of a Party's Consignments into a single delivery vehicle, the DCC may request permission to amend a Communications Hub Order to enable such consolidation. The agreement of the Party to such a request shall not be unreasonably withheld.

Order Verification and Acceptance

3.19 The notification that the DCC is required to provide pursuant to Section F5.16 shall be provided by the DCC via email to all OMS Accounts associated with that Party notifying that information is available via the OMS. Such information will consist of the following;

(a) an OMS Order Reference; and

(b) confirmation that the Communications Hub Order is:

(i) compliant with the requirements of Section F5 (and therefore accepted without amendment); or

(ii) not compliant with the requirements of Section F5.

3.20 Where a notification has been made of the type set out in clause 3.19(b)(ii), the further notification that DCC is required to provide pursuant to Section F5.17 shall be provided by the DCC via email to all OMS Accounts associated with that Party notifying that information is available via the OMS. The information on the OMS shall state whether the Order is:

(a) accepted, in full and is not subject to amendment;

(b) accepted, in part or is subject to amendment; or

(c) rejected; and in each case

(d) the reason for the decision.

3.21 In the event that a Party submits a Communications Hub Order, or subsequently seeks to amend that order pursuant to clause 4.3, that would result in one or more deliveries that do not meet the conditions set out in clause 3.13 and 3.14, such an order shall be deemed to be a request for non-standard delivery instructions in accordance with Section F6.17.

3.22 Where a Party has or has been deemed to have requested non-standard delivery instructions, the DCC shall provide a non-binding estimate of any applicable Charge for that Communications Hub Order to that Party within five Working Days of receipt of such request.

3.23 On receipt of an estimate of the applicable non-standard delivery Charge pursuant to clause 3.22, the relevant Party shall, within five Working Days, either;

(a) leave the non-standard delivery order unchanged on the OMS, and therefore be deemed to have agreed to pay any applicable Explicit Charges pursuant to Sections F6.17 and K7.5(k); or

(b) amend the relevant Communications Hub Order via the OMS using the CH Ordering profile such that it no longer results in non-standard delivery instructions.

4 ORDER MANAGEMENT

Non-standard cancellation of Consignments

4.1 Pursuant to Section F5.19, a Party wishing to obtain an estimate of costs and expenses in relation to the cancellation of a Consignment shall submit a request for this estimate by contacting the Service Desk.

4.2 Where pursuant to Section F5.19 a Party wishes to cancel a Consignment, its notification to this effect must be provided to the Service Desk.

Delivery Date and Time Amendments

4.3 Following acceptance of a Communications Hub Order by the DCC, a Party may request amendments to the Delivery Date or Delivery Window for a Consignment up to 30 days prior to the original Delivery Date. Such requests shall be submitted via the OMS through a direct update to the order details using the CH Ordering profile.

4.4 Any request by a Party for an amendment pursuant to clause 4.3, in addition to the provisions in clauses 3.13 and 3.14, is subject to the following restrictions:

(a) the revised Delivery Date for a Consignment must be a Working Day within five days of the original Delivery Date and within the same Delivery Month; and

(b) the revised Delivery Window for a Consignment must be within Working Hours.

4.5 In the event that a Party wishes to request an amendment to the Delivery Date or Delivery Window for a Consignment within 30 days of the Delivery Date, or where the Party wishes to request an amendment to the Delivery Location because exceptional circumstances mean that delivery to the original specified Delivery Location is no longer practicable, that Party shall contact the DCC directly using the contact details set out in clause 3.16; in this event the restrictions as detailed in clause 4.4 shall apply and DCC may specify further reasonable restrictions which shall be notified via telephone or email and may deem such a request to be a request for non-standard delivery instructions.

4.6 Where the DCC deems such a request to be a request for non-standard delivery instructions, clause 3.22 shall apply. Upon receipt of an estimate of the applicable non-standard delivery Charge, the relevant Party shall, within five Working Days, either;

(a) leave the non-standard delivery order unchanged on the OMS, in which case, the Party shall be deemed to have withdrawn its request for an amendment pursuant to 4.5; or

(b) notify the DCC of its agreement to pay any applicable Explicit Charges pursuant to Sections F6.17 and K7.5(k) and the DCC shall update the OMS accordingly.

4.7 The DCC may consider an amendment to the Delivery Date or Delivery Window for a Consignment made within five Working Days of the Delivery Date, but shall not be obliged to do so.

4.8 Where the DCC has not deemed a request pursuant to clause 4.5 to be a request for non-standard delivery instructions, the DCC shall confirm acceptance of any request made by a Party in accordance with clause 4.5 and the DCC shall update the OMS to reflect the amendments agreed with the Party, as soon as is reasonably practical and in any event within five Working Days of the request having been made.

4.9 Where pursuant to clause 4.8 the DCC confirms to a Party that a change to the Delivery Date or Delivery Window, or Delivery Location is accepted; the DCC shall be obliged to deliver the Communications Hub Order in accordance with those updated instructions.

Monitoring Order Status

4.10 The DCC shall ensure that the following information is available to a Party via the OMS for all OMS Accounts associated with that Party in relation to each Communications Hub Order that it submitted in the previous 12 months:

(a) The Communications Hub Order status, being one of:

(i) Submitted – order submitted to the DCC;

(ii) Accepted – order (where appropriate, as amended) accepted by the DCC;

(iii) Rejected – full order rejected by DCC;

(iv) Partially Delivered – partial order delivered and accepted by the Party; or

(v) Delivered – all Consignments for the order accepted by the Party.

(b) the status of each Consignment within a Communications Hub Order, being one of:

(i) In Progress – Consignment scheduled for delivery within 30 days or less;

(ii) Shipped - Advance Shipment Notification (ASN) issued and Consignment in transit;

(iii) Delivered – Consignment delivered to Delivery Location;

(iv) Rejected – the Party has rejected all of the Consignment;

(v) Partially Delivered – partial Consignment acceptance by the Party;

(vi) Accepted – the Party has accepted delivery of all Communications Hubs in the Consignment; or

(vii) Cancelled – The Party has cancelled delivery of the Consignment.

5 DELIVERY DOCUMENTATION AND PACKAGING

Pre-handover delivery documentation

5.1 At least two Working Days prior to the Delivery Date for a Consignment, the DCC shall:

(a) notify the relevant Party via email that an ASN for that Consignment is available via the OMS; and

(b) ensure that the ASN is available for that Party to download from the OMS under all OMS Accounts associated with that Party in a Comma Separated Values (CSV) file format. The DCC shall ensure that the content of this CSV file is such that:

(i) the first row contains the column headings for each data item;

(ii) the first column in each subsequent row contains the unique CHF Identifier for a Communications Hub, with all other data items in that row being associated to that CHF Identifier;

(iii) the column headings contain the information listed under the header Advanced Shipment Notification in Annex A of this document for the relevant Region;

(iv) fields shall be comma-separated;

(v) fields shall only contain ASCII characters;

(vi) text fields shall be enclosed with opening and closing double quotation marks, but no quotation marks shall be used in date and numeric fields;

(vii) a (double) quote character within a text field must be represented by two (double) quote characters;

(viii) blank fields shall not contain characters other than opening and closing double quotation marks for text fields; and

(ix) records shall be terminated with a line feed (ASCII 10) character.

Delivery documentation and labelling

5.2 The DCC shall ensure that in relation to each Consignment, each carton and pallet will be labelled with identification information as listed under the columns titled “Carton Labels” and “Pallet Labels” in Annex A of this document.

5.3 The DCC shall ensure that a hard copy of the Delivery Note is provided to the Party on the arrival of the Consignment at the Delivery Location.

Communications Hub packaging and labelling information

5.4 The DCC shall permanently mark the identification information listed under the header CH Marking in Annex A of this document onto the front face of each Communications Hub, where that front face is the face of the Communications Hub which contains the M4 retaining screw.

Carton Packaging

5.5 The DCC shall provide packaged Communications Hubs in cardboard boxes within cartons, each carton containing the quantities of Communications Hubs for the relevant Region as set out in Annex B of this document.

5.6 The DCC shall provide cartons that contain only a single WAN Variant.

Pallet Sizes

5.7 The DCC shall ensure that:

(a) cartons are loaded onto pallets of the relevant dimensions for a Region as set out in Annex B of this document;

(b) pallets are wrapped such that cartons are safely secured for transit, and that pallet and carton labelling is visible through the wrapping materials; and

(c) pallets are packed so as not to exceed the maximum specifications as set out in Annex B of this document.

6 HANDOVER PROCEDURE

Pre-delivery Checks

6.1 The DCC shall ensure that, prior to making the ASN for a Consignment available to a Party in accordance with clause 5.1(b), such ASN correctly identifies the total quantity of Communications Hub Device Models requested in that Consignment.

6.2 Each Party (other than the DCC) shall validate the content of an ASN provided to it against the relevant Consignment details derived from its submitted Communications Hub Order to check that the ASN correctly identifies the total quantity of Communications Hub Device Models requested in that Consignment by that Party.

6.3 Where a Party identifies that the ASN is incorrect, it shall notify the DCC using contact details provided in accordance with clause 3.16. The Party shall ensure that this notification is sent to the DCC at least 5 Working Hours before the Delivery Window for that Consignment.

6.4 Where the DCC receives a notification in accordance with clause 6.3, and where DCC agrees that the ASN does not reflect the Consignment, the DCC shall amend the ASN to

correctly reflect the requested Consignment promptly and may propose amendments to the Delivery Date. The DCC shall notify the Party via email and via telephone of the steps that it has taken.

Delivery Changes

6.5 Where, prior to the Delivery Date, the DCC becomes aware that it will be unable to deliver the Consignment on the specified Delivery Date, it shall notify the affected Party of the delay and explain the reasons for the delay as soon as reasonably practicable via email and telephone and shall propose amendments to the Delivery Date.

6.6 Where DCC seeks to change a Delivery Date and Delivery Window in accordance with clause 6.4 or 6.5 the DCC shall list reasonable potential options for revised Delivery Dates and Delivery Windows and request a revised Delivery Date and Delivery Window from the affected Party.

6.7 Where a Party is notified in accordance with clause 6.6, the Party shall indicate which one of the potential Delivery Dates and Delivery Windows it prefers, and the DCC shall update the OMS with the Party's preferred rescheduled Delivery Date and Delivery Window for the affected Consignment.

6.8 Where, on or prior to the Delivery Date, the DCC considers that the Consignment will be delivered outside of the Delivery Window, the DCC shall notify the Party as soon as reasonably practicable via notification email and telephone. The DCC shall explain the reason for the delay and provide an estimate for a revised delivery time.

6.9 Where the Party is not able to accept the Consignment at the revised delivery time proposed pursuant to clause 6.8, the DCC shall provide a list of reasonable potential options for revised Delivery Dates and Delivery Windows and request a revised Delivery Date and Delivery Window from the Party. The Party shall indicate which one of the potential Delivery Dates and Delivery Windows offered by the DCC it prefers, and the DCC shall update the OMS accordingly.

Unloading

6.10 On the Delivery Date the Party shall:

(a) ensure that there is access for the DCC to the Delivery Location during the Delivery Window; and

(b) provide a dry receiving area large enough to receive all the pallets in the Consignment.

6.11 When the Consignment arrives at a Party's Delivery Location that Party shall:

(a) check the Delivery Note information to confirm that the Consignment matches the relevant ASN prior to unloading;

(b) protect the Consignment from moisture and extremes of temperature during unloading in accordance with the environmental conditions set out in Annex C of this document, and as amended from time to time;

(c) except where not required to do so pursuant to clause 6.12, unload pallets from the delivery vehicle; and

(d) unload the vehicle within two hours of the later of:

(i) the agreed Delivery Window: or

(ii) the delayed delivery arrival time where the delivery is delayed.

6.12 A Party:

(a) shall not unload pallets that are not identified on the ASN;

(b) may decline to unload pallets where pursuant to clause 6.18 they are going to reject a complete pallet; and

(c) may decline to unload pallets where to do so would present a health and safety risk.

6.13 Any pallets that are not unloaded for the reasons set out in clause 6.12 of this document shall be deemed to be rejected by the relevant Party, and that Party shall provide a notification to the DCC in accordance with clause 6.20 of this document.

Consignment Reconciliation

6.14 Following unloading, and without removing any packaging or breaking any security seals on the delivered pallets or Communications Hubs, the Party shall take reasonable steps~~use reasonable endeavours~~ to:

(a) scan or visually inspect the label on each unloaded pallet, and confirm that the

(i) pallet identifier;

(ii) OMS Order Reference;

(iii) Consignment reference; and

(iv) any carton identifiers that are visible, match those shown on the ASN; and

(b) verify that the quantity of cartons on each pallet matches the quantity shown on the ASN.

6.15 The Party shall sign the Delivery Note to confirm completion of delivery prior to the delivery vehicle departing the Delivery Location.

6.16 If the Party is aware of any discrepancies that exist between the pallets or cartons of Communications Hubs unloaded and the information contained within the ASN or the Delivery Note, the Party shall note this on the Delivery Note prior to signing it.

6.17 The DCC shall ensure that the Party is provided with a hard copy of the signed Delivery Note as proof of delivery prior to the delivery vehicle leaving the Delivery Location.

Visual Inspection

6.18 In addition to the right to reject pursuant to Section F6.9 (a) to (c), a Party shall reject a complete pallet where any of the following is identified:

(a) heat or smoke damage to the external wrapping or packaging;

(b) evidence of tampering or interference with any packaging tamper seals; or

(c) damage, which is estimated to affect more than 50% of the cartons on that pallet as a result of:

(i) fork lift truck/handling damage or outer-wrapping damage where there are notable signs of packaging or product damage such as crushing, puncturing or scraping;

(ii) water ingress, or other liquid or chemical damage; or

(iii) signs of infestation by pests or mould.

6.19 Pursuant to Section F6.9 (d), a Party receiving a Consignment may reject individual damaged cartons where it has not rejected the whole pallet as set out in clause 6.18.

Delivery Confirmation Procedure

6.20 Pursuant to Section F6.7, a Party shall provide confirmation of whether or not a delivery of Communications Hubs Products has been made in compliance with the order by notifying the DCC via the OMS using either the CH Ordering or the CH Delivery and Returns profile. Such notification shall include details of any pallets or where applicable, individual cartons of Communications Hubs that are rejected, and provide the following:

(a) OMS Order Reference;

(b) Consignment reference;

(c) where a complete pallet is rejected:

(i) the pallet identifier;

(ii) quantity of cartons on the pallet; and

(iii) a description of the reason for rejection as listed in clause 6.21; and

(d) where a carton is rejected that is not part of a complete pallet:

(i) carton identifier; and

(ii) a description of the reason for rejection as listed in clause 6.21.

6.21 For the purposes of the notification under clause 6.20, the reason for rejection of all or part of a Consignment is one of those listed in Section F6.9 (a) to (c), or one of the following:

(a) pallet not unloaded for the reasons set out in clause 6.12;

(b) pallet rejected in accordance with clause 6.13;

(c) missing pallet from the Consignment as unloaded;

(d) pallet not identified within the Party's ASN for that Consignment;

(e) pallet rejected in accordance with clause 6.18;

(f) carton missing from the Consignment as unloaded;

(g) carton not identified within the Party's ASN for that Consignment; or

(h) carton rejected in accordance with clause 6.19.

6.22 A Party may only reject whole cartons of Communications Hubs.

Rejected Delivery Return Procedure

6.23 Following the receipt of a notification via the OMS in accordance with clause 6.20 of this document, the DCC shall notify the Party via an email to all OMS Accounts associated with that Party, that a Delivery Issues Report Notification (DIRN) for rejected Communications Hubs is available via the OMS within one Working Day. The DIRN shall contain the following:

(a) a unique DIRN reference;

(b) the date and time for collecting the Communications Hubs to be returned which shall be within five Working Days of the receipt of the notification.

6.24 Where the Party is unable to accommodate the collection date and time specified in the DIRN, it shall notify the DCC within one Working Day of receipt of the notification in accordance with clause 6.23 using the contact details published via the OMS for this purpose, and the DCC shall list reasonable potential options for revised collection dates and times and request a revised collection date and time from the Party, and that Party

shall notify the DCC using the contact details published via the OMS for this purpose of its preferred collection date and time from the options presented.

6.25 The DCC make a printable DIRN label available via the OMS for each unique DIRN reference within one Working Day of either:

(a) the receipt of the notification of rejection in accordance with clause 6.23; or

(b) notification by the Party of its preferred collection date and time in accordance with clause 6.24.

6.26 Parties shall ensure that rejected Communications Hubs are packaged in the cartons in which they were originally received and loaded so as not to exceed the maximum number of Communications Hubs per layer and layers per pallet as set out in Annex B of this document. The Party shall print and securely attach the DIRN label to the outside of each complete pallet or where the pallet is not complete on the outside of each carton that is to be returned.

Rejected Delivery Return Handover Procedure

6.27 When the collection vehicle arrives at a Party's Delivery Location, that Party shall:

(a) load the vehicle within two hours of the collection time; or

(b) load the vehicle within two hours of the time that the collection vehicle arrives at the Delivery Location, where the delivery vehicle arrives within two hours of the collection time and the arrival time is during Working Hours and where the Party can reasonably be expected to have completed loading during Working Hours;

(c) take reasonable steps~~use reasonable endeavours~~ to load the vehicle within two hours where the arrival time is later than two hours of the collection time and the arrival time is during Working Hours and where the Party can reasonably be expected to have completed loading during Working Hours;

(d) during loading, protect the goods from moisture and extremes of temperature in accordance with the environmental conditions set out in Annex C of this document, and as amended from time to time; and

(e) only load pallets or cartons with IDs that are included on the DIRN and that have a valid DIRN label attached onto the collection vehicle.

6.28 Where it is not possible to fulfil the collection and the DCC (or a Party) seeks to rearrange a collection date and collection window, the DCC shall list reasonable potential options for revised collection dates and collection windows and request a revised collection date and collection window from the affected Party. The Party shall choose a revised date and time from the options provided.

6.29 Where requested to do so the DCC shall sign the Party's collection note to confirm completion of collection prior to the collection vehicle departing the Delivery Location and the Party may provide a hard copy of the collection note to the DCC prior to the collection vehicle leaving the Delivery Location.

Delivery of Replacement Communications Hubs

6.30 Pursuant to Section F6.13, where a Party notifies the DCC of rejection for non-compliance of all or part of a Consignment in accordance with clause 6.20 of this document, the DCC shall by the next Working Day provide to the Party a list of reasonable potential options for revised Delivery Dates and Delivery Windows in respect of replacement goods and request a revised Delivery Date and Delivery Window from the Party. The Party shall indicate which one of the potential Delivery Dates and Delivery Windows offered by the DCC it prefers, and the DCC shall update the OMS accordingly.

6.31 Following the receipt of the DCC notification in accordance with clause 6.30, the replacement goods shall be treated as if a Consignment being delivered as part of a Valid Communications Hub Order and Sections 5 and 6 of this document shall apply accordingly.

7 COMMUNICATIONS HUB STORAGE AND TRANSIT REQUIREMENTS

Storage Conditions

7.1 Parties shall ensure that whilst the Party is in possession of the Communications Hub, Communications Hubs shall be handled, stored and delivered in accordance with the environmental conditions detailed in Annex C of this document.

Transit to and from Consumer Premises

7.2 Parties shall ensure that when transporting Communications Hubs, they meet the specifications as described in Annex D.1.1 and D.1.2 of this document.

7.3 Parties shall take reasonable steps to install Communications Hubs from stock on a 'first-in-first out' basis such that Communications Hubs are not held in storage for longer than is necessary.

Annex A. Annex A. Consignment Information

A.1. Consignment labelling and information

A.1.1. Table 1 below describes the information provided for each Communications Hub, each carton containing a Communications Hub and each pallet of Communications Hubs for delivery, depending upon the Region to which the associated Communications Hub Order relates. A summary of data items included in the Advance Shipment Notification and the associated Delivery Note is also provided.

Table 1; Consignment labelling and information

	CH Marking	Carton Labels	Pallet Labels	Advanced Shipment Notification		Delivery Note	
	All Regions	All Regions	All Regions	North Region	Central & South Regions	North Region	Central & South Regions
CHF Identifier (EUI-64 unique number)	Y	Y		Y	Y	Y	Y
Communications Hub WAN Variant	Y	Y	Y	Y	Y	Y	Y
GPF identifier (EUI-64 unique number)	Y			Y	Y		
Zigbee MAC address	Y			Y	Y		
SM WAN identifier				Y			
OMS Order Reference			Y	Y	Y	Y	Y
Party order reference			Y	Y	Y	Y	Y
Consignment reference			Y	Y	Y	Y	Y
Delivery Location				Y	Y	Y	Y
Scheduled Delivery Date and Time				Y	Y	Y	Y
Firmware version number				Y	Y		
Hardware version number	Y			Y	Y		
Device configuration identifier	Y			Y	Y		
Manufacturer, country and date of manufacture	Y			Y	Y		
Batch number				Y	Y		
Reconditioned status (Y/N)				Y	Y		
Pallet identifier			Y	Y	Y	Y	Y
Quantity of Cartons on the pallet			Y	Y	Y	Y	Y
Carton identifier		Y	Y	Y	Y	Y	Y
Quantity of Communications Hubs in carton		Y		Y	Y	Y	Y

Pallets in delivery						Y	Y

Annex B. Communications Hub Pallet and Carton Quantities

B.1. Communications Hub Packaging

B.1.1. Consignments will be delivered in accordance with the packaging quantities set out in Table 2 below. Maximum delivery volumes assume double stacked pallets. Individual Communications Hub Consignments may therefore include pallets in different pallet layers.

Table 2; Communications Hub delivery packaging

Packaging Information	North Region	Central Region and South Region
DCC Pallet size	Standard 4 Way L:1.2m, w:1m, H: 1m	Standard 4 Way L:1.2m, w:1m, H: 1m
Packaged Communications Hubs per carton	28	14
Cartons per layer	8	16
Maximum layers per pallet	4	4
Cartons per full pallet	32	64
Boxes per full pallet	896 (28 boxes x 32 cartons)	896 (14 boxes x 64 cartons)
Actual weight per full pallet	333 kg	
Maximum weight per pallet		Max 500 kg
Maximum pallet height (incl. Pallet base)	1m	1m
Maximum volume (m^3) per pallet	1.2 m^3	1.2 m^3
Maximum Pallets per trailer	52	40
Maximum packaged Communications Hubs per trailer	46,592	35,840

Annex C. Communications Hub storage and installation environmental conditions

C.1. Storage and installation environmental conditions

C.1.1. Communications Hubs are designed to be stored and operated within a defined range of environmental conditions; exposure to conditions outside this range may lead to premature failure of the device.

C.1.2. Communications Hubs are design to be stored under the following conditions:

(a) individual Communications Hubs should be kept in the original packaging provided for shipment prior to installation;

(b) any storage environment should meet European Telecoms Standards Institute ETSI EN 300 019-1-.1 Class 1.2 (Weather protected not temperature-controlled storage locations), or any equivalent standard that replaces this; and

(c) Good Industry Practices suitable for the handling, storage, preservation and internal delivery of the inventory of Communications Hubs that prevent damage, deterioration or misuse during internal processing should be followed.

C.1.3. Communications Hubs are designed to be transported in the following conditions:

(a) individual Communications Hubs should be transferred between locations packaged in their original packaging such that they are protected from damage during normal handling; and

(b) the transport environment should meet the European Telecoms Standards Institute ETSI EN 300 019-1-.2 Class 2.3 (Public Transportation), or any equivalent standard that replaces this.

C.1.4. Communications Hubs are design to be installed and operated under the following conditions:

(a) the Communications Hub should not be subject to moisture ingress or foreign object ingress during the installation process;

(b) following correct installation onto an ICHS-compliant host, moisture or foreign object ingress conditions should not exceed that specified in the IP53 Code under IEC standard 60529 or any equivalent standard that replaces this;

(c) the Communications Hub should not be subject to humidity outside the range of 10% to 90% non-condensing ; and

(d) the Communications Hub should not be exposed to extremes of temperature of below -20oC or above +55oC.

Annex D. Communications Hub Packaging

D.1.1. Communications Hubs will be individually packaged in a cardboard box that:

(a) is robust enough to protect the ICHIS connector pins during transport and handling; and

(b) allows for both the CHF Identifier and WAN Variant information to be visible directly through a cut-out without removing any of the packaging.

D.1.2. Individually boxed Communications Hubs will be grouped and packed in cardboard cartons that:

(a) protect the Communications Hub from damage during transport and handling;

(b) will contain the quantities set out in Annex B;

(c) are labelled in accordance with Annex B; and

(d) contain a single WAN Variant.

D.1.3. Cartons of Communication Hub will be delivered on UK standard pallets in the quantities per pallet set out in Annex B. The pallets will be wrapped in industrial pallet or stretch wrap material

APPENDIX I – CH INSTALLATION AND MAINTENANCE SUPPORT MATERIALS

Definitions

Central Region	means the Region which covers the majority of Wales and the majority of central England.
CH No SM WAN Installation Procedure	means the procedure by which a Supplier Party installs a Communications Hub where is it not to be connected to the SM WAN as described in clauses 4.7 to 4.9 of this document.
CH Status Information	means the visual information that is displayed by the Communications Hub to indicate the current operational status of the Communications Hub, as further set out in the CH Supporting Information.
CH Supporting Information	has the meaning given to that term in the CH Handover Support Materials.
CHF Identifier	has the meaning given to that term in CHTS.
Communications Hub Availability and Diagnostics Check	means the procedure set out in clause 5.2 of this document.
Communications Hub Fault Handling Procedures	means the processes set out in clauses 8.3 to 8.6 of this document.
Coverage Area	means the geographical coverage of the SM WAN at a point in time.

DCC Installer Training Plan	means the training materials provided by the DCC to support the development of Communications Hub installation and maintenance training.
DCC Returns Location	means a location at which a Party should deliver Communications Hubs that it wishes to return to the DCC.
Fault Analysis Report	means the report provided to a Party by the DCC pursuant to Section F9.11 of the Code.
Installation Location	means the location of a premises at which a Communications Hub is planned to be, or has been, installed.
Installation Point	means the location at an Installation Location where a Communications Hub is installed.
Mesh Communications Hub	means a WAN Variant in the Central Region and the South Region which is capable of using both mobile cellular radio technology and wireless mesh radio technology to connect to the SM WAN.
North Region	means the Region which covers the majority of Scotland and the majority of northern England.
Order Management System (or **OMS)**	has the meaning given to that term in the CH Handover Support Materials.
Return Date	means the date on which a Communications Hub is arranged to be delivered to the DCC by a Party
Return Delivery Note	means an electronic or paper form containing the information set out in clause 10.9.
Return Materials Authorisation (or **RMA**)	means the procedure whereby the DCC authorises a Party's request to return a Communications Hub to the DCC in accordance with clauses 10.3 to 10.5 of this document.

Significant Metallic Obstruction	means a metallic object of such scale and proximity to the Communications Hub as is likely to cause obstruction to SM WAN communications to the Communications Hub, and as further described in the CH Supporting Information.
Substantial Stone Walls	means walls with external or internal structure primarily made of stone and of sufficient thickness to be likely to prevent connectivity to the SM WAN by the Communications Hub, as further described in the CH Supporting Information.
South Region	means the Region which covers the majority of southern England.
Working Hours	has the meaning given to that term in the CH Handover Support Materials.

1 INTRODUCTION

Document purpose

1.1 Sections F7 to F9 set out principal rights and obligations applying to the installation and maintenance of Communications Hubs, which are supplemented by the provisions set out below. This document forms Appendix I of the Code.

General clarifications

1.2 Unless expressly stated otherwise, the obligations set out in this document are applicable to all Regions.

1.3 Unless expressly stated otherwise none of the obligations in this document apply to Test Communications Hubs.

2 GENERAL OBLIGATIONS IN RELATION TO THE INSTALLATION AND MAINTENANCE OF COMMUNICATIONS HUBS

DCC Obligations

2.1 The DCC shall ensure that it provides upon request to Parties a DCC Installer Training Plan which is sufficient to enable individuals accredited in accordance with it to carry out Communications Hub installation and maintenance activities in accordance with the CH Support Materials.

Supplier Party Obligations

2.2 Each Supplier Party shall ensure that any installations or maintenance of Communications Hubs undertaken on its behalf are undertaken by individuals that are certified to carry out Communications Hub installation and maintenance activities in accordance with the process for independent certification set out in the DCC Installer Training Plan.

3 PRE-INSTALLATION PROCEDURES

Activation prior to installation

3.1 A Party shall take all reasonable steps to prevent any Communications Hub in its possession from establishing a connection to the SM WAN prior to its installation for the purposes of Commissioning the Communications Hub Function.

Communications Hub inspections prior to installation

3.2 When installing a Communications Hub, prior to removing any packaging, a Party shall ensure that visual checks are undertaken to confirm that the packaged Communications Hub is not damaged.

3.3 Following the removal of all packaging, a Party shall ensure that visual checks are undertaken to confirm that the connecting pins (as described in the ICHIS) on the Communications Hub appear to be aligned and that the Communications Hub is not otherwise visibly damaged.

3.4 Where a Party, following inspection in accordance with clauses 3.2 and 3.3 above identifies damage to the Communications Hub or its packaging (including where the connecting pins are misaligned) that has caused or may reasonably be assumed to have caused more than superficial scratching or cosmetic damage to the body of the Communications Hub, the Party shall not attempt to install the Communications Hub and shall return the Communications Hub in accordance with clauses 10.1 to 10.17 of this document.

Pre-requisites for Fitting of Communications Hubs

3.5 Each installing Supplier Party shall ensure that a Communications Hub is not installed where it ascertains that the environmental conditions as defined in Annex A of this document are not met.

3.6 Prior to attempting a Communications Hub installation, a Supplier Party shall ensure that the Installation Point is visually inspected to assess whether it lies entirely within a metallic enclosure or if any Significant Metallic Obstruction(s) exists. A Supplier Party shall ensure that a Communications Hub is not installed where its visual inspection determines that:

(a) the Installation Point is entirely within a metallic enclosure; or

(b) a Significant Metallic Obstruction exists with respect to three or more of the following surfaces:

(i) the front surface of the Communications Hub;

(ii) the top surface of the Communications Hub;

(iii) the left-side surface of the Communications Hub; or

(iv) the right-side surface of the Communications Hub.

4 COMMUNICTIONS HUB INSTALLATION

4.1 When attempting the initial installation of a Communications Hub, a Supplier Party shall ensure that it uses the WAN Variant that was identified as being required for the Installation Location on the Coverage Database when the Supplier Party checked the Coverage Database, provided that this check was performed at any time within the period 30 days prior to the Installation Date.

4.2 When installing a Communications Hub or Communications Hub Auxiliary Equipment, as set out in the Annex F, a Supplier Party shall ensure that all appropriate tools and equipment are used.

Fitting and activation

4.3 A Supplier Party shall ensure that a Communications Hub is fitted according to the procedure set out in Annex B of this document.

4.4 On completion of the fitting procedure, the relevant Supplier Party shall ensure that the activation procedures for the Device Model that has been fitted are undertaken, as set out in Annex C of this document.

4.5 Where, during the installation process, the Supplier Party suspects that a fault has occurred with the Communications Hub, the relevant Supplier Party shall follow the procedures set out in clauses 8.1 to 8.8 of this document.

Post Installation Update Procedure

4.6 Where following completion of both the relevant fitting procedures and the relevant activation procedures, the Communications Hub is successfully connected to the SM WAN, the relevant Supplier Party shall:

(a) ensure that the Communications Hub is fitted with a security seal; and

(b) submit a Service Request 8.14.1 (Communications Hub Status Update – Installation Success) within five Working Days.

CH No SM WAN Installation Procedure

4.7 Where, following the fitting and activation procedure, a Supplier Party wishes to leave a Communications Hub installed without establishing a connection to the SM WAN, the Supplier Party shall:

(a) ensure that the power supply to the Communications Hub is capable of being maintained following fitting and activation;

(b) verify that the CH Status Information does not indicate any fault other than failure to connect to the SM WAN;

(c) ensure that the Communications Hub is fitted with a security seal; and

(d) the relevant Supplier Party shall notify the DCC by submitting a Service Request 8.14.2 (Communications Hub Status Update Install No SM WAN) as defined in DUIS, within three (3) Working Days.

4.8 Pursuant to 4.7(d) a Supplier Party submitting an 8.14.2 Service Request shall indicate whether each of the following conditions exists:

(a) a Significant Metallic Obstruction exists at the Installation Point with respect to any of the following surfaces;

(i) the front surface of the Communications Hub;

(ii) the top surface of the Communications Hub;

(iii) the left-side surface of the Communications Hub; or

(iv) the right-side surface of the Communications Hub.

(b) (without detailed or expert assessment), the Installation Point appears to have Substantial Stone Walls; or

(c) the Installation Point is in a shared or communal area, outside the individual premises.

4.9 Following receipt of a Service Request 8.14.2 (Communications Hub Status Update Install No SM WAN), the DCC shall create a coverage Incident.

5 COMMUNICATIONS HUB DIAGNOSTICS

5.1 Where, following successful installation of a Communications Hub and Commissioning of the related Communications Hub Function, a Supplier Party identifies a potential Communications Hub fault, pursuant to Section H9.6 of the Code, that Supplier Party shall take all reasonable steps to complete the Communications Hub Availability and Diagnostics Check procedure prior to raising an Incident with the DCC.

Communications Hub Availability and Diagnostics Check

5.2 A Supplier Party may undertake a Communications Hub Availability and Diagnostics Check, by either:

(a) utilising the Self Service Interface to complete the Communications Hub availability and diagnostic check as defined in the Self-Service Interface Design Specification; or

(b) sending Service Requests 6.13: (Read Event or Security Log) for the CHF event log and Service Request 8.9: (Read Device Log) for the CHF Device Log and interpreting the Service Responses received.

5.3 Where any Communications Hub Availability and Diagnostics Check indicates that the Communications Hub Function does not:

(a) have a network status of 'activated'; or

(b) the Communications Hub Availability and Diagnostics Check response indicates that an error has occurred;

the Supplier Party shall verify that the SMI Status of the Communications Hub Function is not 'Pending', 'Installed Not Commissioned', 'Decommissioned', 'Withdrawn' or 'Suspended', prior to raising an Incident.

5.4 Where any Communications Hub Availability and Diagnostics Check indicates that the SM WAN is unavailable for the Communications Hub, the Supplier Party shall check that there is no planned maintenance or existing DCC notified problem relating to SM WAN connectivity affecting the Installation Location by using the SM WAN network coverage functionality of the Self-Service Interface, prior to raising an Incident.

5.5 A Supplier Party shall include any relevant information from the Communications Hub Availability and Diagnostics Check in any Incident raised relating to that Communications Hub.

6 SPECIAL INSTALLATIONS & MODIFICATIONS

6.1 Where DCC identifies that resolution of an Incident relating to the ability to connect to the SM WAN requires work to be undertaken at a premises, the DCC shall notify the Supplier Party that raised the Incident accordingly. Such notification shall include details of the potential work required. The Supplier Party that raised the Incident may request that the DCC undertakes such work at the premises and the DCC shall be required to undertake such work, subject to the provisions of Section F7.5 – F7.7 of the Code.

6.2 Where a Supplier Party requires the DCC to undertake work at the premises, the Supplier Party shall update the Incident accordingly. The Supplier Party shall update the Incident with the following information when it is available:

(a) confirmation that consent for the work to be carried out has been obtained in accordance with Section F7.5 and F7.6 of the Code;

(b) the date and time at which the DCC should attend the relevant premises to carry out the work where;

(i) the Supplier Party shall ensure that the date is a Working Day, and the time shall be between 09:00 and 17:00;

(ii) the Supplier Party shall ensure that the date is no less than five Working Days after the date of this update; and

(c) contact details that the DCC should use to confirm attendance prior to the agreed date and time or in the event that further liaison with the Supplier Party is required.

6.3 Following the updates made pursuant to clause 6.2, the DCC shall subsequently update the Incident to provide contact details for its field force engineers at least one full Working Day prior to the date and time set for attendance at the relevant premises.

6.4 The DCC shall make all reasonable endeavours to attend the relevant premises at the specified date and time to undertake the work in accordance with Section F7.7 of the Code and shall notify the Supplier Party immediately where a delay to arrival is likely.

6.5 Where the DCC fails to meet the appointment, the DCC shall provide a list of reasonable options for revised dates and times from which the Supplier Party may

select. Where the Supplier Party selects one of the potential dates and times offered by the DCC the provisions of clause 6.4 shall apply to that new date and time.

7 DCC REQUEST TO ATTEND A PREMISES

7.1 Where, in accordance with Section F7.13, DCC wishes to request permission to attend a premises at which a Communications Hub is installed, the DCC shall notify the Supplier Party from whom access is being requested. Such notification shall include:

(a) details of any premises which the DCC wishes to attend, and the nature of the activity or inspection that the DCC intends to conduct; and

(b) DCC email and telephone contact details for the Party to use in relation to the process of arranging attendance at the premises.

7.2 Where the Supplier Party agrees to a request from DCC in accordance Section F7.14, or is required to take all reasonable steps to obtain Energy Consumer consent in accordance with Section F7.15, the Party shall notify the DCC, using the contact details provided pursuant to clause 7.1(b), of the following:

(a) confirmation that consent for the work to be carried out has been obtained or notification that consent has not been obtained;

(b) where consent has been obtained, the date and time at which the DCC should attend the relevant premises where;

(i) the Supplier Party shall ensure that the date is a Working Day, and the time shall be between 09:00 and 17:00;

(ii) the Supplier Party shall ensure that the date is no less than thirty (30) Days after the DCC notification was issued in accordance with clause 7.1 or the Panel determination was made pursuant to Section F7.15; and

(c) contact details that the DCC should use to confirm attendance prior to the agreed date and time or in the event that further liaison with the Supplier Party is required.

7.3 Following notification to the DCC pursuant to clause 7.2, the DCC shall, using the contact details provided, inform the Supplier Party of contact details for their personnel at least one full Working Day prior to the date and time set for attendance at the relevant premises.

7.4 The DCC shall attend the relevant premises at the specified date and time and shall immediately notify the Supplier Party, using the contact details provided, where a delay to arrival is likely.

8 ON-SITE FAULT RESOLUTION AND COMMUNICATIONS HUB REPLACEMENT

Site Visit - Environment Check Procedure

8.1 Where a Supplier Party is at a premises and prior to undertaking any Communications Hub Fault Handling Procedures, or replacing a previously installed Communications Hub, a Supplier Party shall verify that:

(a) the ICHIS compliant host is providing power to the Communications Hub; and

(b) that the prerequisites for installation of a Communications Hub set out in clauses 3.5 to 3.6 of this document are met.

8.2 Where the Supplier Party reasonably determines that the conditions in clause 8.1 are met the Supplier Party shall:

(a) where physical damage that is more than cosmetic is identified, remove the Communications Hub in accordance with clauses 9.1 to 9.9 of this document; and

(b) undertake the relevant Communications Hub Fault Handling Procedures.

Fault Handling Procedures

8.3 Where the Communications Hub, based on the CH Status Information, indicates an error state, the Supplier Party shall ensure that:

(a) the Communications Hub is removed in accordance with clause 9 of this document; and

(b) following a period of no less than five (5) minutes in the North Region and one (1) minute in the Central Region and South Region, during which there is no power to the Communications Hub and no physical connection to the host, the same Communications Hub is re-installed using the fitting and activation procedures as set out in Annex B and Annex C of this document.

8.4 Where, having undertaken the activities set out in clause 8.3(b), the Communications Hub, based on the CH Status Information, continues to indicate an error state, and the Supplier Party wishes to resolve the fault, the Supplier Party shall ensure that:

(a) the Communications Hub is removed in accordance with clause 9; and

(b) a replacement Communications Hub is installed in accordance with the fitting and activation procedures set out in Annex B and Annex C of this document.

8.5 Where the Communications Hub is located within the Central Region or South Region and the Communications Hub, based on the CH Status Information, indicates an 'attempting to connect to the SM WAN' state for longer than the maximum duration set out in the Communications Hub Supporting Information and the Communications Hub is a cellular Communications Hub, the Supplier Party shall ensure that the following steps are undertaken when attempting to resolve the fault:

(a) the Communications Hub is removed in accordance with clause 9 of this document; and

(b) the fitting and activation procedures relevant to a Mesh Communications Hub are undertaken as set out in Annex B and Annex C of this document.

8.6 Where the a Mesh Communications Hub is located within the Central Region or South Region and the Communications Hub, based on the CH Status Information, indicates an 'attempting to connect to the SM WAN' state for longer than the maximum duration set out in the Communications Hub Supporting Information, the Supplier Party shall ensure that an aerial is fitted in accordance with the procedures set out in B.2 of this document.

SM WAN Connectivity

8.7 Where a Supplier Party determines that, having undertaken the relevant Communications Hub Fault Handling Procedure, no fault exists with a Communications Hub, but no SM WAN connection is achieved, that Supplier Party shall raise or update an Incident in accordance with the Incident Management Policy to inform DCC of a local SM WAN connectivity issue, subject to clause 8.8.

8.8 Prior to informing DCC of a local SM WAN connectivity issue a Supplier Party shall:

(a) ensure that the power supply to the Communications Hub is maintained following the completion of the fault handling procedure;

(b) verify that the Communications Hub Status Information does not indicate any fault other than failure to connect to the SM WAN; and

(c) ensure that the Communications Hub is fitted with a security seal.

9 COMMUNICATIONS HUB REMOVAL AND NOTIFICATION OF RETURNS

Communications Hub removal

9.1 A Supplier Party may remove a Communications Hub from an ICHIS compliant host that is powered.

9.2 Where a Supplier Party removes a Communications Hub and any associated Communications Hub Auxiliary Equipment, the Supplier Party shall do so in accordance with the procedures set out in Annex B of this document.

Notification of returns

9.3 Following the removal of a Communications Hub, as a result of a suspected or actual fault in the Communications Hub the Supplier Party shall notify the DCC of its removal by submitting a Service Request in accordance with clauses 9.4 or 9.5 as applicable within five (5) Working Days of the date of removal.

9.4 Where the Communications Hub has been removed due to physical damage, the Supplier Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return) indicating the appropriate fault return type and reason as specified in the DCC User Interface Specification (DUIS).

9.5 Where a Communications Hub is removed in accordance with clause 8.4, the Supplier Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return) indicating the appropriate fault return type as specified in the DUIS.

9.6 Where a Communications Hub is removed and clause 9.4 and 9.5 do not apply, and the Supplier Party wishes to return the Communications Hub, the Supplier Party shall submit a Service Request 8.14.4 (Communications Hub Status Update – No Fault Return) indicating the appropriate return type as specified in Section F9, within five (5) Working Days of the date of removal.

9.7 Where either:

(a) a Communications Hub is to be returned prior to installation pursuant to clause 3.4; or

(b) the DCC has requested the return of a Communications Hub in accordance with Section F8.1(b) of the Code or the Supplier Party is required to return pursuant to Section F8.6 of the Code;

the Party shall submit a Service Request 8.14.3 (Communications Hub Status Update – Fault Return).

9.8 Where a Communications Hub is to be returned prior to installation pursuant to Section F8.7(a) of the Code, the responsible Party shall submit a Service Request 8.14.4 (Communications Hub Status Update – No Fault Return).

9.9 In the event that a Party is not able to submit a Service Request in accordance with clauses 9.4, 9.5, 9.6, 9.7 or 9.8 that Party shall contact the Service Desk.

10 COMMUNICATIONS HUB RETURNS

10.1 Following the acceptance of Communications Hubs, where a Party wishes to return Communications Hubs to the DCC, that Party shall do so in accordance with the procedures set out in this clauses 10.1 to 10.17 of this document.

10.2 The DCC shall make available to all OMS account profiles, the following information for any DCC Returns Location:

(a) the full delivery address;

(b) operating hours; and

(c) the name, email address, and telephone number for a nominated contact in relation to Communications Hub returns.

Return Materials Authorisation

10.3 To return a Communications Hub a Party shall request a Returns Material Authorisation (RMA) once that Party has notified the DCC by either having:

(a) submitted Service Request 8.14.3 or Service Request 8.14.4 in respect of the Communications Hub to be returned; or

(b) contacted the Service Desk.

10.4 The requesting Party shall ensure that the request for an RMA is:

(a) made via the 'CH Ordering' or 'CH Delivery and Returns' OMS profiles; and

(b) includes:

(i) the CHF Identifier for each Communications Hub to be returned under that RMA, as previously notified to the DCC in accordance with clause 10.3

(ii) the contact name, email address, and telephone number to be used by the DCC to contact the Party in relation to that RMA;

(iii) the preferred DCC Returns Location; and

(iv) a preferred Return Date, which shall be on a Working Day at least five (5) Working Days following the date that the request for the RMA is submitted.

10.5 Following acceptance of an RMA request, the DCC shall:

(a) confirm authorisation to the submitting Party using the contact details provided; and

(b) provide the Party with the following information via the Order Management System using either the 'CH Ordering' or 'CH Delivery and Returns' OMS profiles:

(i) a unique booking reference;
(ii) confirmed timeslot for delivery;
(iii) RMA reference; and
(iv) any changes to the DCC contact details for the purposes of the return.

Returns Equipment and Packaging

10.6 A Party shall ensure that all Communications Hubs returned to the DCC are in packaging of equivalent standard to that in which a Communications Hub of that Device Model was originally packaged, not exceeding the maximum number of Communications Hubs per carton and cartons per pallet set out in the CH Handover Support Materials.

10.7 Where a Communications Hub has been subject to environmental or biological contamination, the Party shall:

(a) where it is safe to do so, place the Communications Hub in appropriately sealed packaging such that DCC can clearly identify the nature of the contamination without removing or unsealing such packaging; or

(b) where safe return of a contaminated Communications Hub is not possible, safely and securely dispose of the Communications Hub.

Delivery of Returns

10.8 Where the Party does not return a Communications Hub within 90 days pursuant to Section F8.6 of the Code, the Communications Hub shall be deemed to be lost or stolen and the DCC shall prevent that Communications Hub from connecting to the SM WAN.

10.9 The Party shall ensure that the Communications Hub delivery is accompanied with a Return Delivery Note that contains, as a minimum, the following information:

(a) booking reference for the return delivery as supplied by DCC pursuant to clause 10.5;

(b) return date and return delivery time;

(c) Party Signifier;

(d) DCC Returns Location;

(e) list of all CHF Identifiers being returned; and

(f) (where one or more pallets are to be returned), the pallet identifiers for each pallet being returned.

10.10 The DCC shall provide the Party with a printable RMA label for each return delivery via the OMS (using the CH Ordering or CH Delivery and Returns profile) immediately following authorisation. The Party shall securely attach the corresponding RMA label on each pallet and each carton (where a carton is not part of a pallet) and each Communications Hub (where a Communications Hub is not part of a pallet or carton) for each return delivery.

10.11 The Party shall notify the DCC if there are any known issues that mean the delivery will be late, stating the reason for the delay and the expected time of arrival. The Party shall take all reasonable steps to make such notification a minimum of 5 Working Hours prior to the return delivery booking time. The DCC shall take all reasonable steps to accommodate a revised return delivery booking time and shall confirm to the Party that the DCC is either:

(a) able to accept the late return delivery; or

(b) unable to accept the return delivery.

10.12 Where the DCC is unable to accept the return delivery the DCC shall notify the returning Party as soon as reasonably practicable and shall notify the Party of the full range of available delivery dates and times within the following 90 days and the Party shall notify the DCC of an acceptable revised date and clauses 10.10 and 10.11 shall apply in relation to the revised date.

Delivery Acceptance

10.13 Prior to signing the Return Delivery Note, the DCC may carry out the following;

(a) assessment of pallets delivered against those recorded under the RMA request;

(b) checks between CHF Identifiers received against those listed under the RMA request; and

(c) checks that the number of Communications Hubs returned match the number of CHF Identifiers listed in the RMA request.

10.14 The DCC may reject any returned Communications Hubs where unloading them would present a health and safety risk. Where the DCC rejects the return delivery, the Party shall be required to request a new RMA and rearrange the return delivery following the relevant procedures set out in clauses 10.3 to 10.12 of this document.

10.15 Following the checks performed pursuant to clause 10.13, the DCC shall record any discrepancies between the return delivery and the Return Delivery Note.

10.16 Where requested to do so the DCC shall sign and retain a copy of the Return Delivery Note.

10.17 Where the Party fails to provide the DCC with a fault reason for each CHF Identifier in accordance with the requirements set out in this document, the Communications Hub shall be deemed to be a return pursuant to Section F9.5 (e) of the Code and the Communications Hub Fault shall be a CH User Responsibility in accordance with Section F9.6 (a) of the Code.

11 CH FAULT DIAGNOSIS BY DCC

Receipt of Communications Hubs

11.1 The DCC shall create an individual record for each returned Communications Hub on receipt of Service Request 8.14.3, 8.14.4 or any return notified through the Service Desk. For each returned Communications Hub this record shall contain all details received by DCC from the Party within the Service Request or provided via the Service Desk and other supporting information as set out in Annex E, and shall be made immediately available by the DCC to the Party that returned the Communications Hub via the SSI.

Notification

11.2 Where the DCC intends to undertake any CH Fault Diagnosis, the DCC shall update the relevant record, as described in Annex E of this document, indicating that further analysis is required, in accordance with Section F9.9 of the Code. The DCC shall make this information available via the SSI and notify the Party that returned the Communications Hub of this revision.

11.3 Following a notification received by DCC pursuant to clause 10.2, in the event that a Party is not able to access the SSI in accordance with clause 11.2, that Party shall contact the Service Desk in order to access the updated record, which the DCC shall enable.

Fault Diagnosis Approach

11.4 The DCC shall undertake CH Fault Diagnosis using visual and electronic analysis of returned Communications Hubs, as set out in clauses 11.5 and 11.6.

Visual analysis

11.5 The DCC may undertake the following visual inspections of a returned Communications Hub and shall subsequently update the information in the Fault Analysis Report to include the results from this analysis:

(a) check for any physical damage to any part of the Communication Hub including, but not limited to, the outer casing, external interfaces and connectors;

(b) check to identify any loose internal components and for evidence that such components were previously connected correctly;

(c) check for any evidence of tampering; and

(d) check for any evidence of exposure to adverse environmental conditions including, but not limited to, water, condensation, smoke, chemicals, pests, etc.

Electronic analysis

11.6 Where the Communications Hub is not deemed to be physically damaged in accordance with clause 11.5, the DCC may undertake the electronic diagnostic tests described in Annex D of this document and shall subsequently update the information in the Fault Analysis Report to include the results from this analysis.

Fault Analysis Report

11.7 The DCC shall provide the Party which returned the Communications Hub with a Fault Analysis Report. The DCC shall provide this Fault Analysis Report by updating the relevant record maintained for each returned Communications Hub, as set out in Annex E of this document, with the results of the Fault Analysis and make this available via the SSI.

11.8 The DCC shall immediately notify the Party that returned the Communications Hub when any new or amended Fault Analysis Report is made available via the SSI. Pursuant to Section F9.12 of the Code, where the DCC does not update the Fault Analysis Report within 35 days the DCC shall update the 'Returns Record Status' field to "Closed" and the fault reason provided by the Party shall not be changed.

Acceptance

11.9 Where the fault reason provided by the DCC in the Fault Analysis Report:

(a) matches the fault reason reported by the Party no further action is required and the DCC shall update the 'Returns Record Status' field to "Closed"; or

(b) does not match the fault reason provided by the Party and the Party does not object in accordance with Section F9.13 of the Code, no further action is required by the Party and the DCC shall update the 'Returns Record Status' field to "Closed".

Objections

11.10 Where the Party wishes to notify the DCC of their objection pursuant to Section F9.14 of the Code it shall do so via the Service Desk.

Annex A. CH Installation Environmental Conditions

A.1.1. Communications Hubs shall be installed according to the following conditions:

(a) the Communications Hub should not be subject to moisture ingress or foreign object ingress during the installation process;

(b) following installation, moisture or foreign object ingress conditions should not exceed that specified in the IP53 Code under IEC standard 60529 or any equivalent standard that replaces this;

(c) the Communications Hub should not be subject to humidity outside the range of 10% to 90% non-condensing;

(d) the Communications Hub should not be exposed to extremes of temperature of below -20^{o}C or above +55^{o}C; and

(e) the temperature difference between the Communications Hub to be installed and the ICHIS compliant host shall not exceed 10 degrees Celsius.

Annex B. CH Fitting and removal procedures

B.1. Fitting procedure

B.1.1. A Party shall ensure that all reasonable precautions are taken to avoid electrostatic discharge whilst handling the Communications Hub.

B.1.2. A Supplier Party shall ensure that all reasonable precautions are taken to avoid electrostatic discharge when installing any Communications Hub and Communications Hub Auxiliary Equipment.

B.1.3. The Communications Hub shall be mounted vertically above the ICHIS compliant host, ensuring that the Communications Hub WAN Variant labelling text on the front face is horizontal.

B.1.4. A Party may mount a Communications Hub on an ICHIS compliant host that is powered.

B.1.5. A Supplier Party shall fit a Communications Hub in accordance with the steps set out below:

(a) **Step 1** - Align Communications Hub guide rails with the U-channel of the ICHIS compliant host;

(b) **Step 2** - Slide the Communications Hub on to the ICHIS compliant host, ensuring that the Communications Hub guide rails remain within the U-Channel of the ICHIS compliant host;

(c) **Step 3** - Press the front faceplate in order to lock the Communications Hub on to the interface of the ICHIS compliant host, applying hand pressure only; and

(d) **Step 4** - Screw in the M4 retaining screw located on the front faceplate of the Communications Hub to fasten it to the ICHIS compliant host.

B.2. Installation of Communications Hub aerials - Central Region and South Region

B.2.1. For the South Region or Central Region, where use of a Communications Hub aerial is indicated as being required, either by the Coverage Database or as a result of a failure as described in Annex C of this document, the Supplier Party shall ensure that when installing the Communications Hub aerial:

(a) all reasonable steps are taken to ensure any external aerial is positioned vertically and avoiding any Significant Metallic Obstruction;

(b) all reasonable steps to minimise risk of damage to the aerial lead during installation are undertaken and that the environmental conditions for the Communications Hub are not exceeded;

(c) stub aerials (i.e. with no cable attached) are not used to connect the aerial directly onto the Communications Hub, the cable must always be used as supplied.

B.2.2. For the South Region or Central Region, a Supplier Party shall install a Communications Hub aerial in accordance with the steps below:

(a) **Step 1** - unpack the aerial and inspect for damage prior to attaching to the SMA connector on the cable;

(b) **Step 2** - attach the aerial to the cable SMA connector;

(c) **Step 3** - ensure the Communications Hub is powered when connecting the aerial and cable to the SMA connector on the Communications Hub;

(d) **Step 4** - fasten both aerial and cable connectors to finger-tightness;

(e) **Step 5** - secure the Communications Hub hinged plastic cover over the connector, ensuring that the RF cable remains free to allow aerial positioning once fitted;

(f) **Step 6** - use the Visual Information set out in the CH Supporting Information to identify the strength of the signal at varying positions of the RF cable and position the aerial to first maximise the signal strength and second minimise the distance to the Communications Hub;

(g) **Step 7** - if the aerial position does not require the full length of the supplied RF cable, the spare RF cable shall be loosely coiled and fastened using a soft Velcro cable tie ensuring not to crush or kink the RF cable;

(h) **Step 8** - once the optimum location for the aerial has been confirmed the aerial shall be positioned vertically with the cable connector at the base then either:

(i) fasten the aerial in place using the appropriate fasteners provided in the assembly kit: or

(ii) depending on the type of aerial used, connect to a wall using self-adhesive.

(i) **Step 9** - following installation of the aerial as set out in steps 1-8 above, the installer should wait for a minimum of two (2) minutes, and then undertake the activation processes set out in Annex C of this document.

B.3. Communications Hub removal procedure

B.3.1. Where a Supplier Party removes a Communications Hub, the Supplier Party shall:

(a) **Step 1** -Remove or break the security seal;

(b) **Step 2** -Remove the M4 retaining screw located on the front faceplate of the Communications Hub to enable its removal from the ICHIS compliant host; and

(c) **Step 3** -Slide the Communications Hub from the ICHIS compliant host, ensuring that the Communications Hub guide rails remain within the U-Channel of the Electricity Smart Meter or Hot Shoe.

Annex C. Activation Procedure

C.1. Communications Hub Activation Procedure - North Region

C.1.1. For the North Region, following the fitting of a Communications Hub, the Supplier Party shall verify the successful activation of the Communications Hub by monitoring that the CH Status Information indicates the following Communications Hub states as set out in the CH Supporting Information, in the sequence:

(a) 'SM WAN initialising';

(b) 'attempting to connect to the SM WAN'; and

(c) 'SM WAN connected'.

C.1.2. For the North Region, where the Communications Hub activation fails to complete, the Supplier Party shall ensure that:

(a) where the CH Status Information indicates that the Communications Hub is in an error state, the Communications Hub Fault Handling Procedures are followed; or

(b) where the Communications Hub fails to transition from the 'attempting to connect to the SM WAN' state to the 'SM WAN connected' state within the maximum time set out in the CH Supporting Information, but no fault is indicated, the Supplier Party may wish to undertake the CH No SM WAN Installation Procedure.

C.2. Communications Hub Activation Procedure - Central Region and South Region

C.2.1. Following the fitting of a cellular Communications Hub, the Supplier Party shall ensure that a check is performed to confirm that the following Communications Hub states are achieved, based on the CH Status Information, as set out in the CH Supporting Information:

(a) initialisation complete;

(b) SW LED normal operation;

(c) SM WAN (cellular) connecting; and

(d) SM WAN (cellular) successfully connected.

C.2.2. Where the Communications Hub activation fails to complete, the Supplier Party shall ensure that:

(a) where the CH Status Information indicates that the Communications Hub is in an error state, the fault resolution procedures set out in clauses 8.1 to 8.8 of this document are followed; or

(b) where the SM WAN indicator fails to transition from the 'SM WAN (cellular) connecting' state to the 'SM WAN (cellular) successfully connected' state within the maximum time set out in the CH Supporting Information, the cellular Communications Hub is removed and a Mesh Communications Hub is fitted in accordance with the fitting and activation procedures set out in Annex B and Annex C of this document.

C.2.3. Where installing a Mesh Communications Hub, the Supplier Party shall ensure that the Visual Information set out in the CH Supporting Information is monitored to confirm the following Communications Hub states are achieved :

(a) initialisation complete;

(b) SW LED normal operation;

(c) and either:

(i) SM WAN (cellular) connecting;

(ii) SM WAN (cellular) successfully connected;

or

(iii) Mesh connecting; and

(iv) Mesh connected.

C.2.4. Where the Mesh Communications Hub activation fails to complete, the Supplier Party shall ensure that:

(a) where the CH Status Information indicates that the Mesh Communications Hub is in an error state, the fault resolution procedures set out in clauses 6.1 to 6.5 of this document are followed; and either:

(b) where no Communications Hub aerial has previously been fitted and the SM WAN indicator fails to transition from the 'SM WAN (cellular) connecting' state to the 'SM WAN (cellular) successfully connected' state or from the 'Mesh Connecting' state to the 'Mesh connected' state within the maximum time set out in the CH Supporting Information, a Communications Hub aerial

is fitted in accordance with the fitting and activation procedures set out in Annex B and Annex C of this document.

or

(c) where a Communications Hub aerial has previously been fitted and the Mesh Communications Hub fails to transition from the 'SM WAN connecting' state to the 'SM WAN successfully connected' state or from the 'Mesh Connecting' state to the 'Mesh connected' state within the maximum time set out in the CH Supporting Information, but no fault is indicated, the Supplier Party may wish to undertake the CH No SM WAN Installation Procedure.

Annex D. Electronic Fault Diagnosis

D.1.1. The DCC may carry out the following checks as part of the Communications Hub Fault Handling Procedure :

(a) check of hardware and firmware validity;

(b) check of device configuration;

(c) checks of power consumption;

(d) detection of malfunction of internal components via self-tests;

(e) connectivity test for HAN components;

(f) connectivity test for SM WAN components;

(g) functional check of visual status indicators (LEDs);

(h) verification that power outage power storage is within expected tolerance;

(i) tamper detection check;

(j) clock test (set real-time clock or read real-time clock); and

(k) review of the security and event logs.

Annex E. Fault Analysis Report data items

E.1.1. Table 1 identifies the data fields that will be provided in the Communications Hub Fault Analysis Report. Data items shall be updated in line with the progress of the fault analysis and some items may therefore be blank.

Table 1; Fault Analysis Report data field descriptions

Field name	Description
Returns record id	Unique reference for the returns Record.
Incident reference	This field displays the Incident request identifier if provided by a Party
User ref id	Unique reference for the update provided by a Party.
User id	SEC Party Signifier of the Party that submitted the Communications Hub status update
CHF return type	Category of Return, as provided by a Party and specified in DUIS
User fault diagnosis (CHF fault reason)	Initial fault diagnosis code, as provided by a Party and specified in DUIS.
CSP fault diagnosis	DCC fault diagnosis following the fault analysis process.
DCC fault diagnosis	DCC fault diagnosis following conclusion of any objection process.
User fault responsibility	Derived from user fault diagnosis
DCC fault responsibility	Derived from DCC fault diagnosis
Final agreed fault responsibility	Derived from DCC fault diagnosis
CSP id	The DCC Service Provider identified by the Region.
Device id	The unique CHF ID
Return record create date	The Date and time the returns record was created.
User job date time	Time of removal of the Communications Hub provided by a Party.
Preliminary FA received date	The date the DCC issued the preliminary Fault Analysis Report via the SSI.
CSP FAR received date	The date the DCC issued the final Fault Analysis Report via the SSI.

Field name	Description
Return closed date	The date and time the DCC issued the final Fault Analysis Report.
Received communications hub date	The date and time the DCC receives the Communications Hub from the Party.
Dispute start date	The date and time the dispute started.
Other device id	UID of the ESME
CHF connection method	To record whether hot-shoe or cradle CHF installation
	To record how the Communications Hub has been installed and connected to the rest of the Smart Metering System within the premises Valid set: Hot-shoe Cradle ESME
Cause of fault	A short description of the fault cause supplied by the DCC
Additional information	Further Analysis details from the Fault Cause supplied by the DCC
full analysis	Y/N flag indicating whether a full analysis is required. Will drive the status of the returns record
User organisation	Details of organisation associated with User ID
Premises postcode	Derived from MPAN / MPRN associated with the Communications Hub
Product name+	Derived from CHF ID
Model	Derived from CHF ID
Manufacturer	Derived from CHF ID
Communications hub delivery location	The location the Communications Hub was delivered to (provided by DCC)
Communications hub installation date	From the Smart Metering Inventory, where applicable.
Incident resolved date	Manually populated by Service Desk
CSP region	The Region in which the Communications Hub was installed.
Communications hub commissioned date	From the Smart Metering Inventory

Field name	Description
Communications hub device type	Supplied on creation by DCC
Communications hub returning supplier	Supplied on creation by DCC
Communications Hub delivery date	From the Smart Metering Inventory.

Annex F. Equipment Supplied

F.1. North Region

F.1.1. The DCC shall supply the following equipment:

(a) Standard 420 Communications Hub with captive security screw; and

(b) Variant 450 Communications Hub with captive security screw.

F.2. Central and South Regions

F.2.1. The DCC shall supply the following equipment:

(a) WAN Variant Cellular only Communications Hub with captive security screw;

(b) WAN Variant Cellular + RF mesh Communication Hub with captive security screw; and

(c) Auxiliary equipment, including aerials, RF cable and soft Velcro ties.

SEC - Appendix J: February 2016 Consultation (showing changes in mark-up from last published version)

Appendix J - Enduring Testing Approach Document

1 Introduction

Scope

1.1 The Enduring Testing Approach Document (ETAD) describes the detailed procedural and technical requirements for the Testing Services, as defined in Section H14.1, that the DCC will make available to Testing Participants on an enduring basis. The security requirements and requirements for provision of Test Certificates will also be applicable for RDPs for the purpose of participating in Systems Integration Testing, as signalled in the Systems Integration Testing Approach Document.

1.2 This document is a subsidiary document of the Smart Energy Code (SEC).

2 Security requirements

2.1 For the purposes of this document, "Testing Participant Systems" means:

(a) any Systems (excluding any Devices) that are operated by or on behalf of a Testing Participant and used in whole or in part for the testing equivalent of:

(i) constructing Service Requests;

(ii) sending Service Requests over the DCC User Interface;

(iii) receiving, sending, storing, using or otherwise carrying out any processing in respect of any Pre-Command or Signed Pre-Command;

(iv) receiving Service Responses or Alerts over the DCC User Interface;

(v) generating Data for communication to the OCA, DCA or ICA, or receiving Data from the OCA, DCA or ICA (including any Systems which store or use Secret Key Material for such purposes);

(vi) generating Data for the purposes of lodging in the SMKI Repository, or retrieving Data from the SMKI Repository;

(vii) providing (or procuring the provision of) Registration Data in respect of a particular MPAN or MPRN; and/or

(viii) the collection, storage or communication of the Registration Data referred to in sub-clause vii) above prior to, or for the purposes of, its provision to DCC over the Registration Data Interface; and

(b) any other Systems from which the Systems used in whole or in part for the purposes set out in clause (a) are not Separate.

2.2 Each Testing Participant shall ensure that its Testing Participant Systems are Separate from:

(a) its RDP Systems or User Systems, as appropriate; and

(b) any other Systems not used for the purposes of carrying out tests using the Testing Services.

2.3 Each Testing Participant shall take reasonable steps~~use its reasonable endeavours~~:

(a) to ensure that its Testing Participant Systems are capable of detecting any unauthorised software that has been installed or executed on them and any unauthorised attempt to install or execute software on them;

(b) if those Testing Participant Systems detect any such software or such attempt to install or execute software, to ensure that the installation or execution of that software is prevented; and

(c) where any such software has been installed or executed, to take appropriate remedial action.

2.4 Each Testing Participant shall ensure that it carries out assessments that are designed to identify any vulnerability of its Testing Participant Systems to Compromise:

(a) prior to accessing any Testing Services using such Testing Participant Systems and on at least an annual basis thereafter;

(b) in respect of each new or materially changed component or functionality of its Testing Participant Systems, prior to that component or functionality becoming operational; and

(c) on the occurrence of any security issue in relation to its Testing Participant Systems.

2.5 Where, following any assessment of its Testing Participant Systems in accordance with clause 2.4 or otherwise, any material vulnerability has been detected, the Testing Participant shall:

(a) take reasonable steps~~use its reasonable endeavours~~ to ensure that the cause of the vulnerability is rectified, or the potential impact of the vulnerability is mitigated, as soon as is reasonably practicable; and

(b) promptly notify the DCC of the steps being taken to rectify its cause or mitigate its potential impact (as the case may be) on DCC Systems and the time within which they

are intended to be completed, and comply with any reasonable request from the DCC to mitigate or prevent any potential adverse impact on the DCC Systems arising from such vulnerability.

3 IKI and SMKI Test Certificates

3.1 The DCC shall issue Test Certificates simulating the function of Organisation Certificates, OCA Certificates, Device Certificates, DCA Certificates, IKI Certificates and ICA Certificates in accordance with the relevant provisions of the "Test Documents".

3.2 For the purposes of clause 3.1, the Test Documents means:

(a) the Test Certificate Policy, which shall be a document published by the DCC and approved by the SMKI PMA which corresponds (insofar as relevant in respect of the Testing Services) in purpose, content and effect to the Organisation Certificate Policy, the Device Certificate Policy and the IKI Certificate Policy; and

(b) subject to clause 3.4:

(i) the SMKI RAPP;

(ii) the SMKI Interface Design Specification;

(iii) the SMKI Code of Connection;

(iv) the SMKI Repository Interface Design Specification; and

(v) the SMKI Repository Code of Connection.

3.3 For the purposes of clause 3.2(b)(i), each Testing Participant shall, when completing the forms in the appendices of the SMKI RAPP for test purposes, clearly mark each page with the text, "For Testing Purposes" and submit the completed forms to the SMKI Registration Authority, in writing, as directed on the DCC Website.

3.4 For the purposes of clause 3.2(b):

(a) each of the documents there specified as Test Documents shall, if no such document has yet have been incorporated into the SEC, be interpreted as meaning the draft of that document most recently published on the DCC Website;

(b) any reference in such documents to any office, function, role, system, process or other ting shall be construed as being a reference to the corresponding equivalent of that office, function, roe, system, process or thing which is established, undertaken, operated or given effect (as the case may be) for the purposes of the Testing Services;

(c) Testing Participants shall not be required to complete SMKI and Repository Entry Process Tests to become eligible to obtain IKI and SMKI Test Certificates;

(d) where agreed by the DCC and a Testing Participant, any of the requirements that a Testing Participant must satisfy in order to be entitled to become an Authorised Subscriber for a Test Certificate may be disregarded for the purposes of such entitlement;

(e) the DCC shall publish on the DCC Website, and from time to time update, limits on the number of Certificate Signing Requests that each Testing Participant may submit in any particular time period over any relevant interface for testing purposes;

(f) each Testing Participant shall ~~use all reasonable endeavours~~take all reasonable steps to ensure it does not submit certificate signing requests for testing purposes in excess of any limit published (or updated) in accordance with clause (e) above;

(g) the DCC shall publish on the DCC Website, and from time to time update, limits on the total number of Certificate Signing Requests across all Testing Participants that can be processed each day. The DCC shall not be required to process any Certificate Signing Request in excess of such limits that is submitted by any Testing Participant.

4 DCCKI Test Certificates

4.1 The DCC shall issue DCCKI Test Certificates simulating the function of DCCKI Certificates in accordance with the relevant provisions of the "DCCKI Test Documents".

4.2 For the purposes of clause 4.1, the DCCKI Test Documents means, subject to clauses 4.3 to 4.5:

(a) the Test DCCKI Certificate Policy;

(b) the DCCKI RAPP;

(c) the DCCKI Interface Design Specification and DCCKI Repository Interface Design Specification; and

(d) the DCCKI Interface Code of Connection and DCCKI Repository Code of Connection.

4.3 For the purposes of clause 4.2 (a) and for issuing Test DCCKI Certificates, the Test DCCKI Certificate Policy shall be the most recently published draft of the DCCKI Certificate Policy at that date, modified such that:

(a) the OID in clause 1.2 is replaced by 1.2.826.0.1.8641679.1.2.1.12;

(b) the modifications identified in clause 4.5 below apply; and

(c) any changes that:

(i) have been approved by the DCCKI PMA function prior to taking effect; and

(ii) do not directly affect any rights or obligations of Parties (other than the DCC) or RDPs,

apply.

4.4 For the purposes of identifying the DCCKI Certificate Policy referred to in clause 4.3 and the documents specified as DCCKI Test Documents in clause 4.2 (b), (c) and (d), if no such

document has yet been incorporated into the SEC, be interpreted as meaning the draft of that document most recently published on the DCC Website.

4.5 For the purposes of clause 4.2:

(a) any reference in such documents to any office, function, role, system, process or other thing shall be construed as being a reference to the corresponding equivalent of that office, function, role, system, process or thing which is established, undertaken, operated or given effect (as the case may be) for the purposes of the Testing Services;

(b) Parties and RDPs shall be considered to be DCCKI Authorised Subscribers for testing purposes where they have appointed at least one DCCKI SRO and at least one DCCKI ARO;

(c) any reference to lodging of information in the DCCKI Repository, including DCCKI Certificates, EII DCCKICA CRL and DCCKI ARL, shall be modified such that the DCC may, where the DCCKI Repository is not available, provide such information via an alternative means to be notified to DCCKI Authorised Subscribers, and where approved in advance by the DCCKI PMA function;

(d) all obligations on the DCC in respect of timescales associated with the delivery of DCCKI Services or DCCKI Repository Services, shall be modified so that any such timescales shall be replaced with "as soon as reasonably practicable, having regard to the requirement to provide DCCKI Services and DCCKI Repository Services";

(e) any reference to raising Incidents and Major Security Incidents shall not apply and the provisions of the Testing Issue Resolution Process shall apply; and

(f) the following provisions of the documents shall be disregarded and treated as forming no part of the DCCKI Test Documents:

(i) references to interactions with the Service Desk processes shall not apply, except to the extent that such processes are required to support the identity verification of individuals nominated to become DCCKI SROs or DCCKI AROs for testing purposes; and

(ii) clauses 3.2(b); 3.15; 3.16; and 4.4 to 4.12; in the DCCKI RAPP shall not apply.

4.6 For the purposes of clause 4.2(b), each Testing Participant shall, when completing the forms in the annexes of the DCCKI RAPP for testing purposes, clearly mark each page with the text, "For Testing Purposes" and submit the completed forms to the DCCKI Registration Authority, in writing, as directed on the DCC Website.

5 Obligations on Testing Participants using Remote Test Labs

5.1 In accordance with Section H14.31 Testing Participants are eligible to connect to a simulation of the SM WAN (" a test SM WAN") for the purposes of conducting Device and User System Tests remotely at premises of their choice. As well as providing the necessary Test Communications Hubs, Smart Meters and any other Devices which they choose to test, the Testing Participant may need to establish a connection to the test SM WAN in the chosen Region(s).

5.2 The DCC shall include a description of the equipment that will be provided to enable connection to and use of a test SM WAN for the purposes set out above in the guide for Testing Participants which the DCC is obliged to publish under Section H14.3.

5.3 Where a Testing Participant is considering ordering a connection to the test SM WAN, the Testing Participant shall first contact the DCC via the Service Desk to request a site survey and resulting quotation setting out the charges to apply.

5.4 On receiving a request for a site survey and a quotation of the charges to apply, the DCC shall undertake the steps detailed below as soon as is reasonably practicable:

(a) Conduct a site survey to assess the equipment that needs to be provided by the DCC, and any specific requirements to be fulfilled by the DCC for the premises at which the equipment is to be installed; and

(b) set out the charges to apply, which may comprise:

(i) a connection charge for standard connection equipment;

(ii) an additional charge for additional, non-standard connection equipment; and

(iii) a monthly operating charge.

5.5 Upon receipt of the details of the site survey and the charges which will apply, the Testing Participant shall, if it wishes to place an order, notify the DCC accordingly.

5.6 Where the Testing Participant notifies the DCC that it wishes to place an order under clause 5.5, the DCC shall provide the connection as soon as is reasonably practicable, and in any event within 6 months of the order being placed.

5.7 The DCC shall provide reasonable notice to the Testing Participant of the planned date of installation of the connection equipment and the establishment of the connection to the test SM WAN.

5.8 Where the Testing Participant requests a change to the planned date of installation advised by the DCC, that planned date of installation shall be amended, subject to the Testing Participant agreeing to pay for any additional charges notified by the DCC to cover the additional reasonable costs incurred by the DCC resulting from the change of date. In first providing the connection at the premises, the DCC shall procure that the test SM WAN connection equipment is installed at the premises and that it is done so in accordance with Good Industry Practice and all applicable Laws and Directives.

5.9 A Testing Participant at whose premises test SM WAN connection equipment has been installed shall ensure that no damage is deliberately or negligently caused to that equipment (save that such a Party may take emergency action in accordance with Good Industry Practice to protect the health and safety of persons or to prevent imminent damage to property).

5.10 The test SM WAN connection equipment shall (as between the DCC and the Testing Participant) remain the property of the DCC. No Testing Participant shall hold itself out as the owner of such connection equipment, or purport to sell or otherwise dispose of such connection equipment. Such equipment is installed at the DCC's risk and no Testing Participant shall have liability for any loss or damage to the equipment unless and to the extent that such loss or damage arose as a result of that Testing Participant's breach of this Code.

5.11 Where test SM WAN connection equipment is to be installed at a Testing Participant's premises, the Testing Participant shall:

(a) provide a suitably prepared area, with suitable power feeds prior to the installation of any equipment by the DCC, as specified by the DCC as part of the site survey ahead of an order being confirmed;

(b) provide a dedicated phone connection over which an ADSL connection can be established to the data centre for the relevant CSP Region, as required, which enables transmission of data between the Testing Participant's test laboratory and the DCC; and

(c) carry out routine inspection of the equipment supplied by the DCC and maintenance of the environment in which the equipment is located.

5.12 The Testing Participant shall be entitled to and shall only use the connection to the test SM WAN for the purposes of undertaking the tests set out in Section H14.31 and shall not use it for any other purpose.

Maintenance and Removal of Test SM WAN Connection Equipment

5.13 The DCC shall undertake the following in relation to the test SM WAN connection equipment that the DCC provides:

(a) provide remote assistance to the Testing Participant to diagnose faults with any connection to the test SM WAN, including faults with any test SM WAN connection equipment supplied by the DCC;

(b) rectify any faults with the connection to the test SM WAN, including faults with any test SM WAN connection equipment supplied by the DCC;

(c) provide ongoing configuration management of test SM WAN connection equipment; and

(d) manage and implement firmware and hardware upgrades associated with the test SM WAN connection equipment.

5.14 The Testing Participant, at whose premises the test SM WAN connection equipment is (or is to be) installed, shall provide the DCC with such access to that premises as the DCC may reasonably require in order to allow it to undertake the installation, maintenance or removal of the test SM WAN connection equipment. The DCC shall ensure that all persons exercising such rights of access do so in compliance with the site rules and reasonable instructions of the Testing Participant.

5.15 A Testing Participant using its own test laboratory shall meet all applicable security requirements that are set out in this Enduring Testing Approach Document when accessing and using the Testing Services from that laboratory.

5.16 Where the Testing Participant notifies the DCC that it no longer requires the connection to the test SM WAN (on not less than 1 month's prior notice), then the DCC shall within 30 days of that notice period ending, remove the test SM WAN connection equipment from the relevant premises in accordance with Good Industry Practice and all applicable Laws and Directives.

5.17 In the event that test SM WAN connection equipment is not removed within 30 days, the Testing Participant may dispose of that equipment and shall notify the DCC at least 5 days prior to disposing of the test SM WAN connection equipment, provided that the DCC shall have the right to remove the equipment prior to the end of that 5 day period.

Appendix K

SMKI and Repository Test Scenarios Document

Contents

1 Introduction 2
1.1 Purpose 2
2 Scope 3
3 Test Preparation 4
4 Test Sequence 5
5 SREPT Procedure 6
5.1 Overview 6
5.2 SMKI & Repository Entry Process Testing 6
5.3 SREPT Initiation 10
5.4 SCREP Execution 15
5.5 SREPT Completion 19
5.6 SREPT Regression Testing 21
6 Appendix A: Test Artefacts 22
6.1 Relevant Party or RDP Documents & Reports 23
7 Appendix B: Test Data 31
8 Appendix C: Test Scenarios 32
8.1 SMKI & Repository Entry Process Test Scenarios with DCC Gateway Connection 32
8.2 SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection 42
9 Appendix D: Forms and Templates 46
9.1 Party / RDP Notification of Intention to Undertake Testing Template 47
9.2 DCC Acknowledgement of Intention to Undertake Testing Template 48
9.3 Test Readiness Report Template 50
9.4 Test Plan Template 54
9.5 Test Execution Dashboard Template 56
9.6 Test Completion Report Template 59
10 Appendix E: Test Completion Certificate 62
11 Appendix F: Definitions 64
12 Appendix G: Testing Issue Severity Descriptions 67

1 Introduction

1.1 Purpose

The purpose of this document is to:

- define the procedural steps to be undertaken by a Party or RDP wishing to complete the SMKI and Repository Entry Process Tests (SREPT).Section H14.23 requires those tests to be undertaken in accordance with the SMKI and Repository Test Scenarios Document;
- set out the SMKI and Repository Entry Process Tests that a Relevant Party or RDP must successfully complete in order to be entitled to apply to become an Authorised Subscriber or access the SMKI Repository in accordance with Section L7.1.
- describe the role and responsibilities with regard to the conduct of SREPT including in:
    - Entry and exit requirements;
    - Defining Test Scripts;
    - Defining Test Data;
    - Planning the manner in which tests will be undertaken;
    - Executing the tests;
    - Reporting the results of those tests to the DCC for approval; and
    - Performing regression testing where required.

2 Scope

Section 5 of this document sets out which Test Scenarios a Relevant Party or RDP must successfully complete, depending upon:

- which SMKI Interface or SMKI Repository Interface the Relevant Party or RDP will access and whether this is for Device or Organisation Certificates; and

- whether access to the SMKI Interface will be through a DCC Gateway Connection or using the SMKI Portal interface via the Internet.

Section 8 Appendix C: Test Scenarios of this document sets out the SMKI and Repository Entry Process Test Scenarios as referred to in Section H14.22.

3 Test Preparation

The Enduring Test Approach Document sets out rights and obligations relating to gaining Test Certificates.

Parties or RDPs wishing to undertake SREPT must comply with the security requirements applicable to Testing Participants set out in the Enduring Testing Approach Document.

To gain access to the test systems to undertake SREPT, as set out in the Enduring Testing Approach Document, the following activities must take place:

- the applicant organisation must have completed the procedure to verify the organisational identity for testing purposes;
- an applicant organisation must have at least one test SMKI Senior Responsible Officer (SMKI SRO) appointed for test purposes;
- an applicant organisation must have at least one test SMKI Authorised Responsible Officer (SMKI ARO) appointed for test purposes; and
- the procedure for provision of test credentials to SMKI AROs for accessing test SMKI Services and/or test SMKI Repository Services must have been completed.

4 Test Sequence

A Relevant Party or RDP may undertake the Test Scenarios set out in this document in any order.

5 SREPT Procedure

5.1 Overview

This section describes the procedure that must be completed in order for a Relevant Party or RDP to complete SREPT.

5.2 SMKI & Repository Entry Process Testing

The matrices in Table 1 SREPT Matrix – DCC Gateway Connection and Table 2 SREPT Matrix – No DCC Gateway Connection, below, provide a mapping to determine which test scenarios described in this document a Relevant Party or RDP must undertake. The column 'SMKI RAPP Ref' is used to determine which tests should be performed, based on the interfaces the Relevant Party or RDP wishes to use to access the SMKI and/or Repository Services and whether they wish to subscribe for Organisation and/or Device Certificates.

Detailed test scenarios identified to support the SREPT process are listed in section 8.1 SMKI & Repository Entry Process Test Scenarios with DCC Gateway Connection and section 8.2 SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection.

5.2.1 Test Scenarios for Parties or RDPs with a DCC Gateway Connection

Test Scenario Reference	Test Scenario Title	DCC (DCC Service Provider)	Supplier	RDP	Non-Supplier Party	SMKI RAPP Ref
SMKI 02	Access the test SMKI Service, through the SMKI Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.1 5.4.2
SMKI 03	Access the test SMKI Service, through the Ad Hoc Device CSR Web Service Interface and the Batched Device CSR Web Service interface, over a DCC Gateway Connection	✓	✓		✓*	5.4.3 5.4.4
SMKI 05	Access the test SMKI Repository through the SMKI Repository Portal interface over a DCC Gateway	✓	✓	✓	✓	5.4.5

	Connection					
SMKI 06	Access the test SMKI Repository via the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.6
SMKI 07	Access the test SMKI Repository through the SSH File Transfer Protocol (SFTP) interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.7
SMKI 22	Submit Organisation Certificate Signing Requests and receive Organisation Certificates, through the SMKI Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.1
SMKI 23	Submit a Device Certificate Signing Request and receive a Device Certificate through the SMKI Portal interface over a DCC Gateway Connection	✓	✓		✓*	5.4.2
SMKI 24	Submit Batched Device Certificate Signing Request and receive Device Certificates through the SMKI Portal interface over a DCC Gateway Connection	✓	✓		✓*	5.4.2
SMKI 25	Submit a Device Certificate Signing Request and receive Device Certificate through the Ad Hoc Device Web Service interface over a DCC Gateway Connection	✓	✓			5.4.3
SMKI 29	Download a copy of all 'In Use' SMKI Test Certificates from the test SMKI Repository through the SFTP (SSH File Transfer Protocol) interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.7
SMKI 30	Download a daily delta file of SMKI Test Certificates through the SFTP interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.7
SMKI 31	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.5
SMKI 32	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.6
SMKI 33	Query the test SMKI Repository for Device Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓		✓	5.4.5
SMKI 34	Query test SMKI Repository for Device Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection	✓	✓		✓	5.4.6
SMKI 48	Obtain the latest Organisation CRL and Organisation ARL through the SMKI Repository Portal interface over a DCC Gateway Connection	✓	✓	✓	✓	5.4.5
SMKI 50	Obtain the latest Organisation CRL and Organisation ARL through using the URL to the SMKI Repository over a DCC Gateway Connection	✓	✓	✓	✓	5.4.6
SMKI 57	Submit a Batched Device Certificate Signing Request and receive Certificates for Devices through the	✓	✓		✓*	5.4.4

	Batched Device CSR Web Service interface over a DCC Gateway Connection					

Table 1 SREPT Matrix - DCC Gateway Connection

Key

✓ Applicant organisation required to undertake this test if they wish to receive credentials for this service / access to this interface

✓* Applicant organisation required to undertake this test if they wish to access to this interface and can provide reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises

5.2.2 Test Scenarios for Parties without a DCC Gateway Connection

SMKI SRTSD Scenario Reference	Headline Scenario Title	Supplier	Non-Supplier Party	SMKI RAPP Ref
SMKI 04	Access the test SMKI Services for (i) Organisation Certificates and (ii) Device Certificates, through the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1 5.4.2
SMKI 08	Submit Requests for Repository Content using the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1 5.4.2
SMKI 26	Submit Organisation Certificate Signing Request (CSR) and receive Organisation Certificates through the SMKI Portal interface over the internet	✓	✓	5.4.1
SMKI 27	Submit a Device Certificate signing Request (CSR) through the SMKI Portal interface over the internet	✓	✓*	5.4.2
SMKI 28	Submit a Batched Certificate Signing Request (Batched SCR) through the SMKI Portal interface over the internet	✓	✓*	5.4.2
SMKI 38	Download Organisation Certificates and OCA Certificates through the SMKI Portal interface over the internet	✓ ✓	✓ ✓*	5.4.1 5.4.2

Table 2 SREPT Matrix - No DCC Gateway Connection

Key

✓ Applicant organisation required to undertake this test if they wish to receive credentials for this service / access to this interface

✓* Applicant organisation required to undertake this test if they wish to access to this interface and can provide reasonable evidence to suggest that it is necessary for the applicant organisation to become an Authorised Subscriber for Device Certificates in order for them to carry out business processes that will, or are likely to, lead to the installation of Devices in premises

5.3 SREPT Initiation

Each Relevant Party or RDP and the DCC shall each take reasonable steps~~each use reasonable endeavours~~ to comply with the timescales that are set out within the procedures in Table 3, Table 4 & Table 5.

In the event that a Relevant Party or RDP does not comply with the timescales in Table 3, Table 4 & Table 5, the DCC will reschedule subsequent activities to occur as soon as is reasonably practicable thereafter and for such purposes the DCC may reschedule that Relevant Party or RDP's test execution date.

5.3.1 Procedural Steps

The table below sets out the steps that must be undertaken prior to initiation of the SREPT by both the DCC and the Relevant Party seeking to undertake SREPT and the timeframes within which such steps must be completed

5.3.1.1	60 Working Days (WD) prior to commencement of SREPT	Notify intention to undertake SREPT	Relevant Party or RDP	DCC	Party / RDP notification of intention to undertake testing • Party / RDP id (s) • Confirmation that notification provided to SECAS, User Role(s) • Test start date • Identity of Test Manager and contact details	By email as attachments
5.3.1.2	Within 2 WD of receipt of the notification under 5.3.1.1	Acknowledge request	DCC	Relevant Party or RDP	Confirmation of Party / RDP notification: • Party / RDP id (s) • Test start date	By email as attachments

					• DCC Test Manager contact • Date for SREPT initiation meeting	
5.3.1.3	Within 5 WD of receipt of the notification under 5.3.1.2	Conduct SREPT Initiation Meeting	DCC	Relevant Party or RDP	DCC to provide guidance information on conducting SREPT including a guide to the SMKI and Repository	Meeting
5.3.1.4	In each week occurring within the period from 40 WD prior to start of testing	Provide progress report, demonstrating readiness to begin tests	Relevant Party or RDP	DCC	Test Readiness Report	By email as attachments
5.3.1.5	25 WD prior to start of testing	Provide test artefacts to support conduct of SREPT	Relevant Party or RDP	DCC	• Test Plan incorporating the Test Schedule • Requirements Traceability Matrix (see section 6.1.6) • Test Scripts (see section 6.1.7) • Test Data Plan (see section 7)	By email as attachments
5.3.1.6	By 20 WD prior to start of testing	DCC complete review of test artefacts	DCC	Relevant party or RDP	Details regarding any deficiencies in the test artefacts and where necessary, a revised start date for testing provided - continue from 5.3.1.7 Or, confirmation that the DCC has accepted the test artefacts - continue from 5.3.1.9	By email as attachments
5.3.1.7	By 10 WD prior to start	Party / RDP to	Relevant	DCC	Revised documents	By email as

	of testing	provide revised documents	Party or RDP			attachments
5.3.1.8	B 7 WD prior to start of testing	DCC complete review of revised test artefacts	DCC	Relevant Party or RDP	Details regarding any deficiencies in the test artefacts and a revised start date for testing provided where agreed it is necessary - Regress and continue from 5.3.1.7 Or confirmation that test artefacts accepted - continue from 5.3.1.9	By email as attachments
5.3.1.9	By 5 WD prior to start of testing	1 Review Test Readiness Report and confirm the Entry Criteria for commencing testing in relation to Relevant Party or RDP have been met 2 Confirm Start Date and Test Schedule for execution of tests by Relevant Party or RDP	DCC Quality Gate meeting	Relevant Party or RDP	Source: Test Readiness Report, Test Schedule Output: Confirmation of Relevant Party or RDP readiness to proceed	Quality Gate Review Meeting
	If there is any outstanding documentation presented at the Quality Gate Review, the DCC shall assess it as part of its assessment of the Entry Criteria under clause 5.3.2					

Table 3 SREPT Initiation: Procedural Steps

5.3.2 SREPT Entry Criteria

Each Relevant Party or RDP wishing to undertake SREPT must comply with (and, where specified below, shall provide evidence of complying with) the following criteria prior to entry into SREPT:

- the interfaces that the Relevant Party or RDP wishes to access must have been identified to determine the SMKI & Repository Entry Process Tests that are to be undertaken;
- all relevant test artefacts (as set out in sections 5.3.1.1, 5.3.1.4 and 5.3.1.5) must have been produced by the Relevant Party or RDP and accepted by the DCC. This includes:
    - Party / RDP Notification of Intention to Undertake Testing
    - Test Readiness Report
    - Test Plan incorporating the Test Schedule
    - Requirements Traceability Matrix
    - Test Scripts
    - Test Data Plan
- have provided evidence that an appropriate test environment and an appropriate level of resources available to support the SREPT process; and
- confirm that the security requirements set out in the Enduring Testing Approach Document have been met.

Where the DCC reasonably believes that the Relevant Party or RDP has not met the Entry Criteria, the DCC may:

- prevent the Relevant Party or RDP from undertaking SREPT until such time as the DCC reasonably believes that the Relevant Party or RDP meets the Entry Criteria (and in which case DCC shall inform the Relevant Party or RDP why it believes that they have not met the Entry Criteria); and
- reschedule the test start date for the Relevant Party or RDP. In doing so, the DCC shall provide the earliest practicable alternative date; or
- provide provisional approval of the Test Readiness Report (and approval to proceed) with an understanding that the outstanding documentation will be provided before the start of testing, otherwise testing will not commence.

Pursuant to Section H14.25, where the DCC does not reasonably believe that a Relevant Party or RDP meets the Entry Criteria to commence testing, the Relevant Party or RDP may refer the matter to the Panel. Where the Panel determines that the Relevant Party or RDP has met the Entry Criteria, the DCC shall schedule the start of testing as soon as reasonably practicable thereafter.

SREPT shall only commence when DCC has successfully completed Part 1 of SMKI and Repository Testing.

5.4 SCREP Execution

5.4.1 Procedural Steps

The table below sets out the steps that must be undertaken prior to or during test execution by either the DCC or a Relevant Party or RDP seeking to undertake SREPT and the timeframes within which such steps must be complete as set out in the Test Schedule which will be updated by the Relevant Party or RDP from time to time to reflect test progress.

5.4.1.1	SREPT Start Date or earlier (if appropriate)	Verification of Organisation Identity and appointment of, SMKI SRO and SMKI ARO for test purposes	Relevant Party or RDP	DCC	Submission of relevant forms	As per Enduring Testing Approach Document
5.4.1.2	SREPT Start Date or earlier (if appropriate)	Carry out checks such that the Relevant Party or RDP has at least one test SMKI SRO and at least one test SMKI ARO. Confirm with Relevant Party or RDP.	DCC	Relevant Party of RDP	Confirm Organisation Identity is verified and test SMKI ARO and test SMKI SRO Registration is complete. Grant approval to execute SREPT scenarios and which scenarios will be undertaken	As per Enduring Testing Approach Document
5.4.1.3	In accordance with Test Schedule and 5.4.1.2 completed	Conduct SREPT	Relevant Party or RDP		Approved test artefacts	As per test artefacts
5.4.1.4	Daily Basis, or alternative schedule agreed with DCC	Provide daily progress report using the template	Relevant Party or RDP	DCC	Test execution dashboard and Daily Testing Issue Report	By email as attachment

		provided to DCC				
5.4.1.5	SREPT execution complete	Provide Test Completion report	Relevant Party or RDP	DCC	SREPT completion report including: details of Test Scrimps executed and Testing Issues resolved (ass section 9.6)	

Table 4 SREPT Execution: Procedural Steps

5.4.2 SREPT Test Suspension/Resumption

During the execution of tests the DCC, Relevant Party or RDP each have the right to suspend testing where it reasonably considers that this is necessary.

Testing will only recommence when agreed by both the DCC and the Relevant Party or RDP subject to the suspension.

5.4.2.1 Possible Suspension Criteria

Reasonable grounds for suspension of testing may include any of the following;

- Application components are not available as scheduled
- A Testing Issue prevents further useful testing from proceeding
- A significant percentage of planned Test Scripts for a given day fail, taking Testing Issue severity and volume of tests into consideration which would generate root cause analysis to be undertaken to establish the cause. Testing Issues trending should also be used to determine any recommendation. The outcome of any root cause analysis activity may result in testing being suspended
- Test Scripts to be executed are in a “blocked” status due to an identified Testing Issue
- The Relevant Party or RDP has failed to comply with the procedural steps for executing SREPT

5.4.2.2 Test Resumption Criteria

Where testing has been suspended, either the DCC or the Relevant Party or RDP as appropriate shall produce a test suspension report reflecting the cause of the suspension, and what actions are to be taken by whom and when in order for testing to resume – the ‘Test Resumption Criteria’. The DCC and the Relevant Party or RDP shall take reasonable steps to support each other to achieve the Test Resumption Criteria.

Testing will only resume once the DCC or Relevant Party or RDP has demonstrated to the other Party’s satisfaction that the Test Resumption Criteria have been met.

5.4.2.3 Disputes regarding Test Suspension/Resumption

Each of the DCC and the Party or RDP undertaking the SMKI and Repository Entry Process Tests may suspend testing in accordance with the requirements set out above. Any dispute between the DCC and a Party or the RDP regarding the suspension (or consequent resumption) of such testing may be referred to the Panel for its determination. Where the DCC or the Party or RDP disagrees with any such determination of the Panel, then the DCC or the Party or RDP may refer the matter to the Authority for its determination (which determination shall be final and binding for the purposes of this Code).

Where a dispute regarding the suspension/resumption of testing is made, testing will not resume whilst the dispute is being heard by the Panel, and/or until the Test Resumption Criteria are met by the DCC or the Relevant Party or RDP.

5.5 SREPT Completion

5.5.1 Procedural Steps

The table below sets out the steps that must be undertaken during test completion by either the DCC or Relevant Party or RDP and the timeframes within which such steps must be complete.

5.5.1.1	Within 2 WD of receipt of the report in 5.4.1.5	Confirm receipt of notification of Test complete (Test completion report)	DCC	Relevant Party or RDP	SREPT Test Completion Report (see section 9.6)	By email
5.5.1.2	Within 2 WD of receipt of the report in 5.5.1.1	DCC review completion report and confirm that SREPT concluded or further testing required	DCC	Relevant Party or RDP	SREPT Test Completion Report and evidence as requested by DCC, 5.4.1.5 refers	Quality Gate Review meeting
5.5.1.3	Within 2 WD of successful Quality Gate Review meeting	Confirm Test Complete	DCC	Relevant Party or RDP, SMKI Registration Authority	Issue Test Completion certificate (see section 10) and provide copy to SMKI Registration Authority	By email as attachment

Table 5 SREPT Completion: Procedural Steps

Notwithstanding 5.5.1.3 above pursuant to Section H14.28 the DCC shall confirm on request by the Relevant Party or RDP whether or not it considers that the Relevant Party or RDP has successfully completed SREPT.

5.5.2 SREPT Exit Criteria

A Relevant Party or RDP must meet the following Exit Criteria prior to that Relevant Party's or RDP's completion of and exit from SREPT:

- All Tests have been executed and results have been documented by the Relevant Party or RDP and evidence captured in the Relevant Party or RDP's Test Management Tool (or other system) and provided to the DCC

- All testing issues identified during a Relevant Party's test execution have been recorded in the Test Management Tool. Of those Testing Issues either:

    - the Testing Issue generated by the Relevant Party as a result of its UEPT has been fixed and verified by retest; or

    - where outstanding, the Testing Issue has been reviewed and documented, and been included as part of a remediation plan that outlines the next steps to be taken, including estimated timescales required to resolve each of their outstanding Testing Issues. The remediation plan must be agreed by the DCC

- any outstanding Testing Issue count must not exceed those defined in **Error! eference source not found.**, below:

1	0
2	0
3	5*
4	10*
5	As agreed**

Table 6 Testing Issue Threshold

* - Work around and remediation plan to be agreed with the DCC for each issue that ensures no impact on other Users

** - As agreed with the DCC, requiring no impact on market operations

*** - Refer to Appendix G for definitions of Issue severities.

- A Test Completion Report has been created by the Relevant Party or RDP and approved by the DCC

- A Quality Gate Review meeting has been held between the Relevant Party or RDP and the DCC, with progress approved by the DCC

Pursuant to Section H14.25, where the DCC considers that a Relevant Party or RDP has not met the SREPT Exit Criteria, the Relevant Party or RDP may refer the matter to the Panel.

Where a dispute regarding whether a Relevant Party or RDP has met the SREPT Exit Criteria occurs, the SREPT Completion process will not resume whilst the dispute is being heard by the Panel, or until the SREPT Exit Criteria are met by the Relevant Party or RDP.

5.5.3 Quality Gate Review

Evidence of test completion may be requested for all or any of the tests during the Quality Gate Review, and irrespective of whether the information is reviewed, it shall be retained by the Relevant Party or RDP and may be requested by DCC at a later date.

Any remediation plan shall be discussed by the DCC and the Relevant Party or RDP and agreed as part of the evidence review.

A final decision regarding whether a Relevant Party or RDP has successfully completed SREPT will be provided to the Relevant Party or RDP no later than 2 Working Days after the date on which the Quality Gate Review meeting is held.

In addition, pursuant to Section H14.28, the DCC shall confirm on request by the Relevant Party or RDP whether or not it considers that the Relevant Party or RDP has successfully completed SREPT.

5.5.4 SREPT Test Completion Certificate

The SREPT Test Completion Certificate shall be issued by the DCC to the Relevant Party or RDP once the Quality Gate Review has concluded that the Relevant Party or RDP has met the SREPT Exit Criteria.

5.6 SREPT Regression Testing

DCC shall inform all Relevant Parties and RDPs undertaking SREPT and all Relevant Parties and RDPs that have completed SREPT of any change to DCC Systems that may affect SREPT.

Where the DCC deems that a change to DCC Systems necessitates Regression Testing, DCC may require Relevant Parties and RDPs to perform Regression Testing of the SREPT.

Where DCC does not require Relevant Parties or RDPs to perform Regression Testing, the decision as to whether Regression Testing is performed as a consequence of a change to DCC Systems or a change to User Systems, rests with the Relevant Party or RDP.

Where a Relevant Party or RDP performing Regression Testing has already completed SREPT, the SREPT Test Completion Certificate shall remain effective.

6 Appendix A: Test Artefacts

The DCC and each Relevant Party or RDP will be required to produce and maintain a number of documents, dashboards and reports during the testing lifecycle as depicted in Figure 1 Test Documentation Hierarchy, below.

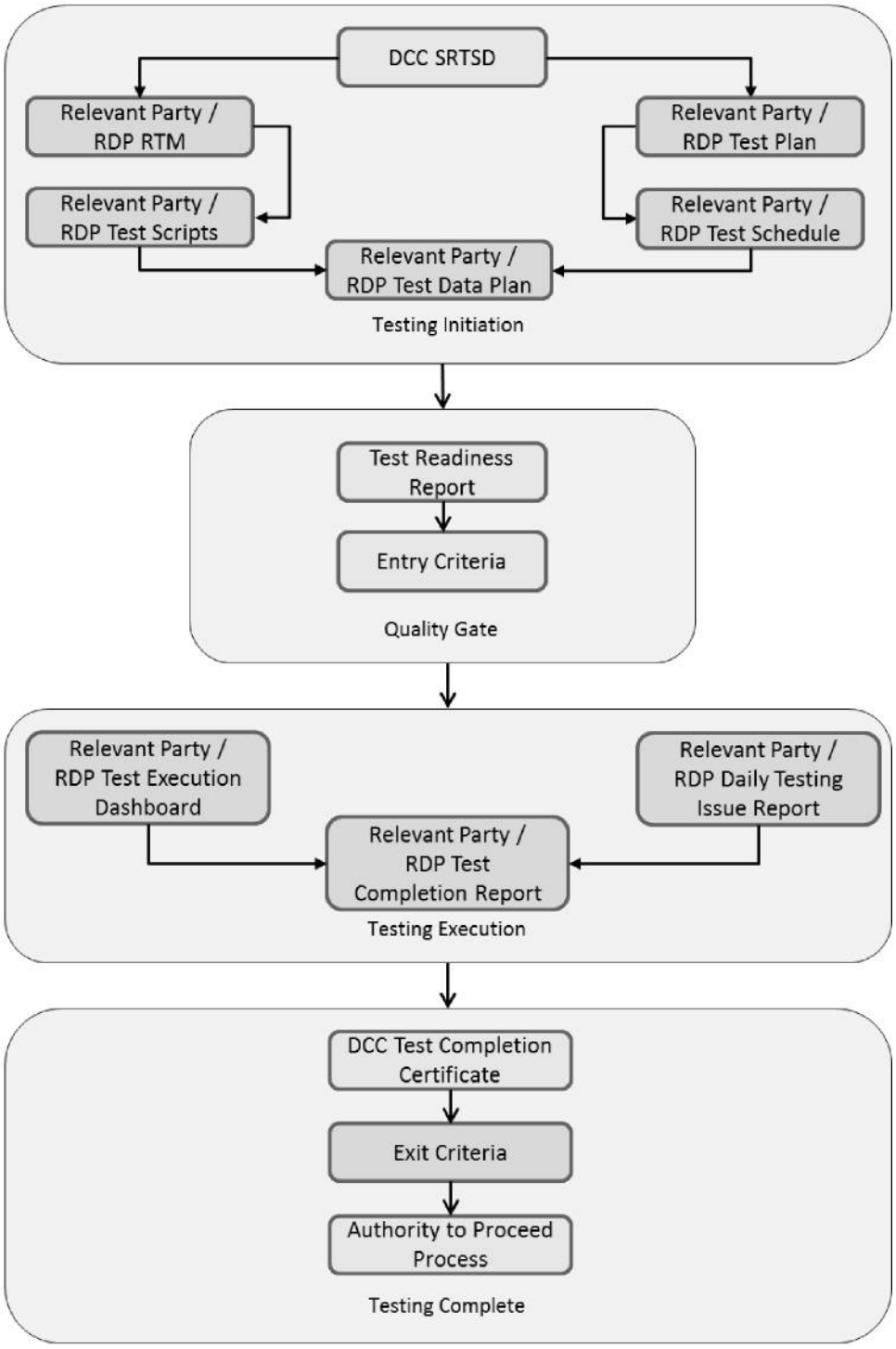

Figure 1 Test Documentation Hierarchy

6.1 Relevant Party or RDP Documents & Reports

6.1.1 Test Preparation of Document Set

The following documentation must be produced by a Relevant Party or RDP before Testing commences:

- Test Readiness Report
- Scope of SREPT testing
- Test Plan
- Test Data Plan
- Test Schedule
- Requirements Traceability Matrix
- Test Scripts
- Note regarding scope of SREPT testing: Which SREPT test scenarios need to be undertaken is determined by:
    - which SMKI Interface or SMKI Repository Interface the Relevant Party or RDP will access and whether this is for Device or Organisation Certificates; and
    - whether access to the SMKI Interface will be through a DCC Gateway Connection or using the SMKI Portal interface via the Internet.

6.1.2 Reports and Dashboard

Table 7 Test Stage Supporting Documentation Set sets out the Reports and Dashboard that a Relevant Party or RDP must produce to demonstrate progress in preparing for and executing testing.

6.1.3 Test Readiness Report (TRR)

The Test Readiness Report shall be produced by the Relevant Party or RDP

The report must be provided to the DCC by the Party or RDP on a weekly basis, commencing 40 Working Days prior to the start of Testing and must indicate progress against the following criteria:

- Previous Test Phase / Stage Exit Criteria (if appropriate)
- Relevant Party or RDP Test Management tool selected and available

- Relevant Party or RDP key RAID (Risk, Assumption, Issue and Dependency) items, including, for each key item that has the potential to cause significant disruption to the commencement and / or completion of SMKI & Repository Entry Process Testing:
    - Priority (High, Medium, Low)
    - Severities of open issues
    - Action taken
    - Target close date
    - Overall RAG status (based on progress to plan)
- Relevant Party or RDP Test Plan produced
- Relevant Party or RDP Test Schedule produced
- Relevant Party or RDP Requirements Traceability Matrix
    - Total numbers of Requirements identified
        - Total number of testable requirements documented
        - Total number of testable requirements in progress
        - Total number of testable requirements not started
    - Total number of Requirements deemed not testable
- Relevant Party or RDP Test Script complete to date – to reflect the following breakdown
        - Planned number of Test Scripts
        - Total number of Test Scripts produced to date
        - Total number of Test Scripts in progress
        - Total number of Test Scripts not started
- % Test Data readiness by Party against planned Test Scripts
- Readiness of Party or RDP Test Resources and Technical (support) Resource
- Relevant Party or RDP test environment readiness – to include
    - Security code of connection satisfied

- All interfaces required to support testing

- Overall RAG status (based on likelihood of starting to plan)

6.1.4 Test Execution Dashboard

The Test Execution Dashboard will identify the Relevant Party or RDP's progress when executing testing and will be provided in a format specified by the DCC. The dashboard must be updated by the Relevant Party or RDP and provided to the DCC on a daily basis once testing commences, or per an alternative schedule agreed with the DCC.

The dashboard will include the following details:

- Name of Relevant Party or RDP, Party or RDP ids under test;

- Location of Relevant Party or RDP testing;

- Date and time test execution dashboard updated by Relevant Party or RDP;

- Total number of tests Relevant Party or RDP scheduled for execution and projected as a test execution glide path;

- Actual number of tests executed by Relevant Party or RDP to date reflected on an incremental daily count including test results (passed, failed, blocked, not run, Ready for Test);

- Relevant Party or RDP summary of Testing Issues to include:

    - Total number of Testing Issues generated

        - Counts by status Open, Fixed, Closed etc.

        - Counts by Severity 1, 2, 3 etc.

        - Counts by Priority

        - Escalated to Issue Resolution Board (IRB).

- Relevant Party or RDP Regression Test execution results;

- Relevant Party or RDP summary progress against Exit Criteria;

- Relevant Party or RDP top 5 risks and issues – to include any environment concerns; and

- Relevant Party or RDP overall RAG status (based on progress against testing schedule)

6.1.5 Test Completion Report

The Relevant Party or RDP shall produce a Test Completion Report and submit the draft to the DCC 10 working days prior to the test completion date or at such time as agreed between DCC and the Party or RDP. The finalised version of the Test Completion Report will be submitted to the DCC on completion of each test execution activity.

A Test Completion Report template will be provided by the DCC to ensure that all Relevant Party or RDP reports contain the same level of detail. The report will include:

- Relevant Party or RDP Test approach and Scope of Testing Undertaken
- Details of updates made to the test environment during the course of testing;
- Relevant Party or RDP Summary of the Test Results
- Total number of tests originally scheduled for execution
- Total number of tests executed
- A table of tests run to include:
    - Overall results achieved
        - Passed, Failed, Blocked, Not Run
- Any tests not run, blocked or not successfully executed end to end must be supported by an explanation.
- Relevant Party or RDP Summary of Testing Issues
    - Total number of Testing Issues generated
    - Total counts by status Open, Fixed, Closed
    - Total counts by Severity

6.1.6 Test Traceability

To provide the DCC with a sufficient level of test assurance, all tests executed by each Relevant Party or RDP undertaking SREPT will be required to demonstrate full traceability as follows:

- Each requirement captured in the Requirements Traceability Matrix that can be tested during SREPT must be linked to one or many Test Scripts
- Each Test Script executed must be reflected in one or many test execution cycles
- A record of each test executed and the results of that test
- Where an executed test generates a Testing Issue;

- Each Testing Issue must be linked to the test that generated the Testing Issue
- Any subsequent retesting to validate a fix of Testing Issue carried out must be linked to the Testing Issue
- Each retest executed must reflect a result achieved as a result of execution

6.1.7 Test Scripts

A Relevant Party or RDP shall develop its own test scripts and demonstrate how those test scripts meet the requirements in accordance with H14.26.

No	Phase	Description	DCC Responsibility	Relevant Party or RDP Responsibility	When/Frequency	Entry Criteria	Exit Criteria	Sign-Off Authority
1	Initiation	Guide to the SMKI and Repository Entry Process Tests	Produce and maintain	None	Prior to commencement of SREPT	N	N	DCC
2	Initiation	Test Data Plan (Device CSRs)	Produce	Use, if required	Prior to commencement of SREPT	N	N	DCC
3	Initiation	Test Plan including Test Schedule	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
4	Initiation	Requirements Traceability Matrix	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	Y	DCC
5	Initiation	Test Scripts	Review and Approve	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage	Y	Y	DCC

No	Phase	Description	DCC Responsibility	Relevant Party or RDP Responsibility	When/Frequency	Entry Criteria	Exit Criteria	Sign-Off Authority
					Exit Quality Gate			
6	Initiation	Test Data Plan	Review	Produce and maintain	Test Stage Entry Quality Gate and updated during execution as required in preparation for Test Stage Exit Quality Gate	Y	N	DCC
7	Initiation	Test Readiness Review Checklist	Provide Template Review and Approve	Produce and maintain	Test Stage Entry Quality Gate	Y	N	DCC
8	Initiation	Test Stage Entry Criteria (part of final Test Readiness Report)	Review and Approve	Produce	Test Stage Entry Quality Gate	Y	N	DCC
9	Execution	Test Execution Dashboard	Review	Produce and maintain	Produced and updated daily (or other schedule agreed with the DCC) during execution in preparation for Test Stage	N	Y	DCC

No	Phase	Description	DCC Responsibility	Relevant Party or RDP Responsibility	When/Frequency	Entry Criteria	Exit Criteria	Sign-Off Authority
					Exit Quality Gate			
10	Execution	Testing Issue Report (part of the Test Execution Dashboard)	Review	Produce and maintain	Produced and updated daily (or other schedule agreed with the DCC) during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
11	Execution	Test Completion Report	Provide Template Review and Approve	Produce and file	Test Stage during execution in preparation for Test Stage Exit Quality Gate	N	Y	DCC
12	Execution	Test Stage Quality Gate Exit Criteria (part of Test Completion Report)	Review and Approve	Produce	Test Stage Exit Quality Gate	N	Y	DCC

Table 7 Test Stage Supporting Documentation Set

Once these steps are complete the DCC will issue a Test Completion Certificate (see section 10).

7 Appendix B: Test Data

A Test Data Plan will be developed by the Relevant Party and coordinated with DCC in accordance with Section 5.4.1.3. The DCC and Relevant Party will be responsible for set up of Test Data on their respective system which must be defined in the Relevant Party Test Data Plan. The Data defined will be based on the following principles;

- No personal data which identifies any individual will be used for testing, but anonymised live Data is acceptable
- Test Data will be representative of data likely to be used in the live environment once the Relevant Party is eligible in the relevant User Role
- A full range of Test Data covering all services to be tested will be used

The DCC shall ensure that data supplied by the DCC for the purposes of testing is segregated when testing is being conducted by multiple Relevant Parties.

Table 8 Test Data Responsibilities below outlines the responsibilities in regard to preparing Test Data required to support UEPT.

Test Data Preparation	DCC Licensee, Relevant Party or RDP	DSP

Table 8 Test Data Responsibilities

The DCC shall not provide the Relevant Party or RDP with either IKI or Organisation Certificate Signing Requests (CSRs). Instead, a Relevant Party or RDP shall provide sufficient test data to be able to demonstrate its capability to produce CSRs for test Organisation Certificates in accordance with ETAD. The DCC shall provide Device CSRs for those Parties who are not able to provide their own to be able to undertake Device-related SMKI Interface testing.

8 Appendix C: Test Scenarios

8.1 SMKI & Repository Entry Process Test Scenarios with DCC Gateway Connection

The following sub sections contain the SMKI & Repository Entry Process Test Scenarios that are applicable to each prospective user of SMKI & Repository Services that have access to a DCC Gateway Connection.

8.1.1 Security Credentials Access Tests for Test SMKI Service

Title:	Access the test SMKI Service, through the SMKI Portal interface over the DCC Gateway Connection
Description	A Party / RDP's SMKI Authorised Responsible Officer (SMKI ARO) accesses the Test SMKI Service, through the SMKI Portal interface via the DCC Gateway Connection, using the security credentials supplied by the DCC.
Objective	• To prove that the SafeNet[1] Client Installed on the SMKI ARO's computer validates their security credentials • To prove that a Party / RDP's ARO can use the FIPS Token which is registered to them and their organisation when accessing the SMKI Portal interface via the DCC Gateway Connection for Organisation and / or Device Certificates (as required)

Title:	Access the test SMKI Service, through the Ad Hoc Device CSR Web Service interface and the Batched Device CSR Web Service interface, over a DCC Gateway Connection

[1] The DCC makes available to PKI Client software (SafeNet Client), as set out in section 2.3.1 of the SMKI Code of Connection.

Description	A Party System using the IKI security credentials supplied by the DCC accesses the Test SMKI Services, through the Ad Hoc Device CSR Web Service interface and the Batched Device CSR Web Service interface over a DCC Gateway Connection
Objective	• To prove that the Party can access the Test SMKI Service through the Ad Hoc Device CSR Web Service interface and Batched Device CSR Web Service interface, as required, using the relevant IKI credentials. • To prove IKI credentials correctly authenticate to the SMKI Device Web Service interfaces.

8.1.2 Security Credentials access Tests to the test SMKI Repository

Title:	Access the test SMKI Repository through the SMKI Repository Portal interface over a DCC Gateway Connection
Description	A Party / RDP's SMKI aRO uses their individual IKI security credentials to access the test SMKI Repository through the SMKI Repository Portal interface
Objective	• To prove access for the Party / RDP's ARO to the test SMKI Repository using the SMKI Repository Portal interface using the SMKI URL, username and password

Title:	Access the test SMKI Repository via the SMKI Repository Web Service interface over a DCC Gateway Connection
Description	The Party's system uses the API Key issued by the DCC to access the test SMKI Repository using the SMKI Repository Web Service interface
Objective	• To prove that the Party's system can access the test SMKI Repository using the SMKI Repository Web Service

	interface

Title:	Access the test SMKI Repository through the SSH File Transfer Protocol (SFTP) interface over a DCC Gateway Connection
Description	The Party / RDP's system or ARO uses the security credentials provided by the DCC to access the test SMKI Repository through the SMKI Repository SFTP (SSH File Transfer Protocol) interface
Objective	• To prove that the Party / RDP's system or ARO can access the test SMKI Repository through the SMKI Repository SSH (Secure File Transfer Protocol) interface

8.1.3 Submission of CSR and Receipt of Certificates

Title:	Submit Organisation Certificate Signing Requests and receive Organisation Certificates through the SMKI Portal interface over a DCC Gateway Connection
Description	A Party / RDP's SMKI Authorised Responsible Officer (SMKI ARO) submits an Organisation Certificate Signing Request (CSR) and receives an Organisation Certificates for that CSR through the SMKI Portal interface
Objective	• To prove a Party / RDP can generate and submit an Organisation CSR in the format specified in the SMKI Interface Design Specification • To prove that a Party / RDP can download Organisation Certificates issued in respect of the submitted CSRs, and to confirm the information contained in the issued Organisation Certificate is consistent with the information contained within the corresponding CSR • To prove that an Organisation Certificate can be rejected by the Party / RDP (according to the mechanism set

	out in the SMKI RAPP and / or specified in the SMKI Interface Design Specification)

Title:	Submit a Device Certificate Signing Request and receive a Device Certificate through the SMKI Portal interface over a DCC Gateway Connection
Description	A Party's SMKI ARO submits a Device Certificate Signing Request (CSR) and receives a Device Certificate for that Device CSR through the SMKI Portal interface
Objective	• To prove that the Party's ARO can use the SMKI Portal Interface to submit an Ad Hoc Device Certificate Signing Request • To prove that the Party can use the SMKI Portal Interface to download individual Device Certificates and confirm the information contained in the issued Device Certificate is consistent with the information contained within the corresponding submitted Device CSR • To prove that the issued Device Certificate can be rejected by the Party (according to the mechanism set out in the SMKI RAPP and / or specified in the Portal specification)

Title:	Submit Batched Device Certificate Signing Requests and receive Device Certificates through the SMKI Portal interface over a DCC Gateway Connection
Description	A Party's SMKI ARO submits a Batched Device Certificate Signing Request (CSR) and receives Device Certificates for each valid Device CSR through the SMKI Portal interface
Objective	• To prove that the Party's ARO can use the SMKI Portal Interface to submit Batched Device CSR

	• To prove that Device CSRs are batched correctly by the Party • To prove that the Party can use the SMKI Portal Interface to download Device Certificates issued from the Batched Device CSRs • To prove that the issued Device Certificates are also lodged in the test SMKI Repository

Title:	Submit a Device Certificate Signing Request and receive Device Certificate through the Ad Hoc Device Web Service interface over a DCC Gateway Connection
Description	A Party's system submits a Device Certificate Signing Request (CSR) and receives a Device Certificates through the Ad Hoc Device Web Service interface
Objective	• To prove that the Party's system can submit a Device CSR through the Ad Hoc Device Web Service interface • To prove that the Party can receive Device Certificates issued in respect of the submitted Device CSR from the Ad Hoc Device Web Service • To prove that the issued Device Certificate is lodged in the test SMKI Repository

Title:	Submit Batched Device Certificate Signing Requests and receive Device Certificates through the Batched Device Web Service interface over a DCC Gateway Connection

[2] Subject to delivery of the Change Request to deliver this functionality.

Description	A Party's system submits Batched Certificate Signing Requests (CSRs) and receives Device Certificates through the Batched Device CSR Web Service interface
Objective	• To prove that the Party's system can use the Batched Device Web Service Interface to submit Batched Device CSRs • To prove that Device CSRs are batched correctly by the Party • To prove that Parties can download their Device Certificates issued in respect of Batched Device CSRs • To prove that the issued Device Certificates are also lodged in the test SMKI Repository

8.1.4 Download Certificates from the test SMKI Repository

Title:	Download a copy of all 'In Use' SMKI Test Certificates from the test SMKI Repository through the SFTP (SSH File Transfer Protocol) interface over a DCC Gateway Connection
Description	Using a file transfer client the Party downloads a copy of all in use SMKI Certificates from the test SMKI Repository via SFTP (SSH File Transfer Protocol) interface
Objective	• To prove that the Party / RDP can use a file transfer client that supports SFTP in accordance with the standards in the SMKI Repository Interface Design Specification to access the SFTP interface • To prove that the Party / RDP's file transfer client can download a complete copy of all in use Certificates (including OCA and DCA Certificates)

Title:	Download a daily delta file of SMKI Test Certificates through the SFTP interface over a DCC Gateway Connection
Description	Using a file transfer the client the Party / RDP downloads a partial / daily "delta file" copy of all SMKI Certificates issued in the preceding twenty four hours from the test SMKI Repository via SFTP (SSH File Transfer Protocol) interface
Objective	• To prove that the Party / RDP's file transfer client can download a partial/"Daily Delta File" batch containing Certificates published to the test SMKI Repository during the preceding twenty four hours (including OCA and DCA Certificates)

8.1.5 Query the test SMKI Repository and Retrieve Certificates

Title:	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection
Description	A Party / RDP's SMKI ARO uses the SMKI Repository Portal Interface to query the test SMKI Repository for an Organisation Certificate and downloads the Organisation Certificate
Objective	• To prove the Party / RDP's ARO is able to use the SMKI Repository Portal Interface • To prove that the Party / RDP's ARO can query the test SMKI Repository using the SMKI Repository Portal interface to locate an Organisation Certificate in the test SMKI Repository • To prove a Party / RDP's ARO is able to download the located Organisation Certificate

Title:	Query the test SMKI Repository for Organisation Certificates through the SMKI Repository Web Service interface over a

	DCC Gateway Connection
Description	A Party / RDP's system queries the test SMKI Repository for an Organisation Certificate via the SMKI Repository Web Service interface and retrieves the Organisation Certificate
Objective	• To prove the Party / RDP's system is able to use the SMKI Repository Web Service • To prove that the Party / RDP's system can query the test SMKI Repository using the SMKI Repository Web Service interface to locate an organisation Certificate in the test SMKI Repository • To prove the Party / RDP's system can receive the located Organisation Certificate

Title:	Query the test SMKI Repository for Device Certificates through the SMKI Repository Portal interface over a DCC Gateway Connection
Description	A Party's SMKI ARO uses the SMKI Repository Portal Interface to query the test SMKI Repository for a Device Certificate and downloads the Device Certificate
Objective	• To prove the Party's ARO is able to use the SMKI Repository Portal Interface (if not already done as part of SMKI 31) • To prove that the Party's ARO can query the test SMKI Repository using the SMKI Repository Portal interface to locate a Device Certificate in the test SMKI Repository • To prove a Party's ARO is able to download the located Device Certificate

Title:	Query test SMKI Repository for Device Certificates through the SMKI Repository Web Service interface over a DCC Gateway Connection
Description	A Party's system queries the test SMKI Repository for a Device Certificate via the SMKI Repository Web Service interface and retrieves an Device Certificate
Objective	• To prove the Party's system is able to query the test SMKI Repository to determine the presence of a Device Certificate in the test SMKI Repository • To prove a Party's system can retrieve the located Device Certificate

8.1.6 Obtain Organisation Certificate Revocation List and Organisation Authority Revocation List

Title:	Obtain the Organisation Certificate Revocation List (CRL) and Organisation Authority Revocation List (ARL) through the SMKI Repository Portal interface over a DCC Gateway Connection
Description	A Party / RDP's SMKI Authorised Responsible Officer (SMKI ARO) wishes to access the Organisation CRL and ARL using the SMKI Repository Portal interface via a DCC Gateway Connection
Objective	• To prove that a Party / RDP's SMKI ARO can access and / or download the Organisation CRL and Organisation ARL using the SMKI Repository Portal interface via DCC Gateway Connection

Title:	Obtain the latest Organisation CRL and Organisation ARL through using the URL to the SMKI Repository over a DCC Gateway Connection
Description	The Party / RDP's system accesses the test SMKI Repository using URL to obtain the latest Organisation CRL and Organisation ARL
Objective	• To prove that a Party / RDP's system can access and / or download the latest Organisation CRL and Organisation ARL using the URL to the SMKI Repository

8.2 SMKI & Repository Entry Process Test Scenarios without DCC Gateway Connection

The following sub sections contain the SMKI & Repository Entry Process Test Scenarios that are applicable to each prospective user of SMKI & Repository Services that do not have access to a DCC Gateway Connection.

8.2.1 Security Credentials Access Tests to SMKI

Title:	Access the Test SMKI Service, through the SMKI Portal interface over the internet
Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the Test SMKI Service, through the SMKI Portal interface using the security credentials supplied by the DCC
Objective	• To prove that the SafeNet Client Installed on the SMKI ARO's computer validates their security credentials • To prove that a Party's ARO can use the FIPS Token which is registered to them and their organisation when accessing the SMKI Portal interface via the internet

8.2.2 Submission of CSR and Receipt of Certificates

Title:	Submit Organisation Certificate Signing Requests and receive Organisation Certificates through the SMKI Portal interface over the internet
Description	For a Party without a DCC Gateway Connection, a SMKI ARO submits an Organisation Certificate Signing Request (CSR) and receives an Organisation Certificates for that CSR through the SMKI Portal interface over the internet
Objective	• To prove a Party can generate and submit an Organisation CSR in the format specified in the SMKI Interface

	Design Specification • To prove that a Party can download Organisation Certificates issued in respect of the submitted CSRs, and to confirm the information contained in the issued Organisation Certificate is consistent with the information contained within the corresponding CSR • To prove that an Organisation Certificate can be rejected by the Party (according to the mechanism set out in the RAPP and / or specified in the Portal specification)

Title:	Submit a Device Certificate Signing Request and receive a Device Certificate through the SMKI Portal interface over the internet
Description	For a Party without a DCC Gateway Connection, SMKI ARO submits a Device Certificate Signing Request (CSR) and receives a Device Certificate for that Device CSR through the SMKI Portal interface over the internet
Objective	• To prove that the Party's ARO can use the SMKI Portal Interface to submit an Ad Hoc Device Certificate Signing Request • To prove that the Party can use the SMKI Portal Interface to download individual Device Certificates and confirm the information contained in the issued Device Certificate is consistent with the information contained within the corresponding submitted Device CSR • To prove that the issued Device Certificate can be rejected by the Party (according to the mechanism set out in the RAPP and / or specified in the Portal specification)

Title:	Submit Batched Device Certificate Signing Requests and receive Device Certificates through the SMKI Portal interface over the internet
Description	For a Party without a DCC Gateway Connection, an SMKI ARO submits a Batched Device Certificate Signing Request (CSR) and receives Device Certificates for each valid Device CSR through the SMKI Portal interface over the internet
Objective	• To prove that the Party's ARO can use the SMKI Portal Interface to submit Batched Device CSR • To prove that Device CSRs are batched correctly by the Party • To prove that the Party's ARO can use the SMKI Portal interface to download Device Certificates issued from the Batched Device CSRs

8.2.3 Submit Requests for Repository Content and Obtain DCA, OCA and DCC Certificates

Title:	Submit Requests for and Receive Repository Content using the SMKI Portal interface over the Internet
Description	For a Party without a DCC Gateway Connection, an SMKI ARO accesses the SMKI Portal interface and makes a request for and receives content from the test SMKI Repository
Objective	• To prove that a Party's SMKI ARO can use the SMKI Portal interface to request and receive the latest Organisation CRL and latest Organisation ARL

Title:	Download Organisation Certificates and OCA Certificates through the SMKI Portal interface over the internet

Description	For a Party without a DCC Gateway Connection, a SMKI ARO accesses the SMKI Portal interface over the Internet, locates and downloads Organisation Certificates that are required to be installed on Devices ahead of installation
Objective	• To prove that the Party's ARO can locate and download the zip file of Device trust anchor Organisation Certificates through the SMKI Portal over the internet

9 Appendix D: Forms and Templates

Extant versions of templates for the following documents will be maintained on the DCC Website or SharePoint. The following templates are provided in this document to support the consultation process:

9.1	Party / RDP Notification of Intention to Undertake Testing Template
9.2	DCC Acknowledgement of Intention to Undertake Testing Template
9.3	Test Readiness Report Template
9.4	Test Plan Template
9.5	Test Execution Dashboard Template
9.6	Test Completion Report Template

9.1 Party / RDP Notification of Intention to Undertake Testing Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

PARTY / RDP NOTIFICATION OF INTENTION TO UNDERTAKE TESTING

TEST: SMKI and REPOSITORY ENTRY PROCESS TESTS

We hereby give notice that we intend to undertake SMKI and Repository Entry Process Tests in accordance with the SMKI & Repository Test Scenarios Document.

The required information is provided in the table below:

faithfully
[Name]

[Position]
Acting on behalf of [Party].

9.2 DCC Acknowledgement of Intention to Undertake Testing Template

To: [PARTY / RDP]

From: [DCC]

Date: [Date]

Dear Sir or Madam,

DCC ACKNOWLEDGEMENT OF INTENTION TO UNDERTAKE TESTING

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby acknowledge your notification that you intend to undertake SMKI & Repository Entry Process Tests in accordance with the SMKI & Repository Test Scenarios Document.

The table below confirms the contact details of our Test Manager and the date of the SMKI & Repository Entry Process Test (SREPT) Initiation Meeting:

Yours faithfully
[Name]
[Position]
Acting on behalf of the DCC.

9.3 Test Readiness Report Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST READINESS REPORT

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our current assessment of our readiness to conduct SMKI & Repository Entry Process Tests for:

Overview:

Party / RDP: [Party / RDP]

Test Start Date: [Test Start Date]

Report Information: Date of Report: [Date]

Period Covered by Report: [From date to date]

Produced by: [Name of Reporter]

Readiness Information:

Overall RAG: [Red / Amber / Green] Test Tool Selected & Available: [Y / N] Party Test Plan produced: [Y/N] Party Test Schedule produced: [Y/N]

Risks, Assumptions, Issues & Dependencies (RAID):

Please detail key RAID (Risk, Assumption, Issue and Dependency) items that have the potential to cause significant disruption to the commencement and / or completion of SMKI & Repository Entry Process Testing

Requirements Traceability Matrix Progress:

Requirements Traceability Matrix complete to date (%)	
Numbers of Requirements identified (number)	
Number of testable requirements in progress (number)	
Number of testable requirements not started (number)	
Number of Requirements deemed not testable (number)	

Test Script Development Progress:

Planned number of Test Scripts (number)	
Number of Test Scripts produced to date (number)	
Number of Test Scripts in progress (number)	
Number of Test Scripts not started (number)	
Test Data readiness by Party against planned Test Scripts (%)	

Resources & Environments Progress:

Test Resources & Technical (support) Resource Ready (Y/N if N, date expected to be ready)	
Environment Readiness:	
All interfaces required to support testing(Y/N)	

Environmental information:

[Environment configuration approved as suitable – to include breakdown and description of hardware]

SREPT Entry Criteria (to be completed by final report):

Confirm that the person requesting to commence testing is a SEC Party / RDP	
Party / RDP has identified the SMKI Interfaces the Party or RDP will access and whether this is for Device or Organisation Certificates and whether access will be through a DCC Gateway Connection	
Party has produced relevant test artefacts in sections 5.3.1.1, 5.3.1.5, and 5.3.1.6 of the SMKI & Repository Test Scenarios Document:	
- Party Notification of Intention to Undertake Testing	
- Test Readiness Report (this document)	
- Test Plan incorporating the Test Schedule	
- Requirements Traceability Matrix	
- Test Scripts	
- Test Data Plan	
has complied with the procedural steps for initiating SREPT (as set out in Table 2 of the SRTSD	
Party has provided evidence to the DCC that a test environment capable of supporting the planned testing has been established and is available	
Party has provided evidence to the DCC that an appropriate level of resources are available to support the SREPT process	
Party has provided confirmation that the Security Requirements set out in the Enduring Testing Approach Document have been met	

Overall Status:

R – testing start in line with planned date is not achievable
A – testing start in line with planned date is at risk
G – testing is expected to start on the planned date

End of report.

Yours faithfully
[Name]
[Position]
Acting on behalf of [Party / RDP].

9.4 Test Plan Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST PLAN INCLUDING TEST SCHEDULE

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our Test Plan, in accordance with the SMKI & Repository Test Scenarios Document.

Overview:

Party: [Party / RDP]

Test Start Date: [Test Start Date]

Scope

[Textual description of testing scope].

Scenarios to be Tested

See the matrices in section 5 to determine the scenarios to be tested.

[redacted]

Approach

[Textual description of the following:

- Test Scenarios & Scripts
- Test Cycles
- Re-Testing
- Regression
- Defect Management
- Test Data
- Tools]

Test Schedule

[Provide a schedule of the testing that you will undertake. This can be the form of a Project Plan, or Spreadsheet, or other format agreed with the DCC.]

Resources

[Provide details of the resources required to support the testing set out above. This can be included in the Project Plan or Spreadsheet.

This should consider roles such as Test Manager, Test Lead, Senior Test Analysts, Test Analysts, IS Support Requirements.]

End of report.

Yours faithfully
[Name]
[Position]
Acting on behalf of [Party / RDP].

9.5 Test Execution Dashboard Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST EXECUTION DASHBOARD

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our Test Execution Dashboard, in accordance with the SMKI & Repository Test Scenarios Document.

Overview:

Party / RDP: [Party / RDP]

Party /RDP ID: [Party / RDP ID]

Location: [Location of Testing / Test Manager]

Test Start Date: [Test Start Date]

Report Information:

Date & Time of Report: [Date, Time]

Period Covered by Report: [Date (for daily reports) or from date to date (for other reporting frequency]

Produced by: [Name of Reporter]

Progress Information:

[Please provide a 'Glide Path' for the testing you are undertaking, showing progress toward execution of 100% of the tests planned. This can be in the form of a spreadsheet or other format agreed with the DCC.]

Total Planned number of Tests (Test Readiness Report)	
Number of Tests scheduled for execution by report date	

Number of Tests executed by report date	
Number of Test passed by report date	
Number of Test failed by report date	
Number of Test blocked by report date	
Number of Test not run by report date	

Test Issue Report Information:

Testing Issue Information Required	
Number of Testing Issues generated	
Number of Testing Issues closed	
Number of Testing Issues open	
Number of open Testing Issues, by severity:	
- Severity 1	
- Severity 2	
- Severity 3	
- Severity 4	
- Severity 5	

Progress Toward Exit Information

[Textual description of progress made so far toward completion of testing]

Anticipated Completion Date (Submission of Test Completion Report)	

Risk Information

1			
2			
3			
4			
5			

Overall Status:

R – completion within one week of planned date is not achievable
A – completion within one week of planned date is at risk
G – completion is expected within one week of planned date

9.6 Test Completion Report Template

To: [DCC]

From: [PARTY / RDP]

Date: [Date]

Dear Sir or Madam,

TEST COMPLETION REPORT

TEST: SMKI & REPOSITORY ENTRY PROCESS TESTS

We hereby provide our Test Completion Report, in accordance with the SMKI & Repository

Test Scenarios Document.

Overview:

Party / RDP: [Party / RDP]

Test Start Date: [Test Start Date]

Approach and Scope of Testing Undertaken:

[Per the Test Plan, noting any variations.]

Summary of Test Results:

Number of tests originally scheduled for execution	
Number of tests passed	
Number of tests failed	
Number of tests not run	
Number of tests blocked	

Detail of Tests Not Successfully Executed

Summary of Testing Issues:

Number of Testing Issues generated	
Number of Testing Issues closed	
Number of Testing Issues open	
Number of open Testing Issues, by severity:	
- Severity 1	
- Severity 2	
- Severity 3	
- Severity 4	
- Severity 5	

SREPT Exit Criteria Checklist:

Test Results have been documented by the Party and evidence captured in the Party's Test Management Tool and are available to be provided to the DCC	
Testing issues identified during a Party's test execution have been recorded in the Test Management Tool (see note, below)	
Test Completion Report has been created by the Party and approved by the DCC	

Note: All testing issues must either:

- been fixed and verified by retest; or
- where outstanding, have been reviewed and documented, and been included as part of a remediation plan that outlines the next steps to be taken, including estimated timescales required to resolve each of their outstanding Testing Issues. The remediation plan must be agreed by the DCC

End of report.

Yours faithfully
[Name]
[Position]
Acting on behalf of [Party].

10 Appendix E: Test Completion Certificate

TEST COMPLETION CERTIFICATE

To: [Party / RDP] [SEC Party / RDP ID]

From: [DCC]

[Date]

Dear Sirs,

TEST COMPLETION CERTIFICATE

The relevant tests have been successfully completed to provide the following credentials:

IKI credentials for submission of Organisation CSRs using SMKI Portal via DCC Gateway Connection
IKI credentials for submission of Device CSRs using SMKI Portal via DCC Gateway Connection
IKI credentials for Ad Hoc Device CSR Web Service
IKI credentials for Batched Device CSR Web Service
Credentials for SMKI Repository Portal
Credentials for SMKI Repository Web Service
Credentials for SMKI Repository Portal SFTP

IKI credentials for submission of Organisation CSRs using SMKI Portal via the Internet IKI credentials for submission of Device CSRs using SMKI Portal via the Internet
IKI credentials for submission of Organisation CSRs using SMKI Portal via the Internet IKI credentials for submission of Device CSRs using SMKI Portal via the Internet

We confirm that the relevant tests have been executed in accordance with the relevant Test Documents. We confirm that the relevant Exit Criteria have been achieved.

Yours faithfully

[Name]
[Position]
Acting on behalf of the DCC

11 Appendix F: Definitions

Authorised Subscriber	means a Party which is an Authorised Subscriber for the purposes (and in accordance with the meaning given to that expression in Annex A [of the SEC]) of either or both of the Certificate Policies	SEC
Daily Testing Issue Report	The document reporting on the status of any testing issues identified (part of the Test Execution Dashboard)	This document
CRL	Certificate Revocation List	SEC
CSR	Certificate Signing Request	SEC
DCA	Device Certification Authority	SEC
User	A Party that has completed the User Entry Process (and, in respect of Services available in accordance with this Code to Users acting only in one or more User Roles, a Party that has completed the User Entry Process for that User Role)	SEC
Exit Criteria	The criteria that must be satisfied before testing can be considered complete	SEC
FIPS token	Cryptographic Credential Token issued in accordance with the SMKI RAPP	This document
OCA	Organisation Certification Authority	SEC
RDP	Registration Data Provider	SEC
Regression Testing	Testing of a previously tested program following modification to ensure that defects have not been introduced or uncovered in unchanged areas of the software, as a result of the changes made (and Regression Test shall be construed accordingly)	International Software Testing Qualifications Board
Relevant Party	A Party which is undertaking SMKI and Repository Entry Process Tests	This document
SMKI RAPP	SMKI Registration Authority Policies and Procedures	SEC
(Requirements) Traceability Matrix	A matrix of defined requirements that provides traceability (linkage) to Test Scripts for the purpose of providing a measurement of test coverage as intended in the relevant	International Software Testing

	specification.	Qualifications Board
SMKI	Smart Metering Key Infrastructure	SEC
SREPT	SMKI and Repository Entry Process Tests	This document
SREPTS	SMKI and Repository Entry Process Test Scenarios	This document
SRT	SMKI and Repository Testing – A test stage that will commence prior to Interface Testing Stage	SEC
SRTSD	SMKI and Repository Test Scenarios Document (this document)	SEC
Test Completion Certificate	A certificate issued by the on successfully completes SREPT as set out in Appendix E: Test Completion Certificate	This document
Test Completion Report	A document summarising testing activities and results. It also contains an evaluation of the corresponding test items against Exit Criteria	This document
Test Completion Certificate	A certificate issued by the DCC to the Party when the Party has met the SREPT Exit Criteria	This document
Test Data	Any data constructed for the purposes of undertaking SMKI and Repository Entry Process Testing	This document
Test Data Plan	The document that sets out: the size and type/format of data, who is responsible for providing the data; and when the data is required to be available to support test activities in a Test Plan	This document
Test Execution Dashboard	The document summarising testing activities and results, produced at regular intervals, to report progress of testing activities against a baseline (such as the original test plan) and to communicate risks and alternatives requiring a decision to management	This document
Test Management Tool	A tool that has the ability to log and track Testing Issues	This document
Test Plan	A document describing the scope, approach, resources and schedule of intended test activities within a Test Stage that will be produced as set out in Section 9.4.	This document

Test Result	The consequence/outcome of the execution of a Test Script	This document
Test Readiness Report	A report that when completed provides the capability to assess the status of test preparation and determine the readiness to proceed into test execution	This document
Test Schedule	A list of test process activities, tasks or events identifying their intended start and finish dates and/or times and interdependencies	This document
Test Script	A document specifying a sequence of actions for the execution of a test	This document
Test SMKI Repository Services	Test versions of the SMKI Repository Services (see definition in SEC) provisioned for the purposes of SREPT	This document
Test SMKI Services	Test versions of the SMKI Services (see definition in SEC) provisioned for the purposes of SREPT	This document
Test Stage	A group of test activities that are organised and managed together	This document
WD	Working Day	SEC

12 Appendix G: Testing Issue Severity Descriptions

Severity 1	An Issue which in relation to the Relevant Party or RDP: • would prevent user from using their systems • would have a critical adverse impact on business activities • would cause significant financial loss • would result in any material loss or corruption of Data. Non-exhaustive examples: • an Issue leading to non-availability of systems • all test progress is blocked.
Severity 2	An Issue which in relation to the Relevant Party or RDP: • would have a major (but not critical) adverse impact on use of systems • would cause limited financial loss Non-exhaustive examples: • an Issue leading to non-availability of or to loss of resilience of a material part of their systems • large areas of functionality will not be able to be tested • testing not completely blocked but has been significantly impacted.
Severity 3	An Issue which in relation to the Relevant Party or RDP: • would have a major adverse impact on business activities but which can be reduced to a moderate adverse impact through a work-around • would have a moderate adverse impact on the business activities Non-exhaustive examples: • testing can progress but the work-around will impact test progress.

Severity 4	An Issue which in relation to the Relevant Party or RDP: • would have a minor adverse impact on business activities Non-exhaustive examples: • minor service interruptions in the business process
Severity 5	An Issue which in relation to the Relevant Party or RDP: • would have minimal impact on business activities Non-exhaustive examples: • trivial Issues with work-arounds which are noted for future releases but minimal impact of running existing activities • tests can still pass but there are cosmetic issues.

Version: L1.0

Appendix L

SMKI Recovery Procedure

Contents

1 Introduction 4

1.1 Purpose & Interpretation 4

1.2 Scope 4

2 Overview of the SMKI Recovery Procedure 7

3 General obligations 9

3.1 DCC Obligations 9

3.2 Notification and confirmation of a suspected Compromise 9

3.3 Permitted mechanisms for confirmation of suspected Compromise 10

3.4 Appointment and responsibilities of Key Custodians 11

3.4.1 Responsibilities in respect of Key Custodians 11

3.4.2 Ceasing to be a Key Custodian 12

3.4.3 Detailed procedure for appointment of Key Custodians 13

4 Procedure to recover from the Compromise of a Private Key corresponding with a Public Key contained within an Organisation Certificate held on a Device (other than the Recovery Private Key) 17

4.1 Method 1 - recovery by the affected Subscriber using its Private Key to replace affected Organisation Certificates on Devices 18

4.1.1 Pre-Recovery 18

4.1.2 Execution of Recovery Procedure 20

4.1.3 Post-Recovery 21

4.2 Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected Devices 22

4.2.1 Pre-Recovery 22

4.2.2 Execution of Recovery Procedure 26

4.2.3 Post-Recovery 28

4.3 Method 3 - recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on Devices 29

4.3.1 Pre-Recovery 29

4.3.2 Execution of Recovery Procedure 32

4.3.3 Post-Recovery 35

5 Recovery using the Contingency Private Key 36

5.1 Pre-Recovery 36

5.2 Execution of Recovery Procedure 39

5.3 Post Recovery 42

b) the DCC Access Control Broker Certificate in each Network Operator Device slot with an Organisation Certificate to which the Network Operator is the Subscriber that is Issued under the new Issuing OCA, for each Device as established in step 5.2.2 within section 5.2 of this document. 43

6 Recovery from Compromise of a Contingency Private Key, Contingency Symmetric Key, Issuing OCA Private Key or Recovery Private Key 45

6.1 Recovery from Compromise of a Contingency Private Key or the Contingency Symmetric Key 45

6.1.1 Pre-Recovery 45

6.1.2 Execution of Recovery Procedure 48

a) a new Contingency Symmetric Key; 49

6.1.3 Post-Recovery 52

6.2 Recovery from Compromise of the Recovery Private Key 53

6.2.1 Pre-Recovery 53

6.2.2 Execution of Recovery Procedure 56

6.2.3 Post-Recovery 57

6.3 Recovery from Compromise of the Issuing OCA Private Key 58

6.3.1 Pre-Recovery 58

6.3.2 Execution of Recovery Procedure 61

6.3.3 Post-Recovery 65

7 Periodic testing of the SMKI Recovery Procedure 66
7.1 Testing Arrangements 66
Appendix A Communication Formats 68
Appendix B Organisation Compromise Notification File 69
Appendix C Organisation Compromise Recovery Progress File 72
Appendix D Other Compromise Notification File 75
Appendix E Other Compromise Recovery Progress File 78
Appendix F Definitions 82

1 Introduction

1.1 Purpose & Interpretation

Section L10.4 of the Code sets out the principle rights and obligations for compliance with any requirements set out in the SMKI Recovery Procedure.

This document, the SMKI Recovery Procedure, sets out the procedural requirements and the rights and obligations in respect of the DCC, Parties and the SMKI PMA relating to recovery from the Compromise of a Relevant Private Key. The scope of the SMKI Recovery Procedure is as set out in Section L10 of the Code and is further set out in more detail in Section 1.2 of this document.

The procedures as set out in this document shall be executed in the event of a Compromise of a Relevant Private Key, other than as directed by the SMKI PMA, in accordance with the procedures set out in this document.

For the purposes of the SMKI Recovery Procedure:

a) notwithstanding the definition as set out in Section A of the Code, “Subscriber” means, in relation to any Certificate associated with a Relevant Private Key, a Party which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate;

b) “M#N Share” means, in relation to a Private Key, that the key is split into N Key Components such that the Private Key may be recreated using any M or more Key Components, and the Private Key may not be recreated using fewer than M Key Components;

c) “Contingency Symmetric Key” means the Symmetric Key used to encrypt the Contingency Public Key;

d) “Contingency Keys” means the Contingency Symmetric Key and the Contingency Private Key;

e) Relevant Private Key has the meaning set out in Section L10; and

f) where an obligation is expressed as being an obligation on a Key Custodian it shall be interpreted as being an obligation on:

   i. in the case of a Key Custodian appointed by a Party, that Party, and

   ii. in the case of a Key Custodian appointed by the SMKI PMA or the Panel, that SMKI PMA Member or Panel Member acting in its capacity as such.

1.2 Scope

The SMKI Recovery Procedure sets out the detail of the arrangements between the DCC, Parties, the SMKI PMA and the Panel in respect of:

a) **Pre-Recovery**:
   i. confirmation of a Compromise or suspected Compromise of a Relevant Private Key reported to the DCC by a Party, resulting in an Incident being raised in accordance with sections 2.1 and 2.2 of the DCC's Incident Management Policy;
   ii. notification to the DCC of the Anomaly Detection Thresholds that are required to support replacement of affected Certificates on Devices;
   iii. where use of the Recovery Private Key or the Contingency Private Key would be required in order to recover, consultation by the DCC with the SMKI PMA to determine the extent to which the recovery procedure should be executed and the manner in which it should be executed;
   iv. revocation of affected Certificates (where required); and
   v. other steps as set out in this SMKI Recovery Procedure;

b) **Execution of Recovery**
   i. execution of activities to recover from a Compromise or suspected Compromise of a Relevant Private Key; and

c) **Post-Recovery**:
   i. replacement of Certificates and Private Keys (where necessary);
   ii. post-Incident review and reporting;
   iii. provision to relevant parties of information intended to prevent reoccurrence of similar Incidents; and
   iv. revocation of replaced Certificates (where necessary).

The SMKI Recovery Procedure addresses recovery from a Compromise, or suspected Compromise in respect of any Relevant Private Key listed immediately below:

a) Private Keys associated with Organisation Certificates stored on Devices (other than those associated with a Recovery Certificate), where such Devices have an SMI Status of 'commissioned';
b) the Contingency Symmetric Key;
c) the Contingency Private Key;
d) the Private Key associated with an Issuing OCA Certificate;
e) the Private Key associated with a Root OCA Certificate; and
f) the Private Key associated with a Recovery Certificate.

Figure 1, immediately below, shows the relevant Certificates that are held on applicable Devices, and the relevant Certificates and Private Keys related to those held on Devices which are covered under the scope of the SMKI Recovery Procedure.

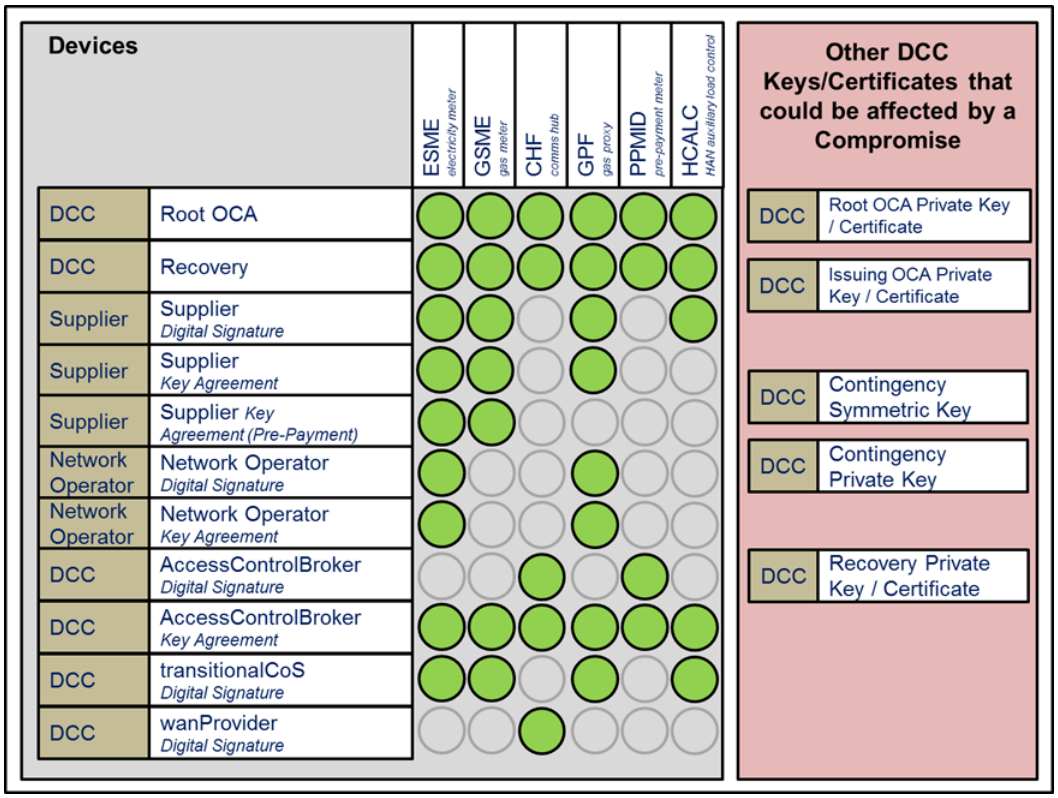

Figure 1: Public Key Certificates / Keys covered by the SMKI Recovery Procedure

2 Overview of the SMKI Recovery Procedure

In the event of an incident which:

a) results in the Compromise of a Relevant Private Key; or

b) causes the Subscriber for the Certificate associated with any of the Keys in a) above (and in the case of the Contingency Symmetric Key, the DCC) to reasonably suspect that there has been a Compromise of any such Key,

the provisions of this SMKI Recovery Procedure shall apply.

The SMKI Recovery Procedure includes procedures which detail the obligations of the DCC, Subscribers and the SMKI PMA, in respect of recovery from Compromise or suspected Compromise of a Relevant Private Key as set out in Section 1.2 of this document.

The table as set out immediately below summarises the actions required and the section(s) of this document which contain the applicable recovery procedure(s).

Compromise or Suspected Compromise of:	**Section(s) of this document containing the procedure(s)**
Private Key associated with Organisation Certificate held on one or more Devices (other than the Recovery Certificate)	**4.1 Method 1 - recovery by the affected Subscriber using its Private Key to replace affected Organisation Certificates on Devices** 4.1.1 Pre-Recovery 1.1.1 **Error! Not a valid result for table.** 4.1.3 Post-Recovery **4.2 Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected Devices (only available to a Supplier Party)** 4.2.1 Pre-Recovery 4.2.2 Execution of Recovery Procedure 4.2.3 Post-Recovery **4.3 Method 3 - recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on Devices** 4.3.1 Pre-Recovery 4.3.2 Execution of Recovery Procedure 4.3.3 Post-Recovery
Root OCA Private Key	5.1 Pre-Recovery 5.2 Execution of Recovery Procedure 5.3 Post Recovery
Contingency Private Key or Contingency Symmetric Key	6.1.1 Pre-Recovery 6.1.2 Execution of Recovery Procedure 6.1.3 Post-Recovery

Compromise or Suspected Compromise of:	Section(s) of this document containing the procedure(s)
Recovery Private Key	6.2.1 Pre-Recovery 6.2.2 Execution of Recovery Procedure 6.2.3 Post-Recovery
Issuing OCA Private Key	6.3.1 Pre-Recovery 6.3.2 Execution of Recovery Procedure 6.3.3 Post-Recovery

3 General obligations

3.1 DCC Obligations

The DCC shall:

a) conduct the procedures set out in this document;
b) comply with any decisions made by the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise, or suspected Compromise;
c) where the DCC attempts but fails to replace one or more Certificates as part of operating these procedures, execute as many retries to replace such Certificates as DCC can reasonably accommodate given the circumstances of the Compromise and capability of the DCC Systems, prior to any deadline for recovery as approved by the SMKI PMA;
d) where the DCC consults with the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise, or suspected Compromise, and the DCC is directed such that recovery using the Recovery Private Key or Contingency Private Key should not be performed, the DCC shall inform all affected Parties of the outcome and any reasons provided by the SMKI PMA, as soon as reasonably practicable following such instruction, via a secured electronic means;
e) maintain confidential, auditable and secured records relating to the recovery from a Compromise (or suspected Compromise), and the Devices and Subscribers affected by such Compromise; and
f) within three Working Days of the recovery from a Compromise or suspected Compromise, prepare a report regarding execution of the recovery and provide such report to the SMKI PMA, where such report shall include:
    i. the process steps executed and the timing of the procedure to recover from the Compromise;
    ii. where possible, analysis of which communications have been submitted to Devices and any anomalous activity that should be investigated further by the DCC and/or affected Subscribers, and/or addressed via remedial actions; and
    iii. any proposed modifications to the SMKI Recovery Procedure that the DCC believes are necessary for the SMKI Recovery Procedure to more effectively meet the objectives as set out in the SEC.

3.2 Notification and confirmation of a suspected Compromise

Any person may notify the DCC that there is a Compromise or suspected Compromise of a Relevant Private Key.

Where the DCC is notified or becomes aware of a Compromise or suspected Compromise of a Relevant Private Key, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall notify the SMKI PMA, via secured electronic means, that a Compromise or suspected Compromise has been notified. The DCC shall contact the Subscriber for the Certificate associated with that Private Key or Contingency Symmetric Key (which may include the DCC itself as the Subscriber), as soon as reasonably practicable, via telephone and email using the contact details held by the SMKI Registration Authority. The DCC shall provide the Subscriber, via secured electronic means, with the appropriate Incident reference number and information relating to the notified Compromise. The DCC shall request confirmation from the Subscriber as to whether the Subscriber reasonably believes that a Compromise has occurred, and wishes to proceed with one or more of the recovery processes, which shall be confirmed by:

a) A SMKI Senior Responsible Officer (SMKI SRO) on behalf of a Party; or

b) A SMKI SRO, SMKI Registration Authority Manager or member of SMKI Registration Authority Personnel on behalf of the DCC.

The Subscriber shall take reasonable steps to ensure that confirmation of whether it reasonably believes that a Compromise has occurred is provided to the DCC by the representatives above, within 24 hours of the request for confirmation from the DCC, via secured electronic means. Where the Subscriber confirms that it does not reasonably believe that a Compromise has occurred, the DCC shall close the Incident in accordance with section 2.12 of the Incident Management Policy.

Where the DCC receives confirmation that the Subscriber reasonably believes that a Compromise has occurred, the DCC shall also identify any Responsible Supplier(s) that are affected by the confirmed Compromise, in accordance with the procedures as set out in this document.

Where the DCC receives multiple Compromise notifications, the DCC may execute a common set of procedural steps to address such multiple Compromises, where it reasonably believes that such an approach would achieve the required recovery in an efficient manner.

3.3 Permitted mechanisms for confirmation of suspected Compromise

The DCC shall only accept the confirmation of a Compromise or suspected Compromise from a representative of the Subscriber as is defined in section 3.2 of this document, for a Certificate associated with a Compromised Private Key or from the DCC in respect of a Compromised Contingency Symmetric Key, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means.

3.4 Appointment and responsibilities of Key Custodians

The Organisation Certification Practice Statement (Organisation CPS) requires the Contingency Private Key and Recovery Private Key to be split into M#N Shares and that such Private Keys may be activated only via collaboration between appointed Key Custodians. The procedure as set out in this section 0 shall be followed in order to appoint such Key Custodians as are required.

Subject in either case to the approval of the SMKI PMA, where steps are taken to appoint a Key Custodian, or where (after such appointment) steps are taken by a Key Custodian, and in either case those steps would have been valid in accordance with this document if they were taken after its designation by the Secretary of State, they shall be treated as valid in accordance with this document, and therefore effective for the purposes of the Code, even if they were taken before its designation.

3.4.1 Responsibilities in respect of Key Custodians

Each Party, the SMKI PMA or the Panel, on behalf of which an individual acting on behalf of that organisation becomes a Key Custodian, shall ensure that the Key Custodian:

a) does not seek to find out the identity of other Key Custodians or otherwise collude with other Key Custodians in relation to matters associated with this Recovery Procedure other than for the purposes as set out in this SMKI Recovery Procedure;

b) does not disclose the fact that they are a Key Custodian, other than:

   i. in the case of each Party, to a Director, Company Secretary, SMKI SRO or Chief Information Security Officer for the organisation they represent; or
   ii. in the case of the SMKI PMA or Panel, to other members of the SMKI PMA or Panel; and
   iii. to those other persons to whom the information reasonably needs to be disclosed for reasons of personnel management within the relevant organisation, and furthermore shall ensure that persons within their organisation who are aware of the identity of a Key Custodian shall not disclose the identity of a Key Custodian more widely;

c) takes all reasonable steps to protect and not to lose any safety deposit box key issued to secure any Cryptographic Module them as part of the relevant Key Generation Ceremony, and which is used by the Key Custodian to secure the Cryptographic Module containing the Key Component issued to them, in accordance with any guidance documentation provided by the DCC to the Key Custodian via secured electronic means;

d) where the safety deposit box securing the Cryptographic Module containing a Key Component cannot be accessed, or the safety deposit key is lost or cannot be accessed , the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall take such steps as are necessary to resolve the Incident;

e) takes all reasonable steps to attend a Key Generation Ceremony or Key Activation Ceremony when requested by the DCC and, where they are to attend, to do so as soon is as reasonably practicable following the request from DCC; and

f) is, upon request to attend a Key Generation Ceremony or Key Activation Ceremony by the DCC, immediately released to perform the Key Custodian role unless it would be materially disruptive to the business of the relevant organisation for them not to be released at that time.

Where a Party is the Subscriber for a Certificate that is Compromised (or is suspected to be Compromised), the Subscriber is not the DCC and an individual acting on behalf of that Subscriber is a Key Custodian; the DCC may exclude that Key Custodian from attending any Key Generation Ceremony or Key Activation Ceremony required as part of the applicable recovery procedure, where the DCC considers such action to be appropriate to mitigate security risks. If such exclusion occurs, the DCC shall record the decision made, and shall notify that Key Custodian and a SMKI SRO for the Subscriber, via secured electronic means.

3.4.2 Ceasing to be a Key Custodian

In the event that a Party, the SMKI PMA or the Panel wishes a particular individual to cease their role as a Key Custodian:

a) such Party, the SMKI PMA or the Panel shall notify the DCC in writing, at least one month in advance of the date on which that it wishes the individual acting as a Key Custodian to cease to be a Key Custodian;

b) the relevant Party, the SMKI PMA or Panel shall return the physical key, for the corresponding safety deposit box in which the Cryptographic Module containing the relevant Key Component is held, to a Registration Authority Manager at the DCC's address as published on the DCC Website, by secure courier;

c) the DCC shall update its records of Key Custodians; and

d) the DCC shall conduct, insofar as necessary, the procedure as set out in section 3.4.3 immediately below, provided that subject to the approval of the SMKI PMA, any action taken by DCC prior to the date of the designation of this SMKI Recovery Procedure shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI Recovery Procedure for the purposes of appointing a Key Custodian, be treated as if it had taken place after that date.

3.4.3 Detailed procedure for appointment of Key Custodians

The procedure as set out immediately below shall be executed by the DCC, Parties, the SMKI PMA and the Panel in order to appoint Key Custodians.

Step	When	Obligation	Responsibility	Next Step
3.4.3.1	As identified by the DCC that Key Custodians are required	The DCC shall identify the need for Key Custodians in respect of a Recovery Private Key or Contingency Private Key.	DCC	3.4.3.2
3.4.3.2	As soon as reasonably practicable, following 3.4.3.1	The DCC shall issue a request for nominations, via a secured electronic means, to Parties, the DCC, the SMKI PMA and the Panel, for individuals to become Key Custodians for the Recovery Private Key or Contingency Private Key as identified in step 3.4.3.1. Such request for nominations shall: a) include the Key Custodian nomination form as published on the DCC Website; b) be marked as confidential; and c) detail the locations where each relevant Key Generation Ceremony and any corresponding Key Activation Ceremony will take place.	DCC	3.4.3.3
3.4.3.3	Within 10 Working Days of the issuance of the request for nominations	Each Party, the SMKI PMA or the Panel wishing to nominate an individual to become a Key Custodian in respect of a particular Private Key shall provide, via secured electronic means, to the DCC for each nominated individual, a completed Key Custodian nomination form using the pro-forma as published on the DCC Website. The nomination form should contain the following information: a) the full name of a Director, Company Secretary or SMKI Senior Responsible Officer who is nominating the individual to become a Key Custodian for a Party, the SMKI PMA Chair for the SMKI PMA or the Panel Chair for the Panel; b) the full name of the nominated individual;	Party, DCC, the SMKI PMA or the Panel	3.4.3.4

Step	When	Obligation	Responsibility	Next Step
3.4.3.3 (continued)		c) contact telephone details for the nominated individual; d) the nominated individual's normal work location; e) the estimated time to travel to the location of the relevant Key Generation Ceremony and to the location of the corresponding Key Activation Ceremony, as notified in step 3.4.2; f) evidence that the individual is: i. for a Party, an employee or Director of the Party; ii. for the DCC, an employee of the DCC or a DCC Service Provider; iii. for the SMKI PMA, an appointed member of the SMKI PMA; or iv. for the Panel, an appointed member of the Panel; and g) evidence that the nominated individual has successfully completed security screening in a manner that is compliant with: i. British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or ii. any equivalent to that British Standard which updates or replaces it from time to time. Where necessary in order to have a sufficient number of Key Custodians appointed, the SMKI PMA may direct any Party to nominate individuals to become Key Custodians. Where this occurs, the directed Party shall identify and nominate individuals in accordance with this step 3.4.3.3.		
3.4.3.4	As soon as reasonably practicable following 3.4.3.3	The DCC shall determine: a) using publicly available information, whether the Director, Company Secretary, SMKI PMA Chair or Panel Chair who is nominating the individual to become a Key Custodian holds such a role on behalf of the organisation; and b) whether the information supplied in the Key Custodian nomination form is complete and accurate.	DCC	If complete, 3.4.3.5; if not complete, 3.4.3.3

Step	When	Obligation	Responsibility	Next Step
		Where there are omissions/discrepancies, agree actions with the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, via secured electronic means or in writing.		
3.4.3.5	As soon as reasonably practicable, following 10 Working Days after issuance of request for nominations	The DCC shall collate nominations received and shall provide to SMKI PMA: a) details of those nominated individuals and the organisation they are representing; and b) upon request from the SMKI PMA, details held by the DCC of all existing holders of Key Components.	DCC	3.4.3.6
3.4.3.6	As soon as reasonably practicable, following 3.4.3.5	The SMKI PMA shall determine the individuals that shall become Key Custodians, which shall take into account geographical location and how many Key Components are held by any particular organisation or individual (where relevant). The SMKI PMA shall inform the DCC of the individuals which shall become Key Custodians.	SMKI PMA	3.4.3.7 if sufficient Key Custodians can be appointed; if not, 3.4.3.3
3.4.3.7	As soon as reasonably practicable, following 3.4.3.6	The DCC shall confirm that the individual has been selected by the SMKI PMA to become a Key Custodian and shall confirm the date and time for a verification meeting for the nominated individual at the DCC's offices, to the Director, Company Secretary, SMKI PMA Chair or Panel Chair of the applicant organisation who nominated the individual to become a Key Custodian, via secured electronic means.	DCC	3.4.3.8
3.4.3.8	At verification meeting	The DCC shall, in person, verify the individual identity of the nominated individual to Level 3 (Verified) pursuant to the CESG GPG45 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.	DCC	If successful for all, 3.4.3.10; for unsuccessful, 3.4.3.9
3.4.3.9	As soon as reasonably practicable following rejection	The DCC shall notify the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, in writing, that the nominated individual could not at that point be appointed as a Key Custodian.	DCC	3.4.3.6

Step	When	Obligation	Responsibility	Next Step
3.4.3.10	As soon as reasonably practicable, following 3.4.3.8	The DCC shall notify, in writing via secured electronic means: a) the individual, in person, that they are eligible to become a Key Custodian; and b) the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, that the nominated individual is eligible to become a Key Custodian.	DCC	3.4.3.11
3.4.3.11	As soon as reasonably practicable, following 3.4.3.10	The DCC shall: a) update its records of eligible Key Custodians for Private Keys for which Key Components are issued and shall store such records in a secured manner; and b) inform the SMKI PMA Chair, in writing, that the nominated individual has become a Key Custodian	DCC	Relevant procedure to recover from a notified Compromise

4 Procedure to recover from the Compromise of a Private Key corresponding with a Public Key contained within an Organisation Certificate held on a Device (other than the Recovery Private Key)

This section sets out the procedures that may be used in order to recover from the Compromise (or suspected Compromise) of a Private Key associated with an Organisation Certificate held on a Device other than the Recovery Private Key, where a Subscriber wishes to recover from the Compromise (or suspected Compromise) using this procedure.

Where a Subscriber wishes to recover from the Compromise (or suspected Compromise) of such an Organisation Certificate using any of the methods listed immediately below, it shall notify the DCC of which of the methods listed immediately below that it wishes to use, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means. The DCC shall update the Incident Management Log to record such notification in accordance with H9.1(g).

a) **Method 1:** the Subscriber shall seek to recover using the Compromised Private Key to replace the Organisation Certificate to which the Relevant Private Key relates on all affected Devices;

b) **Method 2:** (only applicable where the Subscriber is a Supplier Party), the DCC shall use the Recovery Private Key to replace affected Certificates on Devices with a DCC Access Control Broker Certificate. The Responsible Supplier shall then complete the recovery process by replacing the DCC Access Control Broker Certificate with new Organisation Certificates for which it is the Subscriber; or

c) **Method 3:** the DCC shall recover using the Recovery Private Key to replace affected Certificates on Devices with new Organisation Certificates provided by the Subscriber.

Following the notification of the selected recovery method by the Subscriber, the DCC shall:

a) Where method 1 has been selected, perform the procedure as set out in Section 4.1 of this document;

b) Where method 2 has been selected, perform the procedure as set out in Section 4.2 of this document; or

c) Where method 3 has been selected, perform the procedure as set out in Section 4.3 of this document.

4.1 Method 1 - recovery by the affected Subscriber using its Private Key to replace affected Organisation Certificates on Devices

4.1.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

Step	When	Obligation	Responsibility	Next Step
4.1.1.1	As soon as possible, following notification that the Subscriber wishes to recover using its own Private Key	The affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates that are affected by the Compromise (or suspected Compromise). The DCC shall revoke such Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP.	Subscriber, DCC	4.1.1.2
4.1.1.2	As soon as reasonably practicable, following 4.1.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly	Subscriber	4.1.1.3

Step	When	Obligation	Responsibility	Next Step
		Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure.		
4.1.1.3	As soon as reasonably practicable, following 4.1.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a) that a Compromise of an Organisation's Private Key has been notified; b) that the Subscriber intends to use method 1 (as set out in section 4.1 of this document) to recover; and c) of details relating to the Compromise, comprising the Subscriber and the number of Devices affected, which will include the Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	DCC	4.1.1.4
4.1.1.4	As soon as reasonably practicable, following 4.1.1.3	Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.1.1.1, the DCC shall notify the Responsible Supplier, via secured electronic means, that a Subscriber wishes to recover using its own Private Key to recover. The DCC shall also provide to the Responsible Supplier, via a secured electronic means, one or more Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC, which together contain details of the Device IDs to which the Compromise relates.	DCC	Procedure as set out in section 4.1.2 of this document

4.1.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.1.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.1.2.1	As soon as reasonably practicable, following procedure as set out in section 4.1.1	The DCC shall temporarily amend the Anomaly Detection Thresholds for the affected Subscriber to allow submission of Service Requests to replace affected Organisation Certificates, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure.. The DCC shall inform, via a secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.1.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1.2.2
4.1.2.2	As soon as reasonably practicable, following 4.1.2.1	The affected Subscriber shall either: a) identify replacement Organisation Certificates; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	4.1.2.3
4.1.2.3	As soon as reasonably practicable, following 4.1.2.2	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification, to replace affected Organisation Certificates on all relevant Devices and shall, in doing so, monitor replacement of such affected Organisation Certificates.	Subscriber	4.1.2.4
4.1.2.4	As soon as reasonably practicable, following 4.1.2.3	Upon completion of its activities to replace affected Organisation Certificates on affected Devices, the affected Subscriber shall inform the DCC, via a secured electronic means: a) that its activities in respect of the replacement of Organisation Certificates have been completed; and b) of the Devices for which replacement of affected Organisation Certificates has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E.	Subscriber	4.1.2.5

Step	When	Obligation	Responsibility	Next Step
4.1.2.5	As soon as reasonably practicable, following 4.1.2.4	Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.1.1.1, he DCC shall notify the Responsible Supplier for affected Devices, via secured electronic means, which Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in section 4.1.3 of this document

4.1.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Private Key associated with an Organisation Certificate using the procedures as set out in sections 4.1.1 and 4.1.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.1.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.1.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure.	DCC (DSP TAD)	4.1.3.2
4.1.3.2	As soon as reasonably practicable, following 4.1.3.1	The DCC shall notify the SMKI PMA via a secured means of: a) the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1; and b) the Devices for which recovery was not completed, which may be provided in one or more which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	End of procedure

4.2 Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected Devices

4.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document, and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

Step	When	Obligation	Responsibility	Next Step
4.2.1.1	As soon as possible, following notification that the Subscriber wishes to recover using the procedure set out in section 4.2 of this document	The affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP.	Subscriber, DCC	4.2.1.2

Step	When	Obligation	Responsibility	Next Step
4.2.1.2	As soon as possible, following 4.2.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more Organisation Compromise Notification Files that each comply with Appendix B of this document and which together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure.	Subscriber	4.2.1.3
4.2.1.3	As soon as reasonably practicable, following 4.2.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise (or suspected Compromise) of an Organisation Certificate or Organisation Certificates, using the procedure as set out in section 4.2.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Certificates on Devices). The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	4.2.1.4

Step	When	Obligation	Responsibility	Next Step
4.2.1.4	As soon as reasonably practicable, following 4.2.1.3	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices, which may be provided in in one or more Organisation Compromise Notification Files that comply with Appendix B of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); d) anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA.	DCC, Subscriber	4.2.1.5
4.2.1.5	As soon as reasonably practicable, following 4.2.1.4	The DCC shall notify the relevant Network Parties via secured electronic means: a) that a Responsible Supplier wishes to recover using the procedure as set out in section 4.2.2 of this document; and b) the Device IDs to which the Compromise relates, which shall submitted in one or more Organisation Compromise Notification Files that comply with Appendix B of this document.	DCC	4.2.1.6
4.2.1.6	As soon as reasonably practicable, following 4.2.1.5	Where the DCC believes that use of the Recovery Private Key is likely to be agreed by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key;	DCC, Key Custodians	4.2.1.7

Step	When	Obligation	Responsibility	Next Step
		c) notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and d) activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key.		
4.2.1.7	As soon as reasonably practicable, following 4.2.1.6	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.2.1.4 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	4.2.1.8
4.2.1.8	As soon as reasonably practicable, following 4.2.1.7	The DCC shall inform the affected Subscriber, of the SMKI PMA's decision whether or not to execute the procedure as set out in section 4.2.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise procedure as set out in section 4.2.2 of this document

4.2.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.2.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.2.2.1	As soon as possible, following notification from the SMKI PMA to the DCC that this procedure should be executed	The DCC shall disable processing of communications destined for Devices that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status to 'recovery'.	DCC	4.2.2.2
4.2.2.2	As soon as reasonably practicable, following 4.2.2.1	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of recovery Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.2.1 of this document; and b) for the affected Subscriber, to allow submission of Service Requests to replace DCC Access Control Broker Certificates with new Organisation Certificates. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.2.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1.2.3
4.2.2.3	As soon as reasonably practicable, following 4.2.2.2	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key.	DCC	4.2.2.4
4.2.2.4	As soon as reasonably practicable, following 4.2.2.3	The DCC shall send Commands to each affected Device, Digitally Signed using the Recovery Private Key, in order to replace Organisation Certificates in all of the Supplier slots on Devices as notified in step 4.2.1.2, with a DCC Access Control Broker Certificate. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise.	DCC	4.2.2.5
4.2.2.5	As soon as reasonably practicable, following 4.2.2.4	Upon completion of step 4.2.2.4 for each Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status to 'recovered'.	DCC	4.2.2.6

Step	When	Obligation	Responsibility	Next Step
4.2.2.6	As soon as reasonably practicable, following 4.2.2.5	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected Devices: a) upon replacement of affected Certificates on each Device, using a DCC Alert issued via the DCC User Interface; and b) upon completion of attempts to replace all affected Certificates on relevant Devices, in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document, provided via secured electronic means.	DCC	4.2.2.7
4.2.2.7	As soon as reasonably practicable, following 4.2.2.6	The affected Subscriber shall either: a) identify replacement Organisation Certificates; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	4.2.2.8
4.2.2.8	As soon as reasonably practicable, following 4.2.2.7	Where the DCC has recovered by replacing Organisation Certificates of the Responsible Supplier, with a DCC Access Control Broker Certificate, the Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace the DCC Access Control Broker Certificate in each Supplier Device slot with a replacement Organisation Certificate, for each Device as established in step 4.2.1.1 within section 4.2 of this document. Upon successful completion of such replacement for a Device, the DCC shall set the SMI Status for that Device to the SMI Status that was in place immediately prior to the execution of step 4.2.2.1 of this procedure.	Responsible Supplier	4.2.2.9
4.2.2.9	As soon as reasonably practicable, following 4.2.2.8	The Responsible Supplier shall notify the DCC in respect of replacement of such DCC Access Control Broker Certificates with new Organisation Certificates, via secured electronic means and in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document.	DCC	4.2.2.10
4.2.2.10	As soon as reasonably practicable, following the deadline as determined in step 4.2.1.6	For each affected Device that has an SMI Status of ‘recovery’ or ‘recovered’, the DCC shall restore the SMI Status that was in place immediately prior to the execution of step 4.2.2.1 of this procedure.	DCC	Procedure as set out in Section 4.2.3 of this document

4.2.3 Post-Recovery

The procedure as set out immediately below shall be used following execution of the procedures as set out in sections 4.2.1 and 4.2.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.2.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.2.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the affected Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.2 of this document.	DCC (DSP TAD)	4.2.3.2
4.2.3.2	As soon as reasonably practicable, following 4.2.3.1	The DCC shall notify the SMKI PMA, via a secured means, of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document; and b) the number of Devices for which recovery was not successful.	DCC	End of procedure

4.3 Method 3 - recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on Devices

4.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document, and notification from the relevant Subscriber that it wishes to recover from the Compromise (or suspected Compromise) using the procedure set out in this section.

Step	When	Obligation	Responsibility	Next Step
4.3.1.1	As soon as possible, following notification that the Subscriber wishes to recover using the procedure set out in section 4.3.2 of this document	The Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP.	Subscriber, DCC	4.3.1.2
4.3.1.2	As soon as reasonably practicable, following 4.3.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate.	Subscriber	4.3.1.3

Step	When	Obligation	Responsibility	Next Step
4.3.1.3	As soon as reasonably practicable, following 4.3.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise (or suspected Compromise) of its Organisation Certificate using the procedure as set out in section 4.3.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Certificates on Devices). The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	4.3.1.4
4.3.1.4	As soon as reasonably practicable, following 4.3.1.3	Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means: a) that a Subscriber wishes to recover using the procedure as set out in section 4.3.2 of this document; and b) the Device IDs to which the Compromise relates, which shall be submitted in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	DCC	4.3.1.5
4.3.1.5	As soon as reasonably practicable, following 4.3.1.4	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices, which may be provided in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and d) anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA.	DCC, Subscriber	4.3.1.6

Step	When	Obligation	Responsibility	Next Step
4.3.1.6	As soon as reasonably practicable, following 4.3.1.5	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d) activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	4.3.1.7
4.3.1.7	As soon as reasonably practicable, following 4.3.1.6	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.3.1.5 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	4.3.1.8

Step	When	Obligation	Responsibility	Next Step
4.3.1.8	As soon as reasonably practicable, following 4.3.1.7	The DCC shall notify the affected Subscriber, via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2. Where the affected Subscriber is not the Responsible Supplier for a Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise procedure as set out in section 4.3.2 of this document

4.3.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA in accordance with section 4.3.1 of this document, shall be used, following execution of the process as set out in section 4.3.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.3.2.1	As soon as possible, following notification from the SMKI PMA to the DCC that this procedure should be executed	Where the affected Subscriber is not a Network Party, the DCC shall disable processing of communications destined for Devices that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status to 'recovery'.	DCC	4.3.2.2
4.3.2.2	As soon as possible, following 4.3.2.1	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.3.1 of this document. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.3.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.3.2.3

Step	When	Obligation	Responsibility	Next Step
4.3.2.3	As soon as reasonably practicable, following 4.3.2.2	The affected Subscriber shall either: a) identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Private Key; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are not Digitally Signed by the Compromised Private Key. The affected Subscriber shall notify the DCC of the serial number of the replacement Organisation Certificate that should be used to populate a Device and specify the Device slot to which the replacement Organisation Certificate relates, which shall be provided via secured electronic means in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	Subscriber	4.3.2.4
4.3.2.4	As soon as reasonably practicable, following 4.3.2.3	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key.	DCC	4.3.2.5
4.3.2.5	As soon as reasonably practicable, following 4.3.2.4	The DCC shall send Commands to all Devices, Digitally Signed using the Recovery Private Key, in order to replace affected Organisation Certificates on relevant Devices as notified in step 4.3.1.1 with replacement Certificates as notified by the affected Subscriber. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise.	DCC	4.3.2.6
4.3.2.6	As soon as reasonably practicable, following 4.3.2.5	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected Devices: a) upon replacement of affected Certificates on each Device, using a DCC Alert issued via the DCC User Interface; and b) upon completion of attempts to replace all affected Certificates on relevant Devices, in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC, provided by secured electronic means.	DCC	4.3.2.7

Step	When	Obligation	Responsibility	Next Step
4.3.2.7	As soon as reasonably practicable, following 4.3.2.6	Upon completion of step 4.3.2.6 for each Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status for that Device to the SMI Status that was in place immediately prior to the execution of step 4.3.2.1 of this procedure.	DCC	4.3.2.8
4.3.2.8	As soon as reasonably practicable, following 4.3.2.7	The DCC shall notify each Responsible Supplier for affected Devices, by secured electronic means, which Devices were not recovered successfully in one or more one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	4.3.2.9
4.3.2.9	As soon as reasonably practicable, following the deadline as determined in step 4.3.1.7	For each affected Device that has an SMI Status of ‘recovery’ or ‘recovered’, the DCC shall restore the SMI Status that was in place immediately prior to the execution of step 4.3.2.1 of this procedure.	DCC	Procedure as set out in Section 4.3.3 of this document

4.3.3 Post-Recovery

The procedure as set out immediately below shall be used following execution of the procedures as set out in sections 4.3.1 and 4.3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.3.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.3.2 of this document	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.3 of this document.	DCC (DSP TAD)	4.3.3.2
4.3.3.2	As soon as reasonably practicable, following 4.3.3.1	The DCC shall notify the SMKI PMA, via a secured electronic means, of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC; and b) the number of Devices for which recovery was not successful.	DCC	End of procedure

5 Recovery using the Contingency Private Key

5.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following:

a) the notification of the Compromise (or suspected Compromise) of the Root OCA Private Key, in accordance with section 3.2 of this document; or

b) where the use of the Recovery Private Key has been unsuccessful (as set out in sections 4.2, 4.3, 6.2 and 6.3 of this document) and the DCC reasonably believes that the nature of the Compromise could require use of the Contingency Private Key.

Step	When	Obligation	Responsibility	Next Step
5.1.1	As soon as reasonably practicable, following notification of the Compromise (or suspected Compromise) of the Root OCA Private Key or escalation due to failure of recovery using the Recovery Private Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA and all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Root OCA Key has been notified, or that use of the Recovery Private Key has been unsuccessful that the DCC reasonably believes that the nature of the Compromise could require use of the Contingency Private Key. The DCC shall also provide details to affected Subscribers of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	5.1.2

Step	When	Obligation	Responsibility	Next Step
5.1.2	As soon as reasonably practicable, following 5.1.1	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Root OCA Private Key; c) the extent to which the vulnerabilities that caused the Compromise have been addressed; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery.	DCC	5.1.3
5.1.3	As soon as reasonably practicable, following 5.1.2	Where the DCC believes that use of the Contingency Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) inform the requisite number of Key Custodians, via a secured electronic means, that a Key Activation Ceremony for the Contingency Private Key is required (which may be greater than the minimum number required to activate the Contingency Private Key), and the date, time and location of each Key Activation Ceremony; b) notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and c) activities required to prepare the systems environment required to support activation and use of the Contingency Private Key.	DCC, Key Custodians	5.1.4

Step	When	Obligation	Responsibility	Next Step
5.1.4	As soon as reasonably practicable, following 5.1.3	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 5.1.2 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 5.1.5
5.1.5	As soon as reasonably practicable, following 5.1.4	The DCC shall notify affected Subscribers, via a secured electronic means, of the SMKI PMA's decision whether or not to execute the recovery procedure (amended as directed by the SMKI PMA) as set out in section 5.2.	DCC	Where required by SMKI PMA, 5.1.6; otherwise End of procedure
5.1.6	As soon as reasonably practicable, following 5.1.5	The DCC shall execute steps in order, where applicable in accordance with the SMKI PMA's decision, to revoke: a) the Root OCA Certificate; b) the Issuing OCA Certificate The DCC shall update and lodge the relevant ARL in the SMKI Repository and shall destroy affected Private Keys and Symmetric Keys, which may include: a) the old Root OCA Private Key; b) the old Issuing OCA Private Key; c) the old Contingency Private Key; and d) the old Contingency Symmetric Key.	DCC	Procedure as set out in section 5.2 of this document

5.2 Execution of Recovery Procedure

The DCC shall execute the steps as notified by the SMKI PMA, in accordance with the procedure in section 5.1 of this document, which may include (but will not be limited to) some or all of the steps as set out in this section 5.2.

Step	When	Obligation	Responsibility	Next Step
5.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that recovery using the Contingency Private Key should be carried out	The DCC shall disable processing of communications destined for Devices that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status to 'recovery'.	DCC	5.2.2
5.2.2	As soon as possible, following 5.2.1	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure.	Subscriber	5.2.3

Step	When	Obligation	Responsibility	Next Step
5.2.3	As soon as possible, following 5.2.2	The DCC shall temporarily amend the Anomaly Detection Thresholds, as required and including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in step 5.1.2; and b) affected Subscribers to allow submission of Service Requests to replace DCC Access Control Broker Certificates with new Organisation Certificates. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 5.2.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	5.2.4
5.2.4	As soon as reasonably practicable, following 5.2.3	The DCC, shall conduct relevant Key Generation Ceremonies in accordance with the Organisation CPS, in order to generate: a) a new Contingency Symmetric Key; b) a new Contingency Key Pair; c) a new wrappedApexContingencyKey; d) a new Root OCA Key Pair ; and e) a new Issuing OCA Key Pair.	DCC	5.2.5
5.2.5	As soon as reasonably practicable, following 5.2.4	The DCC shall generate a new Root OCA Certificate, embedding the new wrappedApexContingencyKey that has been generated as part of the process as set out in step 5.2.4 of this document. The new Root OCA Certificate shall be Digitally Signed by the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate, signed by the new Root OCA Private Key.	DCC (as TSP)	5.2.6
5.2.6	As soon as reasonably practicable, following 5.2.5	The DCC shall lodge the new Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.	DCC	5.2.7

Step	When	Obligation	Responsibility	Next Step
5.2.7	As soon as reasonably practicable, following 5.2.6	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Contingency Private Key and the plain text version of the Contingency Symmetric Key that were used to generate the wrappedApexContingencyKey that is stored within the Root OCA Certificate that has been deployed to Devices. To facilitate this, the DCC shall bring together all parts of the Contingency Symmetric Key.	DCC	5.2.8
5.2.8	As soon as reasonably practicable, following 5.2.7	The DCC shall send Commands to all Devices, Digitally Signed using the Contingency Private Key and including the Contingency Symmetric Key to enable activation, attaching the following Certificates (where applicable according to the Device type) to the corresponding Devices: a) a new Root OCA Certificate; b) a replacement new DCC Transitional CoS Certificate; c) a replacement new Recovery Certificate; d) a replacement new DCC Access Control Broker Certificate; e) a replacement new DCC WAN Provider Certificate; and f) a new DCC Access Control Broker Certificate which shall be placed in each Supplier Device slot or Network Operator Device slot in the corresponding Device.	DCC	5.2.9
5.2.9	As soon as reasonably practicable, following 5.2.8	Upon completion of step 5.2.8 for each Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status to 'recovered'.	DCC	5.2.10
5.2.10	As soon as reasonably practicable, following 5.2.9	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise.	DCC	5.2.11

Step	When	Obligation	Responsibility	Next Step
5.2.11	As soon as reasonably practicable, following 5.2.10	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected Devices: a) upon replacement of affected Certificates on each Device with a DCC Access Broker Certificate, via DCC Alert issued via the DCC User Interface to the affected Subscriber; and b) upon completion of attempts to replace all affected Certificates (for each affected Subscriber) on relevant Devices, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, which shall be provided via secured electronic means.	DCC	5.2.12
5.2.12	As soon as reasonably practicable, following 5.2.11	The DCC shall notify each Responsible Supplier for affected Devices, via secured electronic means, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, which Devices were not recovered successfully.	DCC	Procedure as set out in Section 5.3 of this document

5.3 Post Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Root OCA Private Key.

Step	When	Obligation	Responsibility	Next Step
5.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 5.2 of this document	The affected Subscriber shall either: a) identify replacement Organisation Certificates; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	5.3.2

Step	When	Obligation	Responsibility	Next Step
5.3.2	As soon as reasonably practicable, following 5.3.1	The Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace: a) the DCC Access Control Broker Certificate in each Supplier Device slot with a replacement Organisation Certificate that is Issued under the new Issuing OCA, for each Device as established in step 5.2.2 within section 5.2 of this document; and b) the DCC Access Control Broker Certificate in each Network Operator Device slot with an Organisation Certificate to which the Network Operator is the Subscriber that is Issued under the new Issuing OCA, for each Device as established in step 5.2.2 within section 5.2 of this document. Upon successful completion of such replacement for a Device, the DCC shall set the SMI Status for that Device to the SMI Status that was in place immediately prior to the execution of step 5.2.1 of this procedure. The Responsible Supplier shall notify the DCC in respect of replacement of affected Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	Subscriber	5.3.3
5.3.3	As soon as reasonably practicable, following the deadline as determined in step 5.1.4	For each affected Device that has an SMI Status of 'recovery' or 'recovered', the DCC shall restore the SMI Status that was in place immediately prior to the execution of step 5.2.1 of this procedure.	DCC	5.3.3

Step	When	Obligation	Responsibility	Next Step
5.3.4	As soon as reasonably practicable, following 5.3.3	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 5 of this document.	Subscriber, DCC (DSP TAD)	5.3.5
5.3.5	As soon as reasonably practicable, following 5.3.4	The DCC shall notify the SMKI PMA and affected Subscribers, via a secured means, of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.; and b) the number of Devices for which recovery was not successful.	DCC	End of procedure

6 Recovery from Compromise of a Contingency Private Key, Contingency Symmetric Key, Issuing OCA Private Key or Recovery Private Key

6.1 Recovery from Compromise of a Contingency Private Key or the Contingency Symmetric Key

6.1.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of the Contingency Private Key or the Contingency Symmetric Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.1.1.1	As soon as reasonably practicable, following notification of the Compromise (or suspected Compromise) of the Contingency Private Key or Contingency Symmetric Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Contingency Private Key or Contingency Symmetric Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.1.1.2
6.1.1.2	As soon as reasonably practicable, following 6.1.1.1	The DCC shall notify all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Contingency Private Key or Contingency Symmetric Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document.	DCC	6.1.1.3

Step	When	Obligation	Responsibility	Next Step
6.1.1.3	As soon as reasonably practicable, following 6.1.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Contingency Private Key; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery.	DCC, SMKI PMA	6.1.1.4
6.1.1.4	As soon as reasonably practicable, following 6.1.1.3	Where the DCC believes that replacement of the Contingency Key Pair and generation of a replacement Root OCA Certificate (and therefore a new Contingency Private Key and Contingency Symmetric Key) is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) informing the requisite number of Key Custodians, via a secured electronic means, that a Key Generation Ceremony for the Contingency Key Pairs is required and the date, time and location of each the Key Generation Ceremony; b) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony may be required; and c) activities required to prepare such systems environment required to support generation of a new Contingency Key Pair, Contingency Symmetric Key, Root OCA Key Pair and replacement Root OCA Certificate, Issuing OCA Key Pair and Issuing OCA Certificate that may be required.	DCC, Key Custodians	6.1.1.5

Step	When	Obligation	Responsibility	Next Step
6.1.1.5	As soon as reasonably practicable, following 6.1.1.4	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.1.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of procedure; otherwise 6.1.1.6
6.1.1.6	As soon as reasonably practicable, following 6.1.1.5	The DCC shall notify all affected Subscribers, via a secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.1.2.	DCC	Procedure as set out in section 6.1.2 of this document

6.1.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 6.1.1 of this document.

Step	When	Obligation	Responsibility	Next Step
6.1.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure.	Subscriber	6.1.2.2
6.1.2.2	As soon as reasonably practicable, following 6.1.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds; including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for the DCC and affected Responsible Suppliers to allow submission of Service Requests to replace the Root OCA Certificate on Devices. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	6.1.2.3

Step	When	Obligation	Responsibility	Next Step
6.1.2.3	As soon as reasonably practicable, following 6.1.2.2	The DCC shall conduct relevant Key Generation Ceremonies, in order to generate the following, in accordance with the Organisation CPS and the Great Britain Companion Specification (GBCS): a) a new Contingency Symmetric Key; b) a new Contingency Key Pair c) a new Root OCA Key Pair; d) a new Issuing OCA Key Pair and e) a new wrappedApexContingencyKey.	DCC (as TSP) for Contingency Symmetric Key; DCC (as DSP) for Contingency Key Pair	6.1.2.4
6.1.2.4	As soon as reasonably practicable, following 6.1.2.4	The DCC shall generate a replacement Root OCA Certificate, embedding the new wrappedApexContingencyKey that has been generated as part of the process as set out in step 6.1.2.3 of this document. The replacement Root OCA Certificate shall be Digitally Signed by the existing Root OCA Private Key and the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate, which shall be Digitally Signed by the new Root OCA Private Key.	DCC (as TSP)	6.1.2.5
6.1.2.5	As soon as reasonably practicable, following 6.1.2.4	The DCC shall lodge the replacement Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.	DCC	6.1.2.6

Step	When	Obligation	Responsibility	Next Step
6.1.2.6	As soon as reasonably practicable, following 6.1.2.5	The DCC shall notify, via secured electronic means: a) the target deadline for the submission of Service Requests to replace affected Root OCA Certificates on affected Devices, which shall be assessed by the DCC based on the number of Devices affected; and b) the replacement Root OCA Certificate serial number, which shall be provided in one or more Other Compromise Notification Files as set out in Appendix D of this document. Such notification shall be provided by the DCC to the organisation responsible, which shall be: a) for all Communications Hub Functions, the DCC (the Service Provider that is the provider of the WAN for the relevant Region); or b) for all other Devices, shall be the Responsible Supplier that is the Subscriber for the Organisation Certificate held in the supplier digital signing slot on that Device, for that Device.	DCC	6.1.2.7
6.1.2.7	As soon as reasonably practicable, following 6.1.2.6	The organisation as defined in step 6.1.2.6, shall retrieve the replacement Root OCA Certificate from the SMKI Repository and shall send such Service Requests, in accordance with the provisions of the DCC User Interface Specification, (or in the case of the DCC, issue such Commands) as are required to replace the existing Root OCA Certificate on all affected Devices with the new Root OCA Certificate.	Supplier	6.1.2.8

Step	When	Obligation	Responsibility	Next Step
6.1.2.8	As soon as reasonably practicable, following 6.1.2.7	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of replacement of the Root OCA Certificate. The DCC shall also monitor for unauthorised use of the Contingency Private Key and shall take all reasonable steps to keep the SMKI PMA informed as to such unauthorised use. Where directed to amend the recovery steps based on unauthorised use, the DCC execute steps as notified by the SMKI PMA. Following the deadline for Root OCA Certificate replacement as set out in step 6.1.2.7, the DCC shall identify whether recovery for all affected Devices has been successfully completed. Where recovery of all affected Devices has not been completed, the DCC shall notify, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, to each organisation as established in step 6.1.2.7 of the list of Devices where the replacement of Root OCA Certificates has not been successfully completed.	DCC (as DSP)	6.1.2.9
6.1.2.9	As soon as reasonably practicable, following 6.1.2.8	The DCC shall notify each Responsible Supplier for affected Devices which Devices were not recovered successfully, using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, via secured electronic means.	DCC	Procedure as set out in Section 6.1.3 of this document

6.1.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Contingency Private Key or the Contingency Symmetric Key.

Step	When	Obligation	Responsibility	Next Step
6.1.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 0 of this document, as applicable	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by an affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.1 of this document.	DCC (DSP TAD)	6.1.3.2
6.1.3.2	As soon as reasonably practicable, following 6.1.3.1	The DCC shall destroy the replaced Root OCA Private Key, Issuing OCA Private Key, Contingency Private Key and Contingency Symmetric Key.	DCC (as DSP, TSP)	6.1.3.3
6.1.3.3	As soon as reasonably practicable, following 6.1.3.2	The DCC shall notify the SMKI PMA, via a secured means of: a) whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document; and b) the number of Devices for which recovery was not successful.	DCC	End of procedure

6.2 Recovery from Compromise of the Recovery Private Key

6.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of the Recovery Private Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.2.1.1	As soon as reasonably practicable, following notification of the Compromise (or suspected Compromise) of the Recovery Private Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Recovery Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.2.1.2
6.2.1.2	As soon as reasonably practicable, following 6.2.1.1	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means that the Compromise of the Recovery Private Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification Files which comply with Appendix D of this document.	DCC	6.2.1.3

Step	When	Obligation	Responsibility	Next Step
6.2.1.3	As soon as reasonably practicable, following 6.2.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification Files which comply with Appendix D of this document; b) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Recovery Private Key; c) the extent to which the vulnerabilities that caused the Compromise have been addressed; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery.	DCC, SMKI PMA	6.2.1.4
6.2.1.4	As soon as reasonably practicable, following 6.2.1.3	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d) activities required to prepare such systems environment required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	6.2.1.5

Step	When	Obligation	Responsibility	Next Step
6.2.1.5	As soon as reasonably practicable, following 6.2.1.4	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.2.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 6.2.1.6
6.2.1.6	As soon as reasonably practicable, following 6.2.1.5	The DCC shall notify all Subscribers to Organisation Certificates, by secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.2.2.	DCC	Procedure as set out in section 6.2.2 of this document

6.2.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA in accordance with section 6.2.1 of this document, shall be used when a Recovery Private Key has been Compromised.

Step	When	Obligation	Responsibility	Next Step
6.2.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds for the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.2.1 of this document.	DCC (DSP TAD)	6.2.2.2
6.2.2.2	As soon as reasonably practicable, following 6.2.2.1	The DCC shall: a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key.	DCC, Key Custodians	6.2.2.3
6.2.2.3	As soon as reasonably practicable, following 6.2.2.2	The DCC shall: a) determine the number of Key Custodians required to attend a Key Generation Ceremony for the Recovery Private Key; b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c) participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate.	DCC, Key Custodians	6.2.2.4

Step	When	Obligation	Responsibility	Next Step
6.2.2.4	As soon as reasonably practicable, following 6.2.2.3	The DCC shall send Commands to all Devices to replace the Recovery Certificate held on such Devices with the Recovery Certificate generated in step 6.2.2.3. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure.	DCC (as DSP)	6.2.2.5
6.2.2.5	As soon as reasonably practicable, following 6.2.2.4	The DCC shall notify each Responsible Supplier for affected Devices, by secured electronic means, which Devices were not recovered successfully, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	Procedure as set out in Section 6.2.3 of this document

6.2.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Recovery Private Key, as set out in section 6.2.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.2.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.2.2 of this document, as applicable	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.2 of this document.	DCC (DSP TAD)	6.2.3.2
6.2.3.2	As soon as reasonably practicable, following 6.2.3.1	The DCC shall destroy the replaced Recovery Private Key and shall revoke the Recovery Certificate that has been replaced in the procedure as set out in Section 6.2.2 of this document.	DCC (as DSP)	6.2.3.3

Step	When	Obligation	Responsibility	Next Step
6.2.3.3	As soon as reasonably practicable, following 6.2.3.2	The DCC shall notify the SMKI PMA, via secured electronic means of: a) whether the recovery from the Compromise has been successfully completed; and b) the number of Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	End of procedure

6.3 Recovery from Compromise of the Issuing OCA Private Key

6.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of an Issuing OCA Private Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.3.1.1	As soon as reasonably practicable, following notification of the Compromise (or suspected Compromise) of an Issuing OCA Private Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA and each Subscriber to affected Organisation Certificates, via a secured electronic means, as soon as reasonably practicable, that a Compromise of an Issuing OCA Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.3.1.2
6.3.1.2	As soon as reasonably practicable, following 6.3.1.1	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means, the Compromise of the Issuing OCA Private Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document	DCC	6.3.1.3

Step	When	Obligation	Responsibility	Next Step
6.3.1.3	As soon as reasonably practicable, following 6.3.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Issuing OCA Private Key; c) the extent to which the vulnerabilities that caused the Compromise have been addressed; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise) e) anticipated timescales for recovery; and f) whether or not DCC is proposing to that multiple Compromises should be dealt with on a common basis and if so why the DCC proposes that they should be so treated.	DCC, SMKI PMA	6.3.1.4

Step	When	Obligation	Responsibility	Next Step
6.3.1.4	As soon as reasonably practicable, following 6.3.1.3	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d) activities required to prepare such systems environment required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	6.3.1.5
6.3.1.5	As soon as reasonably practicable, following 6.3.1.4	The SMKI PMA shall: a) determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.3.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	6.3.1.6

Step	When	Obligation	Responsibility	Next Step
6.3.1.6	As soon as reasonably practicable, following 6.3.1.5	The DCC shall notify all Subscribers to affected Organisation Certificates, via secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.3.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 6.3.1.7
6.3.1.7	As soon as reasonably practicable, following 6.3.1.6	The DCC shall revoke the Issuing OCA Certificate to which the affected Issuing OCA Private Key relates, and shall update and lodge the relevant Organisation ARL in the SMKI Repository. The DCC shall destroy the Issuing OCA Private Key that is Compromised or suspected to be Compromised.	DCC (as DSP)	Procedure as set out in Section 6.3.2 of this document

6.3.2 Execution of Recovery Procedure

The procedure as set out immediately below shall be executed in order to recover from the Compromise, or suspected Compromise of an Issuing OCA Private Key, following completion of the procedure as set out in section 6.3.1 of this document.

Step	When	Obligation	Responsibility	Next Step
6.3.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	A SMKI ARO acting on behalf of each affected Subscribers shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the Threshold Anomaly Detection Procedure.	Subscriber	6.3.2.2

Step	When	Obligation	Responsibility	Next Step
6.3.2.2	As soon as reasonably practicable, following 6.3.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds; including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for affected Subscribers to allow submission of Service Requests to replace affected Organisation Certificates on Devices. The DCC shall inform, via secured electronic means, a SMKI SRO acting and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended. The DCC shall amend its Anomaly Detection Thresholds that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of the affected Recovery Certificate on Devices.	DCC (DSP TAD)	6.3.2.3
6.3.2.3	As soon as reasonably practicable, following 6.3.2.2	The DCC shall generate a new Issuing OCA Key Pair and Issuing OCA Certificate, in accordance with the procedure as set out in the Organisation CPS.	DCC (as TSP)	6.3.2.4
6.3.2.4	As soon as reasonably practicable, following 6.3.2.3	The DCC shall: a) determine the number of Key Custodians required to attend a Key Generation Ceremony for the relevant Recovery Private Key; b) inform such Key Custodians in respect of the relevant Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c) participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate, Digitally Signed using the new Issuing OCA Private Key.	DCC, Key Custodians	6.3.2.5
6.3.2.5	As soon as reasonably practicable, following 6.3.2.4	The DCC shall: a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key);	DCC, Key Custodians	6.3.2.6

Step	When	Obligation	Responsibility	Next Step
		b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c) participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key.		
6.3.2.6	As soon as reasonably practicable, following 6.3.2.5	The DCC shall send Commands to all Devices to replace the Recovery Certificate held on such Devices with the Recovery Certificate generated in step 6.3.2.4. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure. The DCC shall notify each organisation as established in step 6.3.1.3, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, of the list of Devices where the replacement of the Recovery Certificate has been successfully completed.	DCC (as DSP)	6.3.2.7
6.3.2.7	As soon as reasonably practicable, following 6.3.2.6	Each affected Subscriber shall either: a) identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Issuing OCA Private Key; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are Digitally Signed by the new Issuing OCA Private Key.	Subscriber	6.3.2.8

Step	When	Obligation	Responsibility	Next Step
6.3.2.8	As soon as reasonably practicable, following 6.3.2.7	Each affected Subscriber shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, in order to replace all Organisation Certificates for which it is the Subscriber that are held on Devices and are signed using the Compromised Issuing OCA Private Key, with new Organisation Certificate as identified in accordance with step 6.3.2.7 that are signed by the new Issuing OCA Private Key that is generated in accordance with step 6.3.2.3. Following attempts to replace affected Certificates on Devices, each affected Subscriber shall notify the DCC in respect of replacement of affected Certificates with new Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	Subscriber	6.3.2.9
6.3.2.9	As soon as reasonably practicable, following 6.3.2.8	The DCC shall: a) monitor its records of replacement by affected Subscribers against the list as has been compiled in step 6.3.1.2, to identify successful replacement; b) identify any failures to replace affected Organisation Certificates that have been Digitally Signed using the Issuing OCA Private Key that has been Compromised; and c) monitor revocation of Organisation Certificates that are Digitally Signed using the Compromised Issuing OCA Private Key.	DCC	6.3.2.10
6.3.2.10	As soon as reasonably practicable, following 6.3.2.9	The DCC shall notify each Responsible Supplier for affected Devices, via secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, the Devices for which replacement of the Recovery Certificate or affected Organisation Certificates was not successfully completed.	DCC	Procedure as set out in Section 1.1.1 of this document

6.3.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of an Issuing OCA Private Key.

Step	When	Obligation	Responsibility	Next Step
6.3.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.3.2 of this document	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.2 of this document.	DCC (DSP TAD)	6.3.3.2
6.3.3.2	As soon as reasonably practicable, following 6.3.3.1	The DCC shall notify the SMKI PMA, via a secured electronic means of: a) whether the recovery from the Compromise has been successfully completed; and b) the number of Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	End of procedure

7 Periodic testing of the SMKI Recovery Procedure

7.1 Testing Arrangements

This section describes the DCC's obligations in respect of periodic testing of recovery procedures, in accordance with the provisions of Section L10.1(d) of the Code. At least once every year, the DCC shall:

g) develop a testing plan and a series of testing scenarios which the DCC will conduct in a systems environment which will only be accessible by the DCC, which are representative of the Enrolled Smart Metering Systems and shall take account of any lessons learned from each previous execution of the SMKI Recovery Procedure to recover from a Compromise or suspected Compromise. The testing plan and testing scenarios will be conducted by the DCC and may include (but shall not be limited to) the following:
   i. the means by which Key Custodians are notified and participate in Key Generation Ceremonies and/or Key Activation Ceremonies;
   ii. generation of new DCC Key Material, including the Contingency Key Pair, the Recovery Key Pair and the Contingency Symmetric Key used to encrypt the Contingency Public Key;
   iii. processes relating to interactions between the DCC and the SMKI PMA in order to determine what steps (if any) should be taken when the use of the Recovery Private Key or Contingency Private Key would be required to recover from a Compromise;
   iv. preparation of system environments required to support the SMKI Recovery Procedure;
   v. issuance of Commands that are Digitally Signed using the Recovery Private Key and/or Contingency Private Key, and validation that such Commands are successful;
   vi. testing of issuance of DCC Alerts following replacement of affected Certificates in accordance with the SMKI Recovery Procedure; and
   vii. transfer of files between DCC and Subscribers to support the execution of the SMKI Recovery Procedure.

h) develop a testing plan and a series of testing scenarios, and conduct such testing scenarios in a systems environment that is available to all Subscribers, which may include (but is not limited to) scenarios a)(vi) and a)(vii) as set out immediately above, along with replacement of Certificates on Devices that are initiated via Service Requests issued by Subscribers.

i) seek input from Subscribers to Organisation Certificates in relation to those testing scenarios that require participation by Subscribers, and take such input into account when proposing and agreeing the testing scenarios with the SMKI PMA;

j) agree such testing scenarios with the SMKI PMA;

k) create test data based upon data collected by the DCC and, where necessary, acquired from Parties;

l) maintain a test environment in order to carry out such periodic testing of the SMKI Recovery Procedure;

m) carry out testing of the SMKI Recovery Procedure for agreed scenarios; and

n) provide a report to the SMKI PMA and Subscribers to Organisation Certificates following periodic testing, which shall detail the success or otherwise of such testing, proposed amendments to the SMKI Recovery Procedure, and any issues arising that require PMA consideration.

In respect of periodic testing of the SMKI Recovery Procedure:

o) SMKI Users shall provide such reasonable assistance to the DCC as is required to support testing; and
p) The SMKI PMA shall review reports from periodic testing and shall direct the DCC, as necessary, to update the SMKI Recovery Procedure.

Appendix A Communication Formats

In Appendices B to E of this document, each of the CSV files specified shall be encoded using the ASCII character set and:

- must have a comma "," as the field separator;
- must have a line feed character 0x0A as the record separator, which in this section is indicated by the "▲" character; and
- may include consecutive comma separators to the left of a record separator to specify that a field has a null value. Where this is the case, DCC shall interpret consecutive commas within a record to indicate a null value.

Some spreadsheets output a carriage return line feed 0x0D0A as the record separator for CSV files and/or do not terminate CSV files with a record separator. Each User submitting a CSV file that is to be Digitally Signed using the Private Key associated with a File Signing Certificate shall, prior to Digitally Signing that file, ensure that:

- the CSV file is formatted to ensure that each record has a separator which is a 0x0A character and that any 0x0D character is removed from the file; and
- the CSV file is terminated with a 0x0A character.

Details of the function of the software utility and the method of Digital Signing of files to support the recovery procedures are contained within section 6 of the Threshold Anomaly Detection Procedure.

Appendix B Organisation Compromise Notification File

Each Organisation Compromise Notification File shall be in the format set out in this Appendix and shall have a filename of the form:

a) *OC_Priority_UserID_IncidentID_N_FileNum*.csv

Where:

a) *OC* denotes that the file relates an Organisation Compromise.
b) *Priority* contains an integer value which shall be set to a value of 1 or 2, where a lesser value denotes that the file has a higher priority than a file submitted in respect of the same Incident with a Priority field containing a higher value. Where the Subscriber submitting the Organisation Compromise Notification File wishes to apply a priority to Certificate replacement recovery activities, it shall determine such priority values and include the integer priority value within the filename for each Organisation Compromise Notification File submitted.
c) *UserID* contains the EUI-64 Compliant identifier for:
   - the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
   - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
   - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
d) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
e) *N* denotes that the file is a notification of affected Certificates and Devices.
f) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Organisation Compromise Notification File shall be generated in accordance with the procedure set out immediately below:

a) an “initial” CSV file shall be created, which shall contain the following records:
   - UserID ▲
   - Device_ID, Affected_Certificate_Serial_Number_DS, Affected_Certificate_Serial_Number_KAK, Affected_Certificate_Serial_Number_KAKPP, Replacement_Certificate_Serial_Number_DS, Replacement_Certificate_Serial_Number_KAK, Replacement_Certificate_Serial_Number_KAKPP *(repeated for each affected Device, with no more than 100,000 such records permitted within any file)* ▲
b) a File Signing Certificate_ID shall be appended to the end of the “initial” file, comprising:

- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
- the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

c) a Digital_Signature shall be generated from the concatenation of the "initial" CSV file and the File Signing Certificate_ID and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the Threshold Anomaly Detection Procedures.

Where:

a) The *UserID* field contains the EUI-64 Compliant identifier for:
   - the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
   - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
   - the DCC, where the file is being submitted to the SMKI PMA by the DCC.

b) The Device_ID field contains the Device ID.

c) The Affected_Certificate_Serial_Number_DS field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Digital Signing anchor slot on affected Devices.

d) The Affected_Certificate_Serial_Number_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Key Agreement Key anchor slot on affected Devices.

e) The Affected_Certificate_Serial_Number_KAKPP field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the pre-payment Key Agreement Key anchor slot on affected Devices. Where the Subscriber that is submitting the file is a Network Party, the Affected_Certificate_Serial_Number_KAKPP field shall not be populated.

f) The Replacement_Certificate_Serial_Number_DS field contains the Certificate serial number for the Certificate to be used to populate the Digital Signing Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

g) The Replacement_Certificate_Serial_Number_KAK field contains the Certificate serial number for the Certificate to be used to populate the Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

h) The Replacement_Certificate_Serial_Number_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the prepayment Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

i) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.

j) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Where multiple Organisation Compromise Notification Files are submitted by an affected Subscriber to the DCC in respect of single IncidentID, the DCC shall process the files in order of Priority value, where files with a lower Priority value shall be processed first.

Appendix C Organisation Compromise Recovery Progress File

Each Organisation Compromise Recovery Progress File shall be in the format set out in this Appendix and shall have a filename of the form:

a) *OC_Priority_UserID_IncidentID_P_FileNum*.csv

Where:

a) *OC* denotes that the file relates an Organisation Compromise.
b) *Priority* contains an integer value which shall be set to 1 or 2, where a lesser value denoting that the file has a higher priority than a file submitted in respect of the same Incident with a Priority field containing a higher value. Such priority values shall have the same value as the corresponding Organisation Compromise Notification File.
c) *UserID* contains the EUI-64 Compliant identifier for:
   - the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
   - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
   - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
d) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
e) *P* denotes that the file is a notification of progress in respect of replacement of affected Certificates and Devices.
f) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Organisation Compromise Recovery Progress File shall be generated in accordance with the procedure set out immediately below:

a) an “initial” CSV file shall be created, which shall contain the following records:

   - UserID ▲
   - Device_ID, Affected_Certificate_Serial_Number_DS, Affected_Certificate_Serial_Number_KAK, Affected_Certificate_Serial_Number_KAKPP, Replacement_Certificate_Serial_Number_DS, Replacement_Certificate_Serial_Number_KAK, Replacement_Certificate_Serial_Number_KAKPP, Replacement_Status_DS, Replacement_Status_KAK, Replacement_Status_KAKPP *(repeated for each affected Device, with no more than 100,000 such records permitted within any file)* ▲

b) a File Signing Certificate_ID shall be appended to the end of the "initial" CSV file, comprising:

- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
- the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

c) a Digital_Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the Threshold Anomaly Detection Procedures.▲,

Where:

a) The UserID field contains the EUI-64 Compliant identifier for:
   - the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
   - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
   - the DCC, where the file is being submitted to the SMKI PMA by the DCC.

b) The Device_ID field contains the Device ID.

c) The Affected_Certificate_Serial_Number_DS field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Digital Signing anchor slot on affected Devices, where applicable.

d) The Affected_Certificate_Serial_Number_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Key Agreement Key anchor slot on affected Devices, where applicable.

e) The Affected_Certificate_Serial_Number_KAKPP field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the pre-payment Key Agreement Key anchor slot on affected Devices, where applicable.

f) The Replacement_Certificate_Serial_Number_DS field contains the Certificate serial number for the Certificate to be used to populate the Digital Signing Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

g) The Replacement_Certificate_Serial_Number_KAK field contains the Certificate serial number for the Certificate to be used to populate the Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

h) The Replacement_Certificate_Serial_Number_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the prepayment Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

i) The Replacement_Status_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement information from the affected Certificate in the Digital Signing anchor slot on a Device.

j) The Replacement_Status_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Key Agreement Key anchor slot on a Device.

k) The Replacement_Status_KAKPP field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the prepayment Key Agreement Key anchor slot on a Device.

l) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.

m) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Appendix D Other Compromise Notification File

Each Other Compromise Notification File shall be in the format set out in this Appendix and shall have a filename of the form:

a) *OTH_UserID_IncidentID_N_FileNum*.csv

Where:

a) *OTH* denotes that the file relates to notification of affected Devices for a Compromise not applicable to Appendices B or C of this document.
b) *UserID* contains the EUI-64 Compliant identifier for:
   - the Subscriber to which the file is being provided unless the file is being submitted to the SMKI PMA; or
   - the EUI-64 Compliant identifier for the DCC where the file is being submitted to the SMKI PMA.
c) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
d) *N* denotes that the file is a notification of affected Certificates and Devices.
e) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Other Compromise File shall contain the following records:

a) UserID ▲
b) Device_ID, Affected_Certificate_Serial_Number_Root, Affected_Certificate_Serial_Number_Recovery, Affected_Certificate_Serial_Number_Supplier_DS, Affected_Certificate_Serial_Number_Supplier_KAK, Affected_Certificate_Serial_Number_Supplier_KAKPP, Affected_Certificate_Serial_Number_NetworkOperator_DS, Affected_Certificate_Serial_Number_NetworkOperator_KAK, Affected_Certificate_Serial_Number_COS_DS, Affected_Certificate_Serial_Number_WAN_DS, Replacement_Certificate_Serial_Number_Root, Replacement_Certificate_Serial_Number_Recovery, Replacement_Certificate_Serial_Number_Supplier_DS, Replacement_Certificate_Serial_Number_Supplier_KAK, Replacement_Certificate_Serial_Number_Supplier_KAKPP, Replacement_Certificate_Serial_Number_NetworkOperator_DS, Replacement_Certificate_Serial_Number_NetworkOperator_KAK, Replacement_Certificate_Serial_Number_COS_DS, Replacement_Certificate_Serial_Number_WAN_DS *(repeated for each affected Device, with no more than 100,000 such records permitted within any file)* ▲

Where:

a) The UserID field contains the EUI-64 Compliant identifier for:
   - the Subscriber to which the file is being provided unless the file is being submitted to the SMKI PMA; or
   - the EUI-64 Compliant identifier for the DCC where the file is being submitted to the SMKI PMA.

b) The Device_ID field contains the Device ID.

c) The Affected_Certificate_Serial_Number_Root field contains the Certificate serial number of the Root OCA Certificate affected by the Compromise that is used to populate the Root anchor slot on affected Devices, where applicable.

d) The Affected_Certificate_Serial_Number_Recovery field contains the Certificate serial number of the Recovery Certificate affected by the Compromise that is used to populate the Recovery anchor slot on affected Devices, where applicable.

e) The Affected_Certificate_Serial_Number_Supplier_DS field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Supplier Digital Signing anchor slot on affected Devices, where applicable.

f) The Affected_Certificate_Serial_Number_Supplier_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Supplier Key Agreement Key anchor slot on affected Devices, where applicable.

g) The Affected_Certificate_Serial_Number_Supplier_KAKPP field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Supplier pre-payment Key Agreement Key anchor slot on affected Devices, where applicable.

h) The Affected_Certificate_Serial_Number_NetworkOperator_DS field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Network Operator Digital Signing anchor slot on affected Devices, where applicable.

i) The Affected_Certificate_Serial_Number_NetworkOperator_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Network Operator Key Agreement Key anchor slot on affected Devices, where applicable.

j) The Affected_Certificate_Serial_Number_COS_DS field contains the Certificate serial number of the TCoS Certificate affected by the Compromise that is used to populate the TCoS anchor slot on affected Devices, where applicable.

k) The Affected_Certificate_Serial_Number_WAN_DS field contains the Certificate serial number of the WAN Provider Certificate affected by the Compromise that is used to populate the WAN Provider anchor slot on affected Devices, where applicable.

l) The Replacement_Certificate_Serial_Number_Root field contains the Certificate serial number for the Certificate to be used to populate the Device Root anchor slot, where applicable.

m) The Replacement_Certificate_Serial_Number_Recovery field contains the Certificate serial number for the Certificate to be used to populate the Device Recovery anchor slot, where applicable.

n) The Replacement_Certificate_Serial_Number_Supplier_DS field contains the Certificate serial number for the Certificate to be used to populate the Supplier Digital Signing Device anchor slot, where applicable.

o) The Replacement_Certificate_Serial_Number_Supplier_KAK field contains the Certificate serial number for the Certificate to be used to populate the Supplier Key Agreement Key Device anchor slot, where applicable.

p) The Replacement_Certificate_Serial_Number_Supplier_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the Supplier prepayment Key Agreement Key Device anchor slot, where applicable.

q) The Replacement_Certificate_Serial_Number_NetworkOperator_DS field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Digital Signing Device anchor slot, where applicable.

r) The Replacement_Certificate_Serial_Number_NetworkOperator_KAK field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Key Agreement Key Device anchor slot, where applicable.

s) The Replacement_Certificate_Serial_Number_COS_DS field contains the Certificate serial number for the Certificate to be used to populate the Device TCoS anchor slot, where applicable.

t) The Replacement_Certificate_Serial_Number_WAN_DS field contains the Certificate serial number for the Certificate to be used to populate the Device WAN Provider anchor slot, where applicable.

Appendix E Other Compromise Recovery Progress File

Each Other Compromise Recovery Progress File shall be in the format set out in this Appendix and shall have a filename of the form:

a) *OTH_UserID_IncidentID_P_FileNum*.csv

Where:

a) *OTH* denotes that the file relates to notification of affected Devices for a Compromise not applicable to Appendices B or C of this document.
b) *UserID* contains the EUI-64 Compliant identifier for:
   - the Subscriber submitting the file, where a Subscriber is submitting the file to the DCC;
   - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to the Subscriber by the DCC; or
   - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
c) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
d) *P* denotes that the file is a notification of progress in respect of replacement of affected Certificates and Devices.
e) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Other Compromise File shall be generated in accordance with the procedure set out immediately below:

a) an "initial" CSV file shall be created, which shall contain the following records:

   - UserID ▲
   - Device_ID, Replacement_Certificate_Serial_Number_Root, Replacement_Certificate_Serial_Number_Recovery, Replacement_Certificate_Serial_Number_Supplier_DS, Replacement_Certificate_Serial_Number_Supplier_KAK, Replacement_Certificate_Serial_Number_Supplier_KAKPP, Replacement_Certificate_Serial_Number_NetworkOperator_DS, Replacement_Certificate_Serial_Number_NetworkOperator_KAK, Replacement_Certificate_Serial_Number_COS_DS, Replacement_Certificate_Serial_Number_WAN_DS, Replacement_Status_Root, Replacement_Status_Recovery, Replacement_Status_Supplier_DS, Replacement_Status_Supplier_KAK, Replacement_Status_Supplier_KAKPP, Replacement_Status_NetworkOperator_DS, Replacement_Status_NetworkOperator_KAK, Replacement_Status_COS_DS, Replacement_Status_WAN_DS

(repeated for each affected Device, with no more than 100,000 such records permitted within any file) ▲

b) a File Signing Certificate_ID shall be appended to the end of the "initial" CSV file, comprising:
   - all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
   - the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and

c) a Digital_Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the Threshold Anomaly Detection Procedures.

Where:

a) The UserID field contains the EUI-64 Compliant identifier for:
   - the Subscriber submitting the file, where a Subscriber is submitting the file to the DCC;
   - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to the Subscriber by the DCC; or
   - the DCC, where the file is being submitted to the SMKI PMA by the DCC.

b) The Device_ID field contains the Device ID.

c) The Replacement_Certificate_Serial_Number_Root field contains the Certificate serial number for the Certificate to be used to populate the Device Root anchor slot.

d) The Replacement_Certificate_Serial_Number_Recovery field contains the Certificate serial number for the Certificate to be used to populate the Device Recovery anchor slot.

e) The Replacement_Certificate_Serial_Number_Supplier_DS field contains the Certificate serial number for the Certificate to be used to populate the Supplier Digital Signing Device anchor slot.

f) The Replacement_Certificate_Serial_Number_Supplier_KAK field contains the Certificate serial number for the Certificate to be used to populate the Supplier Key Agreement Key Device anchor slot.

g) The Replacement_Certificate_Serial_Number_Supplier_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the Supplier prepayment Key Agreement Key Device anchor slot.

h) The Replacement_Certificate_Serial_Number_NetworkOperator_DS field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Digital Signing Device anchor slot.

i) The Replacement_Certificate_Serial_Number_NetworkOperator_KAK field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Key Agreement Key Device anchor slot.

j) The Replacement_Certificate_Serial_Number_COS_DS field contains the Certificate serial number for the Certificate to be used to populate the Device TCoS anchor slot.

k) The Replacement_Certificate_Serial_Number_WAN_DS field contains the Certificate serial number for the Certificate to be used to populate the Device WAN Provider anchor slot.

l) The Replacement_Status_Root field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Root anchor slot on a Device.

m) The Replacement_Status_Recovery field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Recovery anchor slot on a Device.

n) The Replacement_Status_Supplier_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Digital Signing anchor slot on a Device.

o) The Replacement_Status_Supplier_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Key Agreement Key anchor slot on a Device.

p) The Replacement_Status_Supplier_KAKPP field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier prepayment Key Agreement Key anchor slot on a Device.

q) The Replacement_Status_NetworkOperator_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Digital Signing anchor slot on a Device.

r) The Replacement_Status_NetworkOperator_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Key Agreement Key anchor slot on a Device.

s) The Replacement_Status_COS_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue,

in relation to the replacement of information from the affected Certificate in the TCoS anchor slot on a Device.

t) The Replacement_Status_WAN_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the WAN Provider anchor slot on a Device.

u) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.

v) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Appendix F Definitions

Term	Definition
Chief Information Security Officer	Means a senior security officer within a Party who is responsible for activities including (but not limited to) establishing and maintaining the security vision, strategy, information security governance framework, secure asset and infrastructure control framework, and security risk management program
Data Services Provider, or DSP	Means the DCC acting from those systems identified in part a) of the definition of DCC Live Systems
DSP Threshold Anomaly Detection, or DSP TAD	Means the DCC acting using those systems identified in Part (b) of the definition of DCC Live Systems
Key Activation Ceremony	Means a meeting at which a Private Key or Symmetric Key is activated by the DCC and/or Key Custodians, such that the Private Key or Symmetric Key may be used
Key Generation Ceremony	Means a meeting at which a Private Key or Contingency Symmetric Key is generated by the DCC and Key Custodians
Key Component	Means part of a Key or part of Activation Data used to protect a Key.
Key Custodian	Means an individual, appointed in accordance with section 3.4 of the SMKI Recovery Procedure, to hold a key which may be used as part of the process to access a Key Component.
Organisation Compromise Notification File	A CSV file used to support recovery from a Compromise that is specified in Appendix B of the SMKI Recovery Procedure
Organisation Compromise Recovery Progress File	A CSV file used to support recovery from a Compromise that is specified in Appendix C of the SMKI Recovery Procedure
Other Compromise Notification File	A CSV file used to support recovery from a Compromise that is specified in Appendix D of the SMKI Recovery Procedure
Other Compromise Recovery Progress File	A CSV file used to support recovery from a Compromise that is specified in Appendix E of the SMKI Recovery Procedure
Trusted Service Provider, or TSP	Means the DCC acting using systems identified in part (d) of the definition of DCC Live Systems