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).

Alt HAN Forum means the body of that name established in accordance with Section Z.1.1 (Establishment of the Alt HAN Forum).

Alt HAN Services has the meaning given to that expression in Section Z6.1 (Definitions).

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 ID used by a User in one or more of its User Roles, a number of communications within a period of time, where both that number and the period of time are set by the User in relation to that User ID;

(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.

Applicability Period has the meaning given to that expression in Section A3.26(d) (GB Companion Specification and CPA Security Characteristics)

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 Unambiguous 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.

Authority-Led Modification Report has the meaning given to that expression in Section D9A.5 (Authority-Led Modification Report).

Authority-Led Variations means variations to this Code proposed by the Authority pursuant to a direction under Section D9A (Authority-Led Variations).

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 (or, for the purposes of any Certificate Policy in which the term is defined, it shall have the meaning ascribed to it in that Certificate Policy).

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 I 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 any electronic Data, to check the Digital Signature or Message Authentication Code within 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 those Data identify, or 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 R, 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).

CPA Security Characteristics means the documents published from time to time on the CESG website that set out the features, testing and deployment requirements necessary to obtain a CPA Certificate in respect of one or more of the following:

(a) Gas Smart Metering Equipment;

(b) Electricity Smart Metering Equipment;

(c) Communications Hub Functions;

(d) HAN Connected Auxiliary Load Control Switches.

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.

CSV file has the meaning given to that expression in the Threshold Anomaly Detection Procedures.

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 S.

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 V, 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 T, 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 W, 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 V, 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 U, 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 any electronic Data, a digital signature generated using:

(a) the entirety of those Data (excluding the digital signature itself and, to the extent specified in the code, any other parts of 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 any electronic Data, that such Data have had the necessary Digital Signatures applied to 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.

EII DCCKICA Certificate Revocation List (or EII DCCKICA CRL) 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 Licence means a licence granted, or treated as granted, under 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~~ 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~~ any ~~version~~ Version of the SMETS with a Principal Version number of 1 ~~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 means the DCC Total System, all Enrolled Smart

Metering System 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).

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.

File Signing Software means software provided by the DCC for the purposes of enabling a Party to apply a Digital Signature to a CSV File.

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~~ 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~~ 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~~any Version of the SMETS with a Principal Version number of 1 ~~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~~ 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 means the part(s) of the SMETS identified as applying

Specification 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~~ 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 Q.

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).

IKI File Signing Certificate means an IKI Certificate issued by the IKI File Signing Certification Authority.

IKI File Signing Certification Authority has the meaning given to that expression in the IKI Certificate Policy.

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 Scheme has the meaning given to that expression in Part 2.1 of 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 G2.45(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.

Installation End Date has the meaning given to that expression in Section A3.12(b) (The Installation Validity Period).

Installation Start Date has the meaning given to that expression in Section A3.12(a) (The Installation Validity Period).

Installation Validity Period has the meaning given to that expression in Section A3.11 (The Installation Validity Period).

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.

Maintenance End Date has the meaning given to that expression in Section A3.16(b) (The Maintenance Validity Period).

Maintenance Start Date has the meaning given to that expression in Section A3.16(a) (The Maintenance Validity Period).

Maintenance Validity Period has the meaning given to that expression in Section A3.15 (The Maintenance Validity Period).

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.

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; or (b) a risk of material disruption.

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 Catalogue means the SEC Subsidiary Document of that name set 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 Consultation has the meaning given to that expression in Section 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 G2.45(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~~2015/1535/EU.

~~**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 (or SECCo) by the Code Administrator pursuant to Section B1.17 (Party Signifiers), which uniquely identifies that Party (or SECCo) 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.

Personnel Authentication Certificate has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.

Personnel Authentication Certificate Application has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.

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~~ 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).

Principal Version in relation to:

(a) a Technical Specification, has the meaning given to that expression in Section A3.5(a) (Versions of the Technical Specifications); and

(b) the GBCS or CPA Security Characteristics, has the equivalent meaning, in accordance with and subject to the provisions of Section A3.23 (GB Companion Specification and CPA Security Characteristics).

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 Entry Process Tests has the meaning given to that expression in Section E4.2 (RDP Entry Process Tests).

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 set out in Appendix Y~~ 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 set out in Appendix X~~ 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.

SEC Variation Testing Approach Documents means the SEC Subsidiary Documents set out in Appendix [TBC].

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 (including where the Authority issues a direction under Section D5.7 (SCR: Backstop Direction) or proposes an Authority-Led Variation), and ending on the earlier of:

(a) the date on which the Authority, or DCC at the direction of the Authority, 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) where the Authority has proposed an Authority-Led Variation, the date on which the Authority makes a decision in accordance with Section D9A.11 (Authority Decision);

(~~b~~c) 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~~d) the date 28 days after the date on which the Authority issues its conclusion document in respect of the Significant Code Review.

SIMCH Aerial means an aerial and any other equipment required to enable a Special Installation Mesh Communications Hub to connect to the SM WAN.

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 Card Token has the meaning given to that expression in Annex A of the DCCKI Certificate Policy.

Smart Meter means either an Electricity Smart Meter or a Gas Smart Meter (as the context requires).

Smart Metering Equipment Technical Specification means the document(s) set out in Schedule [TBC].

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;

(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;

(h) 'recovery', indicating that communications to the Device have been disabled in accordance with the SMKI Recovery Procedures; or

(i) 'recovered', indicating that communications to the Device have been restored in accordance with the SMKI Recovery Procedures.

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 N, 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 M, 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 L, 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 P, 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 O, 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 means a description of the overall technical

Information 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 south 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).

Sub-Version in relation to:

(a) a Technical Specification, has the meaning given to that expression in Section A3.5(b) (Versions of the Technical Specifications); and

(b) the GBCS or CPA Security Characteristics, has the equivalent meaning, in accordance with and subject to the provisions of Section A3.23 (GB Companion Specification and CPA Security Characteristics).

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 ID used by a User in one or more of its User Roles, 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 ID 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).

TS Applicability Tables means the document set out in Schedule [X] which has the content described at Section A3.29 (The TS Applicability Tables).

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

Unambiguous 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, taken a positive step amounting to a clear communication of that consent.

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 Assurance Service Provider has the meaning given to that expression in Section 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) but excluding communications in relation to Devices that do not have an SMI Status of "commissioned" or "installed not commissioned"; and/or

(f) 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.

Version in relation to:

(a) a Technical Specification, has the meaning given to that expression in Section A3.2 (Versions of the Technical Specifications); and

(b) the GBCS or CPA Security Characteristics, has the meaning given to that expression in Section A3.22 (GB Companion Specification and CPA Security Characteristics),

and in each case includes both the Principal Version and Sub-Version of that document.

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.

A3 TECHNICAL SPECIFICATIONS, THE GB COMPANION SPECIFICATION AND THE CPA SECURITY CHARACTERISTICS

Introduction

A3.1 This Section A3 makes provision in relation to:

(a) the maintenance in this Code of different versions of each of the Technical Specifications;

(b) the relationship between each version of a Technical Specification and:

(i) the GB Companion Specification; and

(ii) the CPA Security Characteristics; and

(c) the interpretation of the Code in respect of the Technical Specifications, GB Companion Specification, and CPA Security Characteristics.

Versions of the Technical Specifications

A3.2 Each Technical Specification may exist in more than one version (a "**Version**").

A3.3 Each Version of a Technical Specification shall consist of two elements:

(a) a Principal Version; and

(b) a Sub-Version of that Principal Version.

A3.4 Each Version of a Technical Specification shall be identified by a numerical reference in a form equivalent to 'SMETS v 1.2', where:

(a) the number before the decimal point identifies the Principal Version; and

(b) the number after the decimal point identifies the Sub-Version.

A3.5 In respect of any Technical Specification:

(a) the expression "**Principal Version**" shall be interpreted in accordance with Sections A3.6 to A3.7; and

(b) the expression "**Sub-Version**" shall be interpreted in accordance with Sections

A3.8 to A3.9.

The Principal Version

A3.6 Where a Technical Specification is amended in a manner that is entirely prospective, that amendment shall be made by creating a new Principal Version, and:

(a) for this purpose a prospective amendment means one that does not require any change to be made to any Device or apparatus which is already installed;

(b) in consequence a new Principal Version shall be taken to indicate amendments which have no retrospective effect.

A3.7 The first Principal Version of a Technical Specification shall be allocated the number 1, and subsequent Principal Versions of that Technical Specification shall be allocated sequential numbers in the chronological order in which they are created.

The Sub-Version

A3.8 Where any Principal Version of a Technical Specification is amended in a manner that is intended to have retrospective effect, that amendment shall be made by creating a new Sub-Version, and for these purposes:

(a) a Sub-Version means a new form of the Principal Version to which it relates;

(b) an amendment with retrospective effect means one that requires a change to be made to Devices or apparatus which are already installed.

A3.9 The initial form of a Principal Version of a Technical Specification shall be allocated the Sub-Version number of zero, and subsequent Sub-Versions shall be allocated sequential numbers, beginning with 1, in the chronological order in which they are created.

The Installation Validity Period

A3.10 Any Version of a Technical Specification may be assigned an Installation Validity Period.

A3.11 An "**Installation Validity Period**" means the period of time during which any Device or apparatus satisfying the requirements of that Version of the Technical Specification may be installed or provided.

A3.12 An Installation Validity Period shall:

(a) commence on the "**Installation Start Date**" that is identified in relation to that Version of the Technical Specification in the TS Applicability Tables; and

(b) end on any "**Installation End Date**" that may be identified in relation to that Version of the Technical Specification in the TS Applicability Tables.

A3.13 The Installation End Date of any Version of a Technical Specification may be later than the Installation Start Date of a Version that succeeds it, so that:

(a) two or more Versions may be within their Installation Validity Periods at the same time; and

(b) any Device or apparatus to which each such Version relates may be installed or provided in accordance with any such Version that is within its Installation Validity Period at that time.

The Maintenance Validity Period

A3.14 Each Version of a Technical Specification shall be assigned a Maintenance Validity Period.

A3.15 A "**Maintenance Validity Period**" means the period of time during which a Device or other apparatus may be maintained in accordance with the requirements of that Version of the Technical Specification.

A3.16 A Maintenance Validity Period shall:

(a) commence on the "**Maintenance Start Date**" that is identified in relation to that Version of the Technical Specification in the TS Applicability Tables; and

(b) end on any "**Maintenance End Date**" that may be identified in relation to that Version of the Technical Specification in the TS Applicability Tables.

A3.17 The Maintenance End Date of any Version of a Technical Specification may be later than the Maintenance Start Date of a Version that succeeds it, so that:

(a) two or more Versions may be within their Maintenance Validity Periods at the same time; and

(b) any Device or apparatus to which each such Version relates may be maintained in accordance with any such Version that is within its Maintenance Validity Period at that time.

Versions in the Code

A3.18 The Schedule of the Code in which any Technical Specification is set out shall consist of a number of parts, each of which shall correspond to and comprise a Version of that Technical Specification, so that (for example) CHTS v 2.1 shall be set out at Schedule [X] Part 2.1.

A3.19 Each Version of a Technical Specification shall be retained in the relevant Schedule to the Code at all times during which it remains within its Installation Validity Period (if any) and/or its Maintenance Validity Period.

A3.20 Where, in respect of any Version of a Technical Specification:

(a) no Installation Validity Period has been assigned, or any Installation Validity Period that was assigned has expired; and

(b) the Maintenance Validity Period has expired,

that Version shall be deemed automatically to be deleted from the Code on the day immediately following whichever is the later of its Installation End Date (if any) or Maintenance End Date, and the part of the Schedule in which it is set out shall then automatically be marked ‘Not Used’.

A3.21 The Code Administrator shall at all times maintain on the Website copies of those Versions of each Technical Specification which have been deleted from the Code in accordance with Section A3.20, together with a record of the Installation Start and End Dates (if any) and the Maintenance Start and End Dates relating to each such

Version.

GB Companion Specification and CPA Security Characteristics

A3.22 The GB Companion Specification and the CPA Security Characteristics may each exist in more than one version (a "**Version**").

A3.23 The provisions of Sections A3.3 to A3.9 shall apply to the GBCS and CPA Security Characteristics:

(a) as if references in those Sections to a Technical Specification were references to each of those documents; and

(b) in respect of the CPA Security Characteristics, so that:

(i) any reference in those Sections to the creation of a new Version by an amendment that requires a change to be made to a Device or apparatus which is already installed shall be read as if it were a reference to an amendment requiring the Device Model of a Device or apparatus which is already installed to be certified, on the expiry of its CPA Certificate, against the new Version of the CPA Security Characteristics; and

(ii) Section A3.35 shall be interpreted accordingly.

A3.24 The provisions of Sections A3.18 to A3.21 shall apply to the GBCS as if references in those Sections:

(a) to a Technical Specification were references to the GBCS;

(b) to an Installation Validity Period or Maintenance Validity Period were to an Applicability Period; and

(c) to an Installation Start or End Date, or a Maintenance Start or End Date, were to the first and last dates of the Applicability Period.

A3.25 Each Technical Specification requires that the Device or other apparatus to which it relates must be compatible with a relevant Version of the GBCS.

A3.26 For these purposes:

(a) the relevant Version of the GBCS in relation to any Version of a Technical Specification shall be deemed to be that which is specified in relation to it in the TS Applicability Tables;

(b) more than one Version of the GBCS may be relevant to a Version of a Technical Specification at the same time;

(c) a Version of the GBCS may be relevant to more than one Version of a Technical Specification at the same time;

(d) a Version of the GBCS shall be relevant to a Version of a Technical Specification only during such period of time (in each case, an "**Applicability Period**") as may be specified in the TS Applicability Tables.

A3.27 Each Version of the GBCS requires that the Device or other apparatus must be certified as compliant with a relevant Version of the CPA Security Characteristics.

A3.28 For these purposes:

(a) the relevant Version of the CPA Security Characteristics in relation to any Version of the GBCS shall be deemed to be that which is specified in relation to it in the TS Applicability Tables;

(b) more than one Version of the CPA Security Characteristics may be relevant to a Version of the GBCS at the same time;

(c) a Version of the CPA Security Characteristics may be relevant to more than one Version of the GBCS at the same time.

The TS Applicability Tables

A3.29 There shall be a document to be known as the "**TS Applicability Tables**", which shall be set out at Schedule [X] to the Code and shall include:

(a) in relation to each Technical Specification, a list of each of the Versions of that Technical Specification that have been produced;

(b) in relation to each such Version of that Technical Specification:

(i) the Installation Start Date;

(ii) the Installation End Date (or a statement that no such date has yet been determined);

(iii) the Maintenance Start Date;

(iv) the Maintenance End Date (or a statement that no such date has yet been determined);

(v) the relevant Version(s) of the GBCS;

(vi) any Applicability Period relating to any such relevant Version of the GBCS; and

(c) in relation to each Version of the GBCS, the relevant Version(s) of the CPA Security Characteristics.

A3.30 The TS Applicability Tables shall be amended to ensure that it remains accurate and up-to-date:

(a) on the designation or re-designation of a Technical Specification in accordance with Section X5 (Incorporation of Certain Documents into this Code), by the Secretary of State in reliance on Section X5.6 (Supplementary Provisions); and

(b) as part of any modification of the Code which creates a new Version of any Technical Specification or of the GBCS in accordance with Section D (Modification Process).

A3.31 Where the TS Applicability Tables is amended (including by the means described in Section A3.30) the amendment may have retrospective effect, which is to say that any date specified in the TS Applicability Tables by virtue of that amendment may be a date which falls before the date on which the amendment was made.

A3.32 The information set out in the TS Applicability Tables shall be regarded as conclusive for all purposes of any question as to the:

(a) Installation Validity Period of any Version of a Technical Specification;

(b) Maintenance Validity Period of any Version of a Technical Specification;

(c) relevant Version(s) of the GBCS in relation to any Version of a Technical Specification;

(d) Applicability Period of any Version of the GBCS; and

(e) relevant Version(s) of the CPA Security Characteristics in relation to any version of the GBCS.

DCC User Interface Specification and Message Mapping Catalogue

A3.33 The DCC User Interface Specification may exist in more than one version.

A3.34 Where there is more than one version of the DCC User Interface Specification:

(a) there shall be, in respect of each such version, a corresponding version of the Message Mapping Catalogue;

(b) a User may submit any Service Request, in respect of which it is an Eligible User, in accordance with any version of the DCC User Interface Specification;

(c) in accordance with the requirements of each version of the DCC User Interface Specification, each such Service Request must identify the version of the DCC User Interface Specification under which it has been submitted;

(d) any obligation on the DCC or any User in relation to any Service Request or associated communication shall be interpreted by reference to the provisions of the version of the DCC User Interface Specification that is identified in that Service Request;

(e) the obligation on the DCC at Section H11.1 (Parse and Correlate Software) to provide Parse and Correlate Software shall be interpreted as an obligation to provide a separate version of the Parse and Correlate Software in respect of each version of the DCC User Interface Specification (and the corresponding version of the Message Mapping Catalogue); and

(f) any other obligation on the DCC under this Code in relation to the Parse and Correlate Software shall be read as an obligation applying separately in respect of each such version of that software.

Interpretation

A3.35 References in this Section A3 to amendments of a Technical Specification which do (or do not) require changes to be made to any Device or apparatus which is already installed shall be interpreted as references to the effect of those amendments on the duties of:

(a) Electricity and Gas Supplier Parties in accordance with the standard conditions of the Energy Supply Licences; and

(b) the DCC in accordance with the conditions of the DCC Licence.

A3.36 Where:

(a) any provision of this Code relates to a Device or any communication to or from a Device; and

(b) the application of that provision requires that reference is made to a Version of a Technical Specification,

the Version of that Technical Specification which shall be treated as applicable for that purpose shall be the one identified as pertaining to the Device Model of that Device in the Certified Products List.

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**) or a direction under Section D9A (Authority-Led Variations).

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 Authority reasonably considers are necessary to comply with or implement the EU Regulations, any relevant legally binding decisions of the European Commission and/or the Agency for the Co-operation of Energy Regulators; and/or

(ii) ~~any relevant legally binding decisions of the European Commission and/or the Agency for the Co-operation of Energy Regulators~~are in respect of a Significant Code Review; 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, as part of the proposal's implementation, the DCC to undertake testing of the DCC Total System and/or provide testing services;

and

~~(m)~~(n) 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)~~(o) 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-initiated~~led~~

D2.4 A Modification Proposal submitted pursuant to Section D1.3(d), by either the Authority or the DCC at the direction of the Authority~~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, and/or testing as part of implementation; 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~~ Proposal pursuant to Section D4.8 shall have the effect of modifying the timetable applying to that Modification Proposal.

D5 WITHDRAWAL OF A PROPOSAL~~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.

SCR: Backstop Direction

D5.7 Where one or more Modification Proposals that are Path 1 Modifications have been raised, the Authority may issue a direction under this Section D5.7 that requires the withdrawal of those Modification Proposals and of any connected Alternative Proposals. Where the Authority so directs:

(a) the Significant Code Review Phase shall re-commence; and

(b) the Proposer for each such Modification Proposal shall be deemed to have withdrawn the Modification Proposal(s), and Sections D5.3 and D5.4 shall not apply to the withdrawn Modification Proposal(s).

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(b);

(e) consider whether the DCC should, as part of the proposal's implementation (if the Modification Proposal is approved), be required to undertake testing of the DCC Total System and/or provide testing services; and (if so) ensure that the Modification Proposal includes amendments to this Code which provide a robust testing solution (or, if it is not yet reasonably practicable to document the testing solution, which provide a process for developing the testing solution);

~~(e)~~(f) 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)~~(g) 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)~~(h) 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)~~(i) 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)~~(j) 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)~~(k) 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)~~(l) 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 either or both of the following: ~~how the following matters would be affected if that Modification Proposal were to be approved:~~

(a) whether the DCC should, as part of the proposal's implementation (if that Modification Proposal were to be approved), be required to undertake testing of the DCC Total System and/or provide testing services; and (if so) the DCC's proposals for the scope, phases, timetable and participants for such testing (or, to the extent it is not yet reasonably practicable to determine such matters, its proposals for the process pursuant to which such matters should be developed); and/or

(b) how the following matters would be affected if that Modification Proposal were to be approved:

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

(ii) 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)~~(f) 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)~~(g) 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)~~(h) 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)~~(i) 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) specify whether the implementation of the Modification Proposal is likely to 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;

(iii) specify whether, as part of the Modification Proposal's implementation, the DCC is to be required to undertake testing of the DCC Total System and/or provide testing services; and (if so) how such testing is dealt with in the Modification Proposal;

~~(ii)~~(iv) 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)~~(v) 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 as described in ~~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); and

~~(c)~~(d) decide whether to approve or reject a proposed Authority-Led Variation.

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 and Authority-Led Variations, 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).

D9A AUTHORITY-LED VARIATIONS

Power to develop a proposed variation

D9A.1 The Authority may develop a proposed variation to this Code in respect of a Significant Code Review, in accordance with the procedures set out in this Section D9A.

D9A.2 The Authority may commence a Significant Code Review Phase by issuing a direction under this Section D9A.2, or may issue a direction under this Section D9A.2 at any time during a Significant Code Review Phase. The Authority's direction under this Section D9A.2 will set out the scope and/or subject matter of the Significant Code Review.

Authority-Led Consultation

D9A.3 The Authority will, in such manner as it considers appropriate, consult on the merits of the proposed Authority-Led Variation with the Parties, Citizens Advice, Citizens Advice Scotland, and any other persons whose interests are materially affected by this Code.

Authority-Led Modification Report

D9A.4 The Authority may submit its proposed Authority-Led Variation to the Code Administrator, together with such supplemental information as the Authority considers appropriate.

D9A.5 Upon receipt of the Authority’s proposal under Section D9A.4, the Code Administrator shall prepare a written report on the proposal (the "**Authority-Led Modification Report**"). The Authority-Led Modification Report must be consistent with the information provided by the Authority under Section 9A.4, and shall:

(a) be addressed and delivered to the Panel;

(b) set out the legal text of the proposed variation to this Code;

(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 which Party Categories are likely to be affected by the proposed variation;

(f) specify whether the implementation of the proposed variation 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 proposed variation is approved, this Code would better facilitate the achievement of the SEC Objectives than if the proposed variation was rejected;

(h) specify whether it is likely that there would be a material impact on Greenhouse Gas Emissions as a result of the proposed variation 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

(i) specify whether, if the proposed variation 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.

D9A.6 Upon completion of the Authority-Led Modification Report, the Code Administrator will place such report on the agenda for the next meeting of the Panel, which shall refer the report to the Change Board.

Change Board and Change Board Decision

D9A.7 In respect of each Authority-Led Modification Report referred to the Change Board, the Change Board shall vote whether to approve the Authority-Led Variation.

D9A.8 Each vote as referred to in Section D9A.7 shall take the form of a vote in accordance with Sections D8.15 to D8.17 (The Change Board Vote). The Authority's Significant Code Review conclusions document and/or the Authority's proposal submitted in accordance with Section D9A.4 shall not fetter the procedures or voting rights referred to in Section D8 (Change Board and Change Board Decision).

D9A.9 Following the vote of the Change Board in respect of the Authority-Led Variation, the Code Administrator shall populate the Modification Register to include the outcome of the vote and the reasons given by the Change Board Members pursuant to Section D8.17 (The Change Board Vote).

D9A.10 The Code Administrator shall communicate the outcome of the Change Board vote to the Authority and the Panel, and shall send copies of the following to the Authority:

(a) the Authority-Led Modification Report; and

(b) the outcome of the Change Board vote, including the reasons given by the Change Board Members pursuant to Section D8.17 (The Change Board Vote).

Authority Decision

D9A.11 An Authority-Led Variation shall be approved only where the Authority determines that the proposed variation 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 variation, which shall be considered to constitute a recommendation by the Parties as to whether or not to approve the variation; and

(d) such other matters as the Authority considers appropriate.

Send-Back Process

D9A.12 Where the Authority considers that it is unable to form an opinion in relation to a proposed Authority-Led Variation, then it may issue a direction to the Panel specifying any additional steps that the Authority requires in order to form such an opinion. Where the Authority issues a direction to the Panel pursuant to this Section D9A.12:

(a) the decision of the Change Board in respect of the variation shall be null and void;

(b) the Panel shall seek to address the matters raised by the Authority, and shall (where necessary) have an updated Authority-Led Modification Report produced; and

(b) the Secretariat shall update the Modification Register to record the status of the proposed variation.

Implementation

D9A.13 Where an Authority-Led Variation has been approved in accordance with Section D9A.11, Section D10 (Implementation) shall apply.

D10 IMPLEMENTATION

General

D10.1 Once a Modification Proposal has been approved in accordance with Section D9 (Modification Proposal Decision) or an Authority-Led Variation has been approved in accordance with Section D9A.11 (Authority Decision), the Panel shall ensure that this Code is varied in accordance with that Modification Proposal or Authority-Led Variation, as set out in this Section D10. Authority-Led Variations are to be treated as Path 1 Modifications for the purposes of this Section D10 (and references to Modification Proposals shall be interpreted accordingly).

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 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 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 (or, in the case of Registration Data Providers nominated after this Section E2.5 comes into full force and effect, shall be provided in accordance with Section E4 (RDP Entry Process)). 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 (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 <u>DCC GATEWAY CONNECTIONS FOR REGISTRATION DATA PROVIDERS</u>

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.

E4 RDP ENTRY PROCESS

Overview

E4.1 Before Data is exchanged between the DCC and a Registration Data Provider under Section E2 (Provision of Data) for the first time, the Registration Data Provider must successfully complete the RDP Entry Process Tests.

RDP Entry Process Tests

E4.2 The "**RDP Entry Process Tests**" are, in respect of an RDP, tests to demonstrate that the DCC and the RDP are capable of exchanging Data under Section E2 (Provision of Data), as such tests are further described in the Enduring Testing Approach Document. An RDP which successfully completed Systems Integration Testing shall be deemed to have successfully completed the RDP Entry Process Tests.

E4.3 Each RDP that has not (and is not deemed to have) successfully completed the RDP Entry Process Tests shall be entitled to undertake RDP Entry Process Tests. Each RDP that has been nominated by one or more Network Parties for which the RDP was not nominated at the time that it successfully completed the RDP Entry Process Tests (or was deemed to do so) shall be entitled to undertake RDP Entry Process Tests in relation to such Network Parties. Each RDP is only obliged to successfully complete the RDP Entry Process Tests once.

E4.4 Each RDP that undertakes RDP Entry Process Tests shall:

(a) do so in accordance with Section H14 (Testing Services) and the Enduring Testing Approach Document; and

(b) be a Testing Participant for the purposes of RDP Entry Process Tests (and the provisions of Section H14 shall apply accordingly, including in respect of Testing Issues).

E4.5 The RDP will have successfully completed the RDP Entry Process Tests once the DCC considers that both it and the RDP have demonstrated that they have satisfied the applicable requirements set out in the Enduring Testing Approach Document.

E4.6 Where requested by the RDP, the DCC shall provide written confirmation to the RDP confirming whether or not the DCC considers that the RDP Entry Process Tests have been successfully completed.

E4.7 Where the DCC is not satisfied that the RDP Entry Process Tests have been successfully completed, the RDP may refer the matter to the Panel for its determination. Where the RDP disagrees with any such determination of the Panel, then the RDP may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

Liability of and to the Network Parties

E4.8 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 E4. An RDP need not enter into an Enabling Services Agreement (and Section H14.7 shall not apply to RDPs).

E4.9 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 E4.

E4.10 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 E4 will cause the Network Parties to suffer loss for which the DCC may be liable (subject to Section M2 (Limitations of Liability)).

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), in consultation with Parties and Competent Authorities (but without engaging directly with Energy Consumers), 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;

(k) (to the extent to which it reasonably considers that it is necessary to do so) to liaise and exchange information with, provide advice to, and seek the advice of the Alt HAN Forum on matters relating to the Alt HAN Arrangements that affect the End-to-End Technical Architecture and/or the Business Architecture; and

(l) to perform any other duties expressly ascribed to the Technical Architecture and Business Architecture Sub-Committee elsewhere in this Code.

F1.5 In undertaking its duties under Section F1.4(e) to (g), the Technical Architecture and Business Architecture Sub-Committee shall not review the Alt HAN Arrangements but may have regard to any impact of the provision of Alt HAN Services on the End-to-End Technical Architecture and/or the Business Architecture.

F1.6 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.

F1.7 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

F1.8 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

F1.9 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~~ specifying which ~~versions~~ Versions of each Technical Specification are compatible with which ~~versions~~ Versions of ~~each~~ the other Technical Specification, ~~(~~where:

(a) -'compatible' ~~in this context~~ means, in respect of a ~~versions~~ Version of ~~two~~ one ~~or more~~Technical Specification~~s~~, that Devices or apparatus which comply with ~~one such~~that ~~version~~ Version are designed to inter-operate with ~~other~~ Devices or apparatus that comply with ~~another such~~the specified ~~version~~ Version of the other Technical Specification~~or versions)~~; and

(b) each reference to a Version of a Technical Specification shall be read as being to that Version taken together with any relevant Version of the GB Companion Specification (as identified in the TS Applicability Tables), so that if there is more than one relevant Version of the GBCS for any Version of a Technical Specification, the matrix shall make separate provision for each of them.

~~F2.11~~F2.12 -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 Where the DCC receives an Alert from a Communications Hub Function indicating that no power supply has been available to that Communications Hub Function for a period of at least three minutes, the DCC shall send a copy of the Alert to the Import Supplier (if any) and Electricity Distributor (if any) for that Communications Hub Function.

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) 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 the same principles as are described in 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 (as completion of handover is further described in the CH Handover Support Materials);

(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 SIMCH Aerial, then the DCC shall (subject to Section F7.5) attend the premises and (where necessary) undertake such replacement or repair; and

(g) each SIMCH Aerial shall be subject to Section F7.9 as if it was Communications Hub Auxiliary Equipment, save that no Party other than the DCC may replace or repair a SIMCH Aerial.

Special Installations & Modifications

F7.5 Where the CH Installation and Maintenance Support Materials require 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 (and the DCC shall provide all information reasonably requested by the Supplier Party in relation to it obtaining such consent or agreement).

F7.6 A Supplier Party responsible under Section F7.5 for obtaining a consent or agreement in relation to works shall 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 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 F7.21 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 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).

Availability of Test CH Variants

F10.12 The DCC shall ensure that the Test Communications Hubs made available pursuant to this Section F10 represent Communications Hubs that provide for each and every combination of HAN Variant and WAN Variant; subject to Section F10.13.

F10.13 The DCC shall not be obliged to make one or more Test Communications Hub variants available pursuant to this Section F10 where it is not reasonably practicable and/or cost effective to do so.

F10.14 Where the DCC seeks to rely on Section F10.13 in respect of one or more variants, the DCC shall publish notice of that fact on the DCC Website, including within such notice the DCC's justification for why it is not reasonably practicable and/or cost effective to make that variant available pursuant to this Section F10. Where a Party disagrees with the DCC's justification in respect of one or more variants, that Party may refer the matter to the Panel to determine whether the DCC's justification is valid. Where the DCC or any other Party disagrees with the Panel's determination, the DCC or such other Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

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 any dispute between a Party and a User, a question arises as to whether that 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) where either of them disagrees with any such determination of the Panel, then 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

(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:

(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:

(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 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 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 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 to ensure that the DCC Total System prevents any such attempt at unauthorised access.

G2.7 The DCC shall take reasonable steps 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 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 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 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 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 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 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 Credential Tokens and Smart Card Tokens

G2.36 Before supplying any Cryptographic Credential Token or Smart Card 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 or Smart Card 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; and

(b) has been adequately tested for the purpose of ensuring that it fulfils its intended purpose.

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 or Smart Card 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 or Smart Card 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 or Smart Card 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.

File Signing Software

G2.39 Before supplying any File Signing Software to any person in accordance with the provisions of this Code, the DCC shall ensure that the version of that File Signing Software which is being supplied 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.

G2.40 The DCC shall, wherever it is reasonably practicable to do so, establish with the developer of the File Signing Software to be supplied by it in accordance with the provisions of this Code, arrangements designed to ensure that the DCC will be notified where that developer becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, such software.

G2.41 Where the DCC becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of, any File Signing Software which has been supplied by it in accordance with the provisions of this Code, it shall notify each person to whom it has provided that software and (wherever it is reasonably practicable to do so) the developer of the software.

G2.42 The DCC shall ensure that where it provides File Signing Software to any person, that software is provided in a format such that it can be confirmed, on receipt by the person to whom it is provided, as:

(a) having been provided by the DCC; and

(b) being authentic, such that any tampering with the software would be apparent.

Cryptographic Processing

G2.43 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).

G2.44 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

G2.45 For the purposes of Section G2.46:

(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.

G2.46 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

G2.47 The DCC shall take reasonable steps 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.

G2.48 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 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:

(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 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 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 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 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 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 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 Risk 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 Risk 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.

<u>The User Information Security Management System</u>

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, in respect of each User ID used by it in any User Role by virtue of which it is such an Eligible User, 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;

(h) (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the At HAN Forum on matters relating to the Alt HAN Arrangements 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; and

(i) provide such further support and advice to the Panel as it may request.

<u>Modifications</u>

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.

<u>Suitably Qualified Service Provider</u>

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.

<u>Independence Requirement</u>

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.

<u>The User Security Assessment Response</u>

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.

<u>Other Users</u>

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:

(i) in accordance with the Information Commissioner’s guidance concerning the same; and

(ii) where the Party is completing the User Entry Process for the User Role of Other User, having regard to any guidance issued by the Secretary of State and/or the Authority in respect of matters relating to the Processing of Personal Data that are comprised in any Data of a type referred to in Sections I1.2 to I1.4,

(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).

H3.22A A Party that is not a User but expects to submit Service Requests to the DCC at any time during any period referred to in Section H3.22 shall comply with Section H3.22 as if it were a User.

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~~ Not Used.

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 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 also be Decommissioned; 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 of any potential disruption to Services; and/or

(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, consult with Parties and/or RDPs (as applicable) and with the Technical Architecture and Business Architecture Sub-Committee regarding such risk;

(c) provide the Parties and RDPs 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, 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 prior to the implementation of such matters.

H8.11 The DCC shall make the DCC Release Management Policy available to Parties, RDPs and the Technical Architecture and Business Architecture Sub-Committee. The DCC shall consult with Parties, RDPs 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 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 each User to access the information described in Section H8.16 as being accessible to that User (and also allows other Users to access that information to the extent permitted by the first User in accordance with the Self-Service Interface Design Specification).

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

(C) cannot be confirmed as being able to connect to the SM WAN before 1 January 2021;

(ii) any known issues giving rise to poor connectivity at any given location (and any information regarding their likely resolution); and

(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;

(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

(c) where neither paragraph (a) nor (b) above apply (or to the extent the Incident is not resolved despite compliance with paragraph (a) or (b) above), 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~~ Compromise 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;

(b) ensure that all affected 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: (i) the DCC Gateway Party for that DCC Gateway Connection has not procured a backup DCC Gateway Connection; and (ii) the DCC can reasonably demonstrate that the Services could have been restored within eight hours if the DCC Gateway Party had procured a backup DCC Gateway Connection); and

(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 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); and

~~(e)~~(f) RDP Entry Process Tests.

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 Test Communications Hubs for use by Testing Participants at the DCC's physical test laboratories which represent each and every combination of HAN Variant and WAN Variant (subject to Section H14.9A); and

~~(b)~~(c) a reasonable number of Devices (other than Communications Hubs) 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).

H14.9A The DCC shall not be obliged to make one or more Test Communications Hub variants available pursuant to Section H14.9 where it is not reasonably practicable and/or cost effective to do so.

H14.9B Where the DCC seeks to rely on Section H14.9A in respect of one or more variants, the DCC shall publish notice of that fact on the DCC Website, including within such notice the DCC's justification for why it is not reasonably practicable and/or cost effective to make that variant available pursuant to Section H14.9. Where a Party disagrees with the DCC's justification in respect of one or more variants, that Party may refer the matter to the Panel to determine whether the DCC's justification is valid. Where the DCC or any other Party disagrees with the Panel's determination, the DCC or such other Party may refer the matter to the Authority for its determination (which shall be final and binding for the purposes of this Code).

H14.10 Without prejudice to Sections H14.9(b) and (c), 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.

H14.10A The DCC may require a Testing Participant to remove its Devices from a DCC test laboratory in accordance with the requirements set out in the Enduring Testing Approach Document. Any dispute between the DCC and a Testing Participant regarding the removal of such Devices (or the right to resume use of Devices in the test laboratory) may be referred to the Panel for its determination (which determination shall be final and binding for the purposes of this Code).

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 Sections H14.9(b) and (c).

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 Test 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 Test 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, take all reasonable steps to offer 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;

(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

(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 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 an approved Modification Proposal provides for the DCC to provide testing services as part of the Modification Proposal's implementation~~ 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~~ Parties which are eligible, or obliged, to participate in such testing shall be determined ~~by the Panel~~ in accordance with Section D~~10 (Implementation)~~(Modification Process), and either set out in this Code or established via a process set out in this Code.

DCC Internal System Change Testing

H14.36 Where, pursuant to Section H8.8 (DCC Internal Systems Changes), a Party or an RDP 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 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 Data Protection Act and other 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 Unambiguous Consent, which has not been withdrawn, to (as the case may be):

(i) join that Type 2 Device to the Smart Meter or Associated Device, and the User has clearly informed the Energy Consumer before obtaining such Unambiguous Consent that a consequence of joining the Type 2 Device may be that Data relating to the Energy Consumer will be shared with third parties; or

(ii) unjoin it from the Smart Meter or Associated Device, save that the Responsible Supplier for a Smart Metering System at the premises need not obtain such Unambiguous Consent where it has reasonable grounds to believe that the Type 2 Device has Compromised or is likely to Compromise any Device forming part of that Smart Metering System (and the Responsible Supplier shall, where it unjoins a Type 2 Device in such circumstances, take all reasonable steps to inform the Energy Consumer that it has done so).

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 Unambiguous 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 <u>OTHER USER PRIVACY AUDITS</u>

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.

<u>Scope of Privacy Audit Services</u>

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:

(a) shall, in discussion with the Other User to which the assessment relates, produce a written report (a "**Privacy Assessment Report**") which shall:

(i) set out the findings of the Independent Privacy Auditor on all the matters within the scope of the Privacy Assessment;

(ii) 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;

(b) 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

(a) 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.

<u>The Privacy Self-Assessment Report</u>

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 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 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;

(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.

L3.3 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.

L3.4 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.

L3.5 The DCC shall ensure that in the provision of the SMKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

L3.6 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.

L3.7 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

L3.8 Where the DCC has notified SECCo, a Party or an RDP that has applied to become an Authorised Subscriber that the DCC does not consider that 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.

L3.9 Following any reference made to it under Section L3.8, the Panel:

(a) shall determine whether the relevant applicant satisfies the criteria set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where the Panel determines that the relevant applicant meets those criteria, it shall notify the DCC, and the applicant shall (subject to any other requirements of the relevant Certificate Policy or the SMKI RAPP) become an Authorised Subscriber.

L3.10 Subject to the provisions of Section L3.11, any such determination of the Panel shall be final and binding.

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

L3.12 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.

L3.13 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 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 Authorised Subscriber does not continue to satisfy the relevant criteria, notify the Authorised Subscriber which, subject to Section L3.14, shall cease to be an Authorised Subscriber in accordance with the

Certificate Policy.

L3.14 Where the DCC has notified an Authorised Subscriber in accordance with Section L3.13(b):

(a) the provisions of Section L3.8 to L3.11 shall apply as if 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 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 person is the Subscriber as may be set out in that Certificate Policy or in the SMKI RAPP.

Eligible Subscribers

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.

<u>Device Certificates</u>

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’.

<u>DCA Certificates</u>

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 any Party or RDP is an Authorised Subscriber in accordance with the IKI Certificate Policy, it will be an Eligible Subscriber in respect of an IKI Certificate in the circumstances set out in the IKI Certificate Policy.

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)	digitalSignature	wanProvider	wanProvider

Certificate			
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 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 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).

<u>Breach of the Code by the Relevant Subscriber</u>

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 either:

(a) where appropriate, in the case of a Certificate Signing Request for the Issue of an IKI Certificate, that Certificate Signing Request has been generated using a Cryptographic Credential Token that was provided by the DCC to the Eligible Subscriber in accordance with the SMKI RAPP; or

(b) in every other case, the Public Key that is included within a 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.

L11.4 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

L11.5 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

L11.6 Where any Device Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a) 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

L11.7 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

L11.8 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

L11.9 Each Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) 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

L11.10 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 Cryptographic Protection in respect of the Organisation CRL on the SMKI Repository; 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 Cryptographic Protection in respect of the Organisation ARL on the SMKI Repository; 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 Cryptographic Protection in respect of the IKI CRL; 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 Cryptographic Protection in respect of the IKI ARL; 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, 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, or any User to submit a Personnel Authentication Certification Application, and so to become a DCCKI Subscriber, where that person 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) shall specify the technical details of the DCCKI Service Interface;

(b) shall include the protocols and technical standards that apply to the DCCKI 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; and

(d) may set out the procedure by which a DCCKI Authorised Subscriber and the DCC may communicate over the DCCKI Service Interface, and may in particular specify any requirements on:

(i) a DCCKI Authorised Subscriber which accesses, or is seeking to access, the DCCKI Service Interface;

(ii) the DCC in relation to the provision of means of access to the DCCKI Service Interface and/or any steps which must be taken by it in relation to communications made by a DCCKI Authorised Subscriber and received by it over the DCCKI Service Interface.

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) shall set out the way in which DCCKI Authorised Subscribers may access the DCCKI Service Interface;

(b) shall specify the procedure by which DCCKI Authorised Subscribers and the DCC may communicate over the DCCKI Service Interface;

(c) shall include a description of the way in which the mutual authentication and protection of communications taking place over the DCCKI Service Interface will operate; and

(d) may specify any requirements on a DCCKI Authorised Subscriber which accesses, or is seeking to access, the DCCKI Service.

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.

<u>The DCCKI Repository Service</u>

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

<u>Obligations on the SMKI PMA</u>

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.

<u>Obligations on DCCKI Participants</u>

L13.32 Each DCCKI Participant shall (in so far as they apply to it) comply with the requirements of the DCCKI SEC Documents.

<u>The DCCKI Document Set</u>

L13.33 For the purposes of this Section L13, the "**DCCKI Document Set**" means:

(a) the DCCKI SEC Documents; and

(b) the DCCKI CPS.

<u>The DCCKI SEC Documents</u>

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.

<u>The DCCKI Registration Authority Policies and Procedures: Document Development</u>

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.

<u>The DCCKI Certification Practice Statement</u>

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 and Personnel Authentication Certificate Applications

L13.43 Each DCCKI Eligible Subscriber shall ensure that all of the information contained in each DCCKI Certificate Signing Request and each Personnel Authentication Certificate Application made by it is true and accurate.

L13.44 No DCCKI Eligible Subscriber may make a DCCKI Certificate Signing Request or Personnel Authentication Certificate Application 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 or Personnel Authentication Certificate Application.

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, or any Personnel Authentication Certificate is Issued to a DCCKI Eligible Subscriber in response to a Personnel Authentication

Certificate Application, that DCCKI Eligible Subscriber shall:

(a) establish whether the information contained in that DCCKI Certificate or Personnel Authentication Certificate is consistent with information that was contained in the DCCKI Certificate Signing Request or Personnel Authentication Certificate Application (as the case may be);

(b) if it identifies that the DCCKI Certificate or Personnel Authentication Certificate contains any information which is untrue or inaccurate immediately inform the DCC that it rejects the DCCKI Certificate or Personnel Authentication Certificate and give to the DCC its reasons for doing so; and

(c) in the absence of any such rejection, become a DCCKI Subscriber for that DCCKI Certificate or Personnel Authentication 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 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 Cryptographic Protection in respect of the EII DCCKICA CRL (or, in the case of DCC only, any DCCKI Certificate Revocation List relevant to that DCCKI Certificate) on the DCCKI Repository, in accordance with IETF RFC 5280; and

(ii) where that DCCKI Certificate is shown on the EII DCCKICA CRL (or, in the case of DCC only, any DCCKI Certificate Revocation List relevant to that DCCKI Certificate) as having been revoked, not rely on the DCCKI Certificate; and

(b) before relying on any DCCKICA Certificate:

(i) Check Cryptographic Protection in respect 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 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 N: SMETS1 METERS

N1 <u>DEFINITIONS FOR THIS SECTION N</u>

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 which were included within the scope of the Initial Enrolment Project Feasibility Report or within the scope of any additional analysis pursuant to Section N4A (Further Initial Enrolment Analysis).

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~~Code Amendments 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~~Code Amendments 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~~Code Amendments 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~~otherwise). 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, N4A 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) undertake further analysis and evaluation as directed by the Secretary of State under Section N4A (Further Initial Enrolment Analysis); and

~~(b)~~(c) 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).

N4A FURTHER INITIAL ENROLMENT ANALYSIS

Further Analysis and Reporting

N4A.1 Where from time to time directed to do so by the Secretary of State, the DCC shall undertake further analysis and/or evaluation relating to Initial Enrolment, and report to the Secretary of State on such analysis and/or evaluation.

N4A.2 The DCC shall comply with the Secretary of State's directions from time to time pursuant to this Section N4A, which may include directions in relation to one or more of the following:

(a) additional Energy Meters which are to be included within the scope of Initial Enrolment (including in terms of either or both Device Models or numbers of Energy Meters);

(b) Energy Meters which are to be excluded from the scope of Initial Enrolment (including in terms of either or both Device Models or numbers of Energy Meters);

(c) the aspects of Initial Enrolment that are to be further analysed and/or evaluated;

(d) consultation with such persons as the Secretary of State may direct regarding Initial Enrolment and/or the DCC's analysis and/or evaluation;

(e) further invitations to Supplier Parties to have additional Energy Meters included within the scope of Initial Enrolment;

(f) the timing and process to be followed by the DCC in relation to the further analysis and/or evaluation, and/or any consultation or information requests relating to such analysis and/or evaluation; and

(g) redaction of published information equivalent to that outlined in Section N4.10 (Redaction for Reasons of Security).

Supplier Information

N4A.3 The DCC may request information from Supplier Parties in relation to any further analysis and/or evaluation which the DCC is required to undertake under this Section N4A, where:

(a) such information is reasonably necessary for the purpose of the analysis and/or evaluation which the DCC is required to undertake (which may include copies of Communications Contracts); or

(b) the DCC is directed by the Secretary of State to request such information.

N4A.4 Each information request pursuant to Section N4A.3 must specify a reasonable date by which Supplier Parties who wish to respond must respond, and may specify a reasonable format in which Supplier Parties who wish to respond must respond.

N4A.5 Each Supplier Party which wants its Energy Meters to remain within the scope of Initial Enrolment must provide the information requested by the DCC in accordance with Section N4A.3. No Supplier Party is obliged to provide the information requested, but each Supplier Party acknowledges that failure to provide the requested information will result in its Energy Meters being excluded from the scope of Initial Enrolment (unless the Secretary of State otherwise directs).

N4A.6 In respect of each response from a Supplier Party to a DCC request pursuant to Section N4A.3, the DCC shall notify the Supplier Party whether the DCC considers that the response has been made in accordance with the request (identifying any omissions or other deficiencies and allowing a reasonable period of time within which such omissions or other deficiencies can be rectified).

N4A.7 For the avoidance of doubt, the DCC shall only use the information obtained pursuant to this Section N4A for the purposes of the further analysis and/or evaluation required by this Section N4A.

Disputes

N4A.8 Without prejudice to Section N2.7 (SMETS1 Compliance), where the DCC issues information requests as referred to in Section N4A.3, and:

(a) a Supplier Party disputes whether that request has been made in compliance with Section N4A.3 and/or N4A.4; or

(b) a Supplier Party disagrees with the DCC's notification that the Supplier Party's response has not been made in accordance with the request or with the period it has been allowed to rectify an omission or other deficiency,

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).

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 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

(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

X1.18 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.

Developing ETAD for RDP Entry Process Tests

X1.19 The DCC shall develop a revised Enduring Testing Approach Document which provides the detailed processes concerning the RDP Entry Process Tests in accordance with Section X1.20, such that the revised document can be re-designated pursuant to Section X5 (Incorporation of Certain Documents into this Code). The revisions shall include the following in respect of the RDP Entry Process Tests:

(a) entry criteria for RDPs wishing to undertake the tests;

(b) exit criteria demonstrating successful completion of the tests; and

(c) the process for first exchanging between the RDP and the DCC a full set of the Data to be exchanged under Section E2 (Provision of Data).

X1.20 The procedure by which the DCC is to develop the revisions to the Enduring Testing Approach Document is as follows:

(a) the DCC shall produce a draft by such date as the Secretary of State may direct;

(b) in producing the draft, the DCC must consult appropriately with Parties and other interested persons;

(c) where disagreements with the Parties arise concerning the proposed content of the draft, 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 the draft revisions to the Secretary of State as soon as is reasonably practicable, and in any case by such date as the Secretary of State may direct; or

(e) when submitting a draft under paragraph (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, timeframe and/or further development of content in any direction that is given by the Secretary of State regarding the draft document.

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" , and the variation set out in this paragraph (d) shall be capable of being cancelled with effect from different dates in respect of Sections E2.1, E2.2 and E2.3 (and the obligation in Section E2.5 to provide a full set of Data on Section E2.5 coming into full force and effect shall be an obligation to provide a full set of Data under Section E2.1, E2.2 or E2.3 on the variation to Section E2.5 being cancelled in respect of that Section);

(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.[1]

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.

[1] The variation set out in this X2.4(f) ceased to apply from 6 July 2016 (see letter of 5 July 2016).

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 Part G of ~~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 Part G ~~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 Part G ~~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 Part G ~~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~~29(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~~30 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 INTERIM DEVICE AND USER SYSTEM TESTING[2]

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 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, H14.9, H14.10 and H14.11);

(d) persons undertaking GFI Testing must each comply with such reasonable supplemental obligations as the DCC may notify to them from time to time

[2] This section X9 was included from 18 April 2016 as a variation under section X6 provisions.

(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 allow each Party that is entitled to use a DCC Gateway Connection to establish and validate a connection via that DCC Gateway Connection to a test environment to be used for the purposes of Pre-UEPT Testing.

X9.4 The DCC shall, with effect from 6 May 2016, 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, 8.6, 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).

X9.5 From as soon as the DCC is reasonably able to do so, the DCC shall expand the Pre-UEPT Testing to include the ability of Parties to test their capability (and that of their Systems) to send each of the Service Requests identified in the Common Test Scenarios Document but not listed in Section X9.4(a).

X9.6 The following shall apply in respect of Pre-UEPT Testing:

(a) the references in Sections X9.4 and X9.5 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 and H14.10);

(c) persons undertaking Pre-UEPT Testing must each comply with such reasonable 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

X9.7 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.

X9.8 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.

X9.9 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.

X11 TESTING FOR SECRETARY-OF-STATE-LED VARIATIONS

Overview

X11.1 This Section X11 applies in respect of variations to this Code which the Secretary of State has the power to make under statute, Energy Licences and/or other provisions of this Code, and provides for a testing process to be followed in respect of such variations. References in this Section X11 to proposed variations includes variations which the Secretary of State is considering, is consulting on or has decided upon but not yet fully implemented.

Optional Analysis

X11.2 Where the Secretary of State so directs from time to time in respect of one or more proposed variations to this Code, the DCC shall analyse and report to the Secretary of State on the matters set out in that direction. Such matters may include, without limitation:

(a) the extent to which changes would be required to the DCC Total System were the proposed variation to be made; and/or

(b) the likely development, capital and operating costs associated with such changes, and any consequential impact on the Charges.

SEC Variation Testing Approach Document

X11.3 Each SEC Variation Testing Approach Document is to be developed by the DCC pursuant to this Section X11, and then incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).

X11.4 Where the Secretary of State so directs from time to time in respect of one or more proposed variations to this Code, the DCC shall develop a draft SEC Variation Testing Approach Document in respect of those proposed variations. The DCC shall develop that document in accordance with the timetable directed by the Secretary of State, in consultation with such other persons (if any) as the Secretary of State may direct, and otherwise in accordance with any process that the Secretary of State may direct.

X11.5 Each draft SEC Variation Testing Approach Document produced by the DCC shall set out the following in respect of the proposed variation(s), which must be consistent with any directions concerning the same made by the Secretary of State:

(a) the testing objectives;

(b) the testing to be undertaken;

(c) the testing environments to be used;

(d) the timetable for testing;

(e) the entry criteria for the start of testing or for the start of testing phases;

(f) the persons other than the DCC that are entitled or obliged to participate in testing;

(g) the entry criteria for the testing participants and the DCC;

(h) roles, responsibilities and obligations of the DCC and of the testing participants in respect of testing;

(i) the process for making amendments to the document, which shall include amendments directed by the Secretary of State;

(j) the process for resolving disputes under the document;

(k) the exit criteria for completion of testing (or stages of testing); and

(l) the process by which testing will be determined to be complete.

X11.6 The DCC shall submit each draft SEC Variation Testing Approach Document to the Secretary of State, indicating:

(a) why the DCC considers the draft to be fit for purpose;

(b) copies of the consultation responses received; and

(c) any areas of disagreement that arose during the consultation process and that have not been resolved, and, the DCC shall comply with any direction given by the Secretary of State to re-consider, re-consult and/or re-submit the draft document.

Compliance with SEC Variation Testing Approach Document

X11.7 The DCC and each person other than the DCC that participates in (or is required to participate in) testing under a SEC Variation Testing Approach Document shall comply with the SEC Variation Testing Approach Document.

X11.8 Section H14 (Testing Services) and the Enduring Testing Approach Document shall apply in respect of testing under a SEC Variation Testing Approach Document as if such testing was a Testing Service under Section H14.34 (Modification Implementation Testing); and each participant in such testing shall be deemed to be a Testing Participant for such purposes.

Version Q1.1

APPENDIX Q

IKI Certificate Policy

(IKI CP)

CONTENTS

Part Heading Page

1 INTRODUCTION

The document comprising this Appendix Q (together with its Annexes A and B):

- shall be known as the "IKI Certificate Policy" (and in this document is referred to simply as the "Policy"); and
- 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) IKI Certificates; and

(ii) IKI Certificate Authority (ICA) 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 1.2.826.0.1.8641679.1.2.1.3

1.3 SMKI PARTICIPANTS

1.3.1 The IKI Root Certification Authority

(A) The definition of IKI 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, RDPs and SECCo 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; and

(ii) Subscriber.

(G) Eligible Subscribers are defined in Annex A of this Policy

1.3.4 Subjects

(A) The Subject of an IKI Certificate shall be an entity or object which may be an individual, organisation or System and must be identified in the `subject` field of the IKI Certificate Profile in accordance with Annex B

(B) The Subject of an ICA Certificate must be the entity named in the `subject` field of the Root ICA Certificate Profile or Issuing ICA 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 (E) The only Relying Party for IKI Certificates and ICA Certificates is the DCC.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 IKI CERTIFICATES AND ICA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The ICA shall ensure that IKI Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of either authenticating the Subject to the SMKI Services or signing files related to Threshold Anomaly Detection, the Certified Products List and the SMKI Recovery Procedure that are sent to the DCC..

(B) The ICA shall ensure that ICA Certificates are Issued only to the ICA:

(i) in its capacity as, and for the purposes of, exercising the functions of, the Root ICA; and

(ii) in its capacity as, and for the purposes of, exercising the functions of, an Issuing ICA.

(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, RDP or SECCo 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 ICA or the SMKI PMA.

1.5.3 Person Determining IKI 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 IKI CPS.

1.5.4 IKI 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 IKI CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The SMKI 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

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 ICA shall ensure that the following are lodged in the SMKI Repository:

(i) all IKI Certificates Issued by the IKI File Signing CA;

(ii) each version of this Policy; and

(iii) 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 ICA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The ICA shall ensure that:

(i) each IKI Certificate Issued by the IKI File Signing CA is lodged in the SMKI Repository within 24 hours of its acceptance by a Subscriber; and

(ii) 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) The ICA shall ensure that the IKI CPS contains provisions to ensure that the entity that is the Subject of each Certificate Issued to Eligible Subscribers is in accordance with the relevant Certificate Profile at Annex B

3.1.2 Need for Names to be Meaningful

(A) The ICA shall ensure that the IKI CPS contains provisions to ensure that the name of the Subject of each IKI Certificate Issued to Eligible Subscribers is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) The ICA shall ensure that the IKI CPS contains provisions to:

(i) prohibit Eligible Subscribers from requesting the Issue of a Certificate anonymously or by means of a pseudonym; and

(ii) require the ICA to Authenticate Eligible Subscribers.

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) The ICA shall ensure that the IKI CPS contains provisions on:

(i) the procedure to be followed by Eligible Subscribers in order to prove its possession of the Private Key which is associated with the Public Key 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, RDP or SECCo in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the ICA will determine whether a Party, RDP or SECCo is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party, RDP or SECCo shall be Authenticated by the ICA for that purpose.

(B) Provision is made in the SMKI RAPP for the purpose of ensuring that the criteria in accordance with which the ICA shall Authenticate a Party, RDP or SECCo 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 ICA shall verify all information in relation to Certificates.

(B) Further provision on the content of ICA 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 ICA 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 AND LIFECYCLE 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 IKI Certificate:

(a) the circumstances in which a DCC RA Manager, DCC RA Personnel and ARO 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

(B) The ICA shall ensure that the IKI CPS contains provisions:

(i) in respect of an IKI Certificate:

(a) the circumstances in which Eligible Subscribers may submit a Certificate Signing Request; and

(b) the means by which it may do so, including through the use of an authorised System.

4.1.2 Enrolment Process and Responsibilities

(A) Provision is made in the SMKI RAPP in relation to the:

(i) establishment of an enrolment process in respect of organisations, individuals and Systems in order to Authenticate them and verify that they are authorised to act on behalf of an Eligible Subscriber in its capacity as such; and

(ii) maintenance by the ICA of a list of organisations, individuals and Systems 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 ICA Personnel and ICA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the ICA 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 ICA of DCC RA Managers, DCC RA Personnel and AROs which submit a Certificate Signing Request.

(B) The ICA shall ensure that the IKI CPS contains provisions in relation to the Authentication by the ICA 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 ICA:

(i) shall reject it and refuse to Issue the Certificate which was the subject of the Certificate Signing Request; and

(ii) shall give notice to the Party, RDP or SECCo 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 ICA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) The ICA shall ensure that it processes all Certificate Signing Requests relating to IKI Certificates promptly, and in any event in accordance with such time as is specified in the SMKI RAPP.

4.3 CERTIFICATE ISSUANCE

4.3.1 ICA Actions during Certificate Issuance

(A) The ICA may Issue a Certificate only:

(i) in accordance with the provisions of this Policy; and

(ii) in response to a Certificate Signing Request made by an Eligible Subscriber in accordance with this Policy.

(B) The ICA shall ensure that:

(i) each ICA Certificate Issued by it contains information that it has verified to be correct and complete; and

(ii) each IKI Certificate Issued by it contains information consistent with the information in the Certificate Signing Request.

(C) An ICA Certificate may only be:

(i) Issued by the ICA; and

(ii) for that purpose, signed using the Root ICA Private Key.

(D) An IKI Certificate may only be:

(i) Issued by the ICA; and

(ii) for that purpose, signed using an Issuing ICA Private Key.

(E) The ICA shall not Issue:

(i) an Issuing ICA Certificate using a Root ICA Private Key after the expiry of the Validity Period of a Root ICA Certificate containing the Public Key associated with that Private Key; or

(ii) an IKI Certificate using an Issuing ICA Private Key after the expiry of the Validity Period of an Issuing ICA Certificate containing the Public Key associated with that Private Key.

4.3.2 Notification to Eligible Subscriber by the ICA of Issuance of Certificate

(A) Provision is made in the SMKI RAPP for the ICA to notify DCC RA Manager, DCC RA Personnel and ARO where that DCC RA Manager, DCC RA Personnel or AROs is Issued with a Certificate which was the subject of a Certificate Signing Request made by them.

(B) The ICA shall ensure the IKI CPS includes provisions for the ICA to notify Eligible Subscribers where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by them.

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 the Eligible Subscriber may clearly indicate to the ICA its rejection of a Certificate which has been Issued to it; and

(ii) ensure that the Eligible Subscriber to which a Certificate has been Issued, and which has not been rejected, is treated as having accepted that Certificate.

(B) A Certificate which has been Issued by the ICA 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 ICA 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 ICA

(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 ICA to Other Entities

(A) The ICA 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 ICA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

(A) Where any ICA System or any ICA Private Key is (or is suspected by the ICA of being) Compromised, the ICA 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 ICA Private Key:

(a) ensure that the Private Key is no longer used;

(b) promptly notify each of the Subscribers for any IKI Certificates Issued using that Private Key; and

(c) promptly notify the SMKI PMA, verifiably destroy the ICA Private Key Material and revoke the corresponding ICA Certificate.

(B) Where the ICA Root Private Key is Compromised (or is suspected by the ICA of being Compromised), the ICA:

(i) may issue a replacement for any ICA Certificate that has been Issued using that Private Key; and

(ii) shall ensure that the Subscriber for that ICA Certificate both applies for the Issue of a new Certificate in accordance with this Policy and revokes that ICA Certificate.

(C) The ICA shall ensure that a replacement for each ICA Certificate is Issued prior to end of the Validity Period of that ICA Certificate.

(D) A Subscriber for an IKI Certificate may request a replacement for that Certificate at any time by applying for the Issue of a new IKI Certificate in accordance with this Policy and, where this replacement is for purposes other than to replace an expiring Certificate, shall submit a Certificate Revocation Request in respect of the replaced IKI Certificate.

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 ICA

[Not applicable in this Policy]

4.6.8 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable in 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 ICA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated, the Subscriber shall apply for a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[Not applicable to this Policy]

4.7.3 Processing Certificate Re-Keying Requests

[Not applicable to this Policy]

4.7.4 Notification of New Certificate Issuance to Subscriber

[Not applicable to this Policy]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[Not applicable to this Policy]

4.7.6 Publication of the Re-Keyed Certificate by the ICA

[Not applicable to this Policy]

4.7.7 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable to this Policy]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

(B) Neither the ICA nor any Subscriber may modify a Certificate.

4.8.2 Who may request Certificate Modification

[Not applicable to this Policy]

4.8.3 Processing Certificate Modification Requests

[Not applicable to this Policy]

4.8.4 Notification of New Certificate Issuance to Subscriber

[Not applicable to this Policy]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[Not applicable to this Policy]

4.8.6 Publication of the Modified Certificate by the ICA

[Not applicable to this Policy]

4.8.7 Notification of Certificate Issuance by the ICA to Other Entities

[Not applicable to 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) 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;

(ii) when any of the permitted reasons for revocation of authentication credentials, as set out in the SMKI RAPP, are met; or

(iii) immediately upon ceasing to be an Eligible Subscriber in respect of that Certificate.

(B) The ICA must revoke a Certificate upon:

(i) 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 ICA must revoke a Certificate in relation to which it has not received a Certificate Revocation Request:

(i) 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; or

(ii) 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 ICA 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 ICA 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 ICA to revoke a Certificate.

(C) The ICA 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 associated with Certificates Issued to DCC Registration Authority (RA) Managers, DCC RA Personnel, Authorised Responsible Officers (AROs).

(B) The ICA shall ensure that the IKI CPS contains provisions in relation to the procedure for submitting and processing a Certificate Revocation Request associated with Certificates Issued to Eligible Subscribers.

(C) On receiving a Certificate Revocation Request, the ICA shall use its reasonable steps 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.

(D) Where the ICA, 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 stepsprior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation.

(E) The ICA 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 ICA must process the Revocation Request

(A) The ICA 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 ICA shall ensure that an up to date version of the IKI ARL is made available to Relying Parties set out in 1.3.5(E) of this Policy.

(i) at least once in every period of twelve months; and

(ii) promptly on the revocation of an ICA Certificate.

(B) Each version of the IKI ARL shall be valid until the date which is 12 months after the date on which that version of the IKI ARL is produced.

(C) Further provision in relation to the reliance that may be placed on the IKI ARL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(D) The ICA shall ensure that an up to date version of the IKI CRL is made available to Relying Parties set out in 1.3.5(E) of this Policy.:

(i) at least once in every period of twelve hours; and(ii) within one hour on the revocation of an IKI Certificate.

(E) Each version of the IKI CRL shall be valid until 48 hours from the time at which it is produced. (F) Further provision in relation to the reliance that may be placed on the IKI CRL (and on versions of it) is set out in Section L12 of the Code (Relying Party Obligations).

(G) The ICA shall ensure that each up to date version of the IKI ARL and IKI 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 ICA shall ensure that the IKI 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 ICA shall retain a copy of the information contained in all versions of the IKI CRL and IKI 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 ICA 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 IKI ARL has not been made available to the DCC in accordance with Part 4.9.7(A) of this Policy,

the DCC shall be entitled to rely on the IKI 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 IKI CRL has not been made available to the DCC in accordance with Part 4.9.7(C) of this Policy

the DCC shall be entitled to rely on the IKI 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 IKI 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 ICA 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 ICA shall ensure that the ICA 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 ICA shall ensure that:

(i) all of the physical locations in which the ICA 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 ICA shall ensure that the ICA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The ICA shall ensure that the IKI 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 ICA shall ensure that the IKI CPS incorporates provisions designed to ensure that all PINs, pass-phrases and passwords used for the purposes of carrying out the functions of the ICA are stored in secure containers accessible only to appropriately authorised individuals.

(F) The ICA shall ensure that the ICA Systems are Separated from any DCA or OCA Systems, save that any Systems used for the purposes of the Registration Authority functions of the ICA and DCA or OCA shall not require to be Separated.

5.1.2 Physical Access

(A) The ICA shall ensure that the IKI 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 ICA 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 ICA shall ensure that the IKI CPS incorporates provisions in relation to power and air conditioning at all physical locations in which the ICA Systems are situated.

5.1.4 Water Exposure

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to water exposure at all physical locations in which the ICA Systems are situated.

5.1.5 Fire Prevention and Protection

(A) The ICA shall ensure that the IKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the ICA Systems are situated.

5.1.6 Media Storage

(A) The ICA shall ensure that the IKI 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 ICA.

5.1.7 Waste Disposal

(A) The ICA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the ICA 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 ICA shall regularly carry out a Back-Up of:

(i) all Data held on the ICA 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 ICA shall ensure that the IKI CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The ICA 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 IKI CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise ICA 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 ICA shall ensure that, where any elements of the ICA Systems, any Data held for the purposes of providing the SMKI Services, or any items of ICA 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 ICA shall ensure that:

(i) no individual may carry out any activity which involves access to resources, or Data held on, the ICA Systems unless that individual has been expressly authorised to have such access;

(ii) each member of ICA Personnel has a clearly defined level of access to the ICA Systems and the premises in which they are located;

(iii) no individual member of ICA Personnel is capable, by acting alone, of engaging in any action by means of which the ICA Systems may be Compromised to a material extent; and

(iv) the IKI CPS incorporates provisions designed to ensure that appropriate controls are in place for the purposes of compliance by the ICA with the requirements of this paragraph.

5.2.2 Number of Persons Required per Task

(A) The ICA shall ensure that the IKI CPS incorporates provisions designed to establish:

(i) the appropriate separation of roles between the different members of ICA Personnel; and

(ii) the application of controls to the actions of all members of ICA 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 ICA Certificate is one such function.

(B) The ICA shall ensure that the IKI CPS, as a minimum, makes provision for the purposes of paragraph (A) in relation to the following roles:

(i) ICA Systems administration;

(ii) ICA Systems operations;

(iii) ICA Systems security; and

(iv) ICA 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 ICA shall ensure that all ICA 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 ICA, not have been previously relieved of any past assignment (whether for the ICA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The ICA shall ensure that all ICA 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 ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of ICA Personnel.

5.3.5 Job Rotation Frequency and Sequence

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to the frequency and sequence of job rotations to be undertaken by members of ICA Personnel.

5.3.6 Sanctions for Unauthorised Actions

(A) The ICA shall ensure that the IKI CPS incorporates appropriate provisions relating to sanctions for unauthorised actions undertaken by members of ICA Personnel.

5.3.7 Independent Contractor Requirements

(A) In accordance with the provisions of the Code, references to the ICA in this Policy include references to persons with whom the ICA contracts in order to secure performance of its obligations as the ICA.

5.3.8 Documentation Supplied to Personnel

(A) The ICA shall ensure that all ICA 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 IKI CPS; and

(iii) any supporting documentation, statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The ICA shall ensure that:

(i) the ICA Systems record all systems activity in an audit log;

(ii) the IKI CPS incorporates a comprehensive list of all events that are to be recorded in an audit log in relation to:

(a) the activities of ICA Personnel;

(b) the use of ICA equipment;

(c) the use of (including both authorised and unauthorised access, and attempted access to) any premises at which functions of the ICA are carried out;

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the ICA 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 ICA shall ensure that:

(i) the audit logging functionality in the ICA Systems is fully enabled at all times;

(ii) all ICA 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 ICA 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 ICA shall ensure that the IKI 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 ICA shall ensure that the IKI 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 ICA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The ICA 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 ICA 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 ICA 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 ICA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The ICA 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 IKI 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 ICA shall ensure that the IKI 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 ICA shall ensure that the IKI 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 ICA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The ICA 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 ICA 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 ICA 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 ICA shall ensure that the IKI 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 ICA shall ensure that the IKI 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 ICA 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 ICA's operations.

(B) The ICA shall ensure that the IKI CPS incorporates provisions in relation to the periodic verification by the ICA of the Data held in the Archive.

5.6 KEY CHANGEOVER

5.6.1 IKI Certificate Key Changeover

(A) The ICA shall Issue a new IKI Certificate in relation to a Subject 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 ICA Key Changeover

(A) Where the ICA ceases to use an ICA Private Key in accordance with the requirements of Part 4.3.1(E) of this Policy, it shall:

(i) either:

(a) verifiably destroy the ICA Private Key Material; or

(b) retain the ICA Private Key Material in such a manner that it is adequately protected against being put back into use;

(ii) generate a new Key Pair;

(iii) ensure that any relevant Certificate subsequently Issued by it is Issued using the ICA 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

(iv) in its capacity as the Root ICA Issue a new relevant ICA Certificate.

(B) The ICA 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 ICA a Certificate Signing Request for the Issue of a replacement Certificate,

the ICA 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 ICA shall ensure that the IKI 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 ICA Systems or major failure in the ICA 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 IKI ARL and IKI CRL.

(B) The ICA 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 ICA shall ensure that the IKI 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 ICA Private Key or any part of the ICA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The ICA 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 ICA 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 ICA shall ensure that the IKI 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 ICA the Issuing ICA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The ICA shall ensure that all ICA Keys 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 ICA Key; and

(iii) using random numbers of such length as to make it computationally infeasible to regenerate them even with knowledge of when and by means of which equipment they were generated.

(B) The ICA shall not generate any Private Key or Public Key other than an ICA Key.

6.1.2 Private Key Delivery to Subscriber

(A) In accordance with Part 6.1.1(B), the ICA shall not generate any Private Key for delivery to a Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

(A) The ICA shall ensure that the IKI 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 ICA and Issuing ICA; and

(ii) ensuring that the mechanism uses a recognised standard protocol such as PKCS#10.

6.1.4 ICA Public Key Delivery to Relying Parties

(A) The ICA shall ensure that the IKI CPS incorporates provisions:

(i) in relation to the manner by which each IKI Certificate Issued by the IKI File Signing CA is made available to Relying Parties;

(ii) designed to ensure that the IKI Certificates Issued by the IKI File Signing CA are made available to Relying Parties in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The ICA 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 following size and characteristics

(i) 4096-bit RSA for the Root Certificate, or 2048-bit RSA for all subordinate Certificates including the Issuing ICA Certificate; and

(ii) SHA256-with-RSA Encryption as specified in RFC4055.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The ICA 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 Key Usage Field)

(A) The ICA shall ensure that each Certificate that is Issued by it has a 'keyUsage' field in accordance with RFC5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by it has a 'keyUsage' of 'digitalSignature'.

(C) The ICA shall ensure that each ICA Certificate that is Issued by it has a 'keyUsage' of either:

(i) 'keyCertSign'; or

(ii) 'CRLSign'.

(D) The ICA shall ensure that no 'keyUsage' values may be set in an IKI Certificate or ICA Certificate other than in accordance with this Part 6.1.7.

6.1.8 Extended Key Usage Purposes

(A) The ICA shall ensure that each Certificate that is Issued by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Device Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Web Service Subscriber CA and IKI Registration Authority CA has an 'extendedkeyUsage' field in accordance with RFC5280.

(B) The ICA shall ensure that each IKI Certificate that is Issued by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Device Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI Authorised Web Service Subscriber CA and IKI Registration Authority CA has an 'extendedKeyUsage' set to 'clientAuth'.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The ICA shall ensure that all ICA 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 ICA shall ensure that all ICA 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 ICA shall ensure that no ICA 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 ICA 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 IKI CPS; and

(ii) require to be unblocked by an authorised member of ICA Personnel who has been Authenticated as such following a process which shall be set out in the IKI 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 ICA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The ICA may Back-Up ICA 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 ICA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

(A) The ICA shall ensure that no ICA Key which is a Private Key is archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The ICA shall ensure that no ICA 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 ICA shall ensure that the Cryptographic Module in which any ICA Private Key is stored may be accessed only by an authorised member of ICA 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 ICA shall ensure that any ICA Private Key shall be capable of being de-activated by means of the ICA 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 IKI CPS.

6.2.10 Method of Destroying Private Key

(A) The ICA shall ensure that the IKI CPS incorporates provisions for the exercise of strict controls in relation to the destruction of ICA Keys.

(B) The ICA shall ensure that no ICA 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 ICA 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 ICA shall ensure that it archives ICA 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 ICA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an IKI Certificate, 10 years;

(ii) in the case of an Issuing ICA Certificate, 25 years; and

(iii) in the case of a Root ICA Certificate, 50 years.

(B) For the purposes of paragraph (A), the ICA shall set the 'notAfter' value specified in Annex B in accordance with that paragraph.

(C) The ICA shall ensure that no ICA 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 ICA shall ensure that any Cryptographic Module within which an ICA Key is held has Activation Data that are unique and unpredictable.

(B) The ICA 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 ICA Keys; and

(ii) where the Activation Data comprise any PINs, passwords or pass-phrases, the ICA shall have the ability to change these at any time.

6.4.2 Activation Data Protection

(A) The ICA shall ensure that the IKI 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 ICA shall ensure that the IKI 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 ICA;

(ii) the appropriate allocation of responsibilities to Privileged Persons;

(iii) the identification and Authentication of organisations, individuals and Systems involved in ICA activities;

(iv) the use of cryptography for communication and the protection of Data stored on the ICA Systems;

(v) the audit of security related events; and

(vi) the use of recovery mechanisms for ICA Keys.

6.5.2 Computer Security Rating

(A) The ICA shall ensure that the IKI CPS incorporates provisions relating to the appropriate security rating of the ICA Systems.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The ICA shall ensure that any software which is developed for the purpose of establishing a functionality of the ICA 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 ICA shall ensure that the IKI CPS incorporates provisions which are designed to ensure that the ICA 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 ICA

(A) The ICA shall ensure that its functions as the Root ICA are carried out on a part of the ICA Systems that is neither directly nor indirectly connected to any System which is not a part of the ICA Systems.

6.7.2 Protection Against Attack

(A) The ICA shall use its best endeavours to ensure that the ICA 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 ICA shall use its reasonable steps to ensure that the ICA 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 ICA

(A) The DCC shall ensure that, where its functions as the Issuing ICA are carried out on a part of the ICA Systems that is connected to an external network, they are carried out on a System that is Separated from all other ICA Systems.

6.7.4 Health Check of ICA Systems

(A) The ICA shall ensure that, in relation to the ICA 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 ICA shall ensure that Time-Stamping takes place in relation to all Certificates and all other ICA activities which require an accurate record of time.

(B) The ICA shall ensure that the ICA 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 ICA.

7 CERTIFICATE CRL AND OCSP CONTROLS

7.1 CERTIFICATE PROFILES

The ICA 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 ICA shall ensure that the IKI ARL and IKI CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL Entry Extensions

(A) The ICA shall notify Parties of the profile of the IKI CRL and of any IKI 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 IKI 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 IKI 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 IKI 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 IKI 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.

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 Responsible Officer (ARO) means an individual that has successfully completed the process for becoming an ARO on behalf of a Party, an RDP, a DCC Service Provider or SECCo in accordance with the SMKI RAPP.

Authorised Subscriber means a Party, RDP or SECCo which has successfully completed the procedures set out in this Policy and has been authorised by the ICA to submit a Certificate Signing Request.

Certificate means either an IKI Certificate or an ICA 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 ICA, submitted by the Subscriber for that Certificate to the ICA 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.

Cryptographic Credential Token has the meaning set out in the SMKI RAPP

Eligible Subscriber Means an Authorised Subscriber and:

a) in respect of each IKI Certificate Issued by the IKI Administrator CA or the IKI Registration Authority CA, the DCC;

b) in respect of each IKI Certificate Issued by the IKI Authorised Organisation Subscriber CA, each Eligible Subscriber in respect of Organisation Certificates;

c) in respect of each IKI Certificate Issued by the IKI Authorised Device Subscriber CA, each Eligible Subscriber in respect of Device Certificates;

d) in respect of each IKI Certificate Issued by the IKI Authorised Web Service Subscriber CA, each Eligible Subscriber for Device Certificates that is the DCC or a Supplier; or

e) in respect of each ICA Certificate, the DCC;

f) in respect of each IKI Certificate Issued by the IKI File Signing ~~Certificate~~ Certification Authority, an Authorised Subscriber that is a Party, RDP or SECCo.

File Signing Certificate means a Certificate Issued by the IKI File Signing Certification Authority.

ICA See IKI Certification Authority

ICA Certificate means either a Root ICA Certificate or an Issuing ICA Certificate.

ICA Key means any Private Key or a Public Key generated by the ICA for the purposes of complying with its obligations under the Code.

ICA Private Key means either a Root ICA Private Key or an Issuing ICA Private Key.

ICA Systems means the Systems used by the ICA in relation to the SMKI Services.

IKI Certification Authority (or ICA) means the DCC, acting in the capacity and exercising the functions of one or more of:

(a) the Root ICA;

(b) the Issuing ICA; and

(c) the Registration Authority.

IKI Administrator Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing IKI Certificates to Registration Authority Personnel, Registration Authority Managers and Authorised Responsible Officers acting on behalf of DCC Service Providers for the purposes of Authenticating such persons to SMKI Services.

IKI Authorised Device Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of issuing an ICA Certificate for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs in respect of Device Certificates over a DCC User Gateway Connection.

IKI Authorised Organisation Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting Certificate Signing Requests (CSRs) and Certificate Revocation Requests (CRRs) in respect of Organisation Certificates over a DCC User Gateway Connection.

IKI Authorised Internet Device Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs in respect of Device Certificates over the Internet.

IKI Authorised Internet Organisation Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates for the purposes of authenticating Authorised Responsible Officers to SMKI Services for the purposes of submitting CSRs and CRRs in respect of Organisation Certificates over the Internet.

IKI Authorised Web Service Subscriber Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates to Authorised Subscribers for the purposes of authenticating a Subscriber's Systems to SMKI Services for the purposes of submission of CSRs in respect of Device Certificates via the Web Service interface.

IKI Authority Revocation List (or IKI ARL) means a list, produced by the ICA, of all ICA Certificates that have been revoked in accordance with this Policy.

IKI Certificate means a certificate in the form set out in the IKI Certificate Profile in accordance with Annex B, and Issued by the Issuing ICA in accordance with this Policy.

IKI Certificate Revocation List (IKI CRL) means a certificate revocation list issued by the Issuing ICA.

IKI File Signing Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates to Authorised Responsible Officers for the purpose of signing files related to Threshold Anomaly Detection, SMKI Recovery Procedure and the Certified Products List sent to the DCC.

IKI Registration Authority Certification Authority (or CA) means the Issuing ICA when performing the function of Issuing Certificates to DCC in relation to DCC Systems for the purposes of authenticating such Systems to SMKI Services

Issue means the act of the ICA, in its capacity as the Root ICA or Issuing ICA, 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 ICA Certificate means a certificate in the form set out in the Issuing ICA Certificate Profile in accordance with Annex B, and Issued by the Root ICA to the Issuing ICAs in accordance with this Policy. The Issuing ICA may act in one of the following capacities:

a) IKI Administrator CA;

b) IKI Registration Authority CA;

c) IKI Authorised Organisation Subscriber CA;

d) IKI Authorised Device Subscriber CA;

e) IKI Authorised Internet Organisation Subscriber CA;

f) IKI Authorised Internet Device Subscriber CA;

g) IKI Authorised Web Service Subscriber CA; and

h) IKI File Signing CA

Issuing ICA Private Key means a Private Key which is stored and managed by the ICA acting in its capacity as the Issuing ICA.

Issuing ICA Public Key means the Public Key which is part of a Key Pair with an Issuing ICA Private Key.

Issuing IKI Certification Authority (or Issuing ICA) means the DCC exercising the function of Issuing IKI Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.

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.

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 ICA Private Key means a Private Key which is stored and managed by the ICA acting in its capacity as the Root ICA.

Root ICA Certificate means a certificate in the form set out in the Root ICA Certificate Profile in accordance with Annex B and self-signed by the Root ICA in accordance with this Policy.

Root IKI Certification Authority (or Root ICA) means the DCC exercising the function of Issuing ICA Certificates to the Issuing ICA and storing and managing Private Keys associated with that function.

Security Related Functionality means the functionality of the ICA Systems which is designed to detect, prevent or mitigate the adverse effect of any Compromise of that System.

Subject means: in relation to an IKI Certificate, the entity or object identified by the Distinguished Name in the ‘Subject field of the IKI Certificate Profile. The Distinguished Name of the subject of an IKI Certificate is as set out in Annex B; and in relation to an ICA Certificate, the globally unique name of the Root ICA or Issuing ICA as identified in the ‘Subject’ field of the relevant Certificate Profile in Annex B.

Subscriber means, in relation to any Certificate, a Party, RDP or SECCo 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 ICA 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 ICA 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: ICA Certificate and IKI Certificate Profiles

Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which ICA Certificates and IKI Certificates 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 RFC5280.

Common requirements applicable to Root ICA Certificates, Issuing ICA Certificates and IKI Certificates

All ICA Certificates and IKI Certificates that are validly authorised within the SMKI for use within the scope of GB Smart Metering:

- shall be compliant with IETF RFC5280.
- all ICA Certificates and IKI Certificates shall:
  - contain the `authorityKeyIdentifier` extension, except where the Certificate is the Root ICA 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 that are 4096-bit RSA for the Root ICA Certificate or 2048-bit RSA Public Keys for all subordinate certificates which shall include Issuing OCA Certificates;
- only provide for signature methods that are RSA with SHA 256
- contain a `certificatePolicies` extension containing at least one PolicyIdentifier which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Parties 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 *option [0]* `KeyIdentifier` which shall be marked as non-critical, except where the Certificate is the Root ICA Certificate. Note this exception only applies where RemotePartyRole as specified in the `X520OrganizationalUnitName` field = root;

- only contain `keyIdentifiers` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280;
- contain an `issuer` name which MUST be identical to the signer's `subject` name; and
- 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 IKI Certificates only

All IKI Certificates that are Issued by an Issuing ICA shall:

- contain a non-empty `subject` field which for:
  - IKI Certificates issued by the IKI Administrator CA, contain an `X520organisationalName` attribute whose value will be set to that of the Authorised Subscriber, an `X520OrganizationalUnitName` attribute whose value shall be set to ADMIN, a `X520commonName` attribute whose value will be set to the individual's name and an `X520emailAddress` attribute whose value will be set to the individual's email address;
  - IKI Certificates issued by the IKI Registration Authority CA, contains an organisationalName whose value will be set to that of the Authorised Subscriber, an `X520OrganizationalUnitName` attribute whose value shall be set to one of 'RA', 'MULTI_ALLOWED' or 'Super RA' and a `X520commonName` attribute whose value will be set to the individual's name;
  - IKI Certificates issued by the IKI Authorised Organisation Subscriber CA, contain an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520 commonName attribute whose value will be set to the ARO's name;
  - IKI Certificates issued by the IKI Authorised Device Subscriber CA, contain an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520commonName attribute whose value will be set to the ARO's or system name

    - IKI Certificates issued by the IKI Authorised Web Service Subscriber CA, contain an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under and a X520commonName attribute whose value will be set to the system's name.
    - IKI Certificates issued by the IKI Authorised Internet Organisation Subscriber CA, contain an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates underand a X520commonName attribute whose value will be set to the ARO's name;
    - IKI Certificates issued by the IKI Authorised Internet Device Subscriber CA, contains an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to the two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates underand a X520commonName attribute whose value will be set to the ARO's or system name.
    - IKI Certificates issued by the IKI File Signing CA, contain an X520organisationalName attribute whose value will be set to that of the Authorised Subscriber, an X520OrganizationalUnitName attribute whose value shall be set to two octet hexadecimal representation of the RemotePartyRole that this Certificate allows the subject of the certificate to request SMKI Organisation Certificates under, a second X520OrganiszationalUnitName attribute whose value should be set to the Party Signifier of the Authorised Subscriber and a X520commonName attribute whose value will be set to the ARO's name.
- contain a single Public Key;
- contain a `keyUsage` extension marked as critical, with value of:
    - `digitalSignature`;
- For Certificates Issued by by the IKI Administrator CA, IKI Authorised Device Subscriber CA, IKI Authorised Organisation Subscriber CA, IKI Authorised Internet Device Subscriber CA, IKI Authorised Internet Organisation Subscriber CA, IKI

Authorised Wed Service Subscriber CA and IKI Registration Authority CA contain a extKeyUsage extension marked critical, with a value of:

- clientAuth.

- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is Issued.

Requirements applicable ICA Certificates only

All ICA Certificates Issued by the Root ICA shall:

- be such that, per RFC5280, the IssuerName MUST be identical to the signer's SubjectName;
- have a subject name field unique within the Root ICA;
- contain a single public key;
- contain a keyUsage extension marked as critical and defined as:
  - keyCertSign; and
  - cRLSign;
- for Issuing ICA Certificates, contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is Issued;
- for the Root ICA Certificate, contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for any Policy;
- for Issuing ICA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical;
- for the Root ICA Certificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

IKI 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 RSA encryption	
`issuer`	`Name`	Globally unique name of Issuing ICA	
`Authoritykeyidentifier`	`KeyIdentifier`	A unique value that matches the `subjectKeyIdentifier` of the issuer’s credential	
`subjectKeyIdentifier`	`KeyIdentifier`	Provides a means for identifying certificates containing the particular Public Key used in an application	
`notBefore`	`Time`	Creation time of the Certificate	
`notAfter`	`Time`	Expiry time of the Certificate	
`subject`	`Name`	Name of the Subject of the Certificate	
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The subject’s Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	
`signatureAlgorithm`	`AlgorithmIdentifier`	2048 bit RSA and SHA256,	
`signatureValue`	`BIT STRING`	Subject IKI Certificate signature	

Interpretation

`version`

The version of the X.509 IKI Certificate. Valid IKI Certificates shall identify themselves as version 3.

`serialNumber`

IKI Certificate serial number, a positive integer of up to 16 octets. The `serialNumber` identifies the IKI Certificate, and shall be created by the Issuing ICA that signs the IKI Certificate. The `serialNumber` shall be unique in the scope of IKI Certificate signed by the Issuing I CA.

`signature`

The identity of the signature algorithm used to sign the IKI Certificate. The field is identical to the value of the IKI Certificate 'signatureAlgorithm' field explained further under the next '**signatureAlgorithm**' heading below.

`issuer`

The name of the signer of the IKI Certificate. This will be the gloablly unique name of the Issuing ICA.

`authorityKeyIdentifier`

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 IKI Certificates. The IKI Certificate shall contain an `authorityKeyIdentifier` in the form *option [0]* `KeyIdentifier`.

`subjectKeyIdentifier`

The Subject Key Identifier extension shall be included and marked as non-critical in the IKI Certificate. The IKI Certificate shall contain a `subjectKeyIdentifier` with KeyIdentifier generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and which shall always be 8 octets in length.

`validity`

The time period over which the Issuing ICA expects the IKI 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 IKI Certificate may be used. This shall be the time the IKI Certificate is created.

notAfter

The latest time an IKI Certificate is expected to be used. The value in a `notAfter` field shall be treated as specified in RFC 5280.

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN) with the value as defined earlier in the Requirements Sections in Annex B to this IKI Certificate Policy.

subjectPublicKeyInfo

The IKI Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280.The object identifiers for the supported algorithms and the methods for encoding the Public Key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The `rsaEncryption` OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have `ASN`.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
RSAPublicKey ::= SEQUENCE {

          modulus             INTEGER,     -- n

          publicExponent      INTEGER  }  -- e
```

where `modulus` is the modulus n, and publicExponent is the public exponent e. The DER encoded `RSAPublicKey` is the value of the BIT STRING `subjectPublicKey`.

signatureAlgorithm

The `signatureAlgorithm` field shall indicate the Issuing ICA signature algorithm used to sign this IKI Certificate is as defined under the next '**Signature Method**' heading below.

signatureValue

The Issuing ICA's signature of the IKI Certificate is computed using the Issuing ICA's private RSA 2048-bit IKI Certificate signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The IKI Certificates shall be signed by the Issuing ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

`extensions`

IKI Certificates SHOULD contain the extensions described below. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`: critical; OID as a policyIdentifier
- `keyUsage`: critical; digitalSignature.
- `extKeyUsage`: critical;clientAuth[1]
- `basicConstraints`: critical; cA=false.
- `authorityKeyIdentifier`.
- `subjectKeyIdentifier`.
- `cRLDistributionPoint`: non-critical; URI string, which shall identify the URL of the IKI CRL
- Private extensions used internally by the SMKI application with an extension OID of 2.16.840.1.113733.1.16.3, 2.16.840.1.113733.1.16.4, 2.16.840.1.113733.1.16.5 or 2.16.840.1.113733.1.16.11 where:
  - 2.16.840.1.113733.1.16.3 - Contains Cert Profile OID
  - 2.16.840.1.113733.1.16.4 - Contains Account ID
  - 2.16.840.1.113733.1.16.5 - Contains Base64 encoded URL for Symantec PKI Client web service.
  - 2.16.840.1.113733.1.6.11 - Containd Jurisdiction Hash of Symantec Master account

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57part1.

The signature algorithm shall be `SHA256-with-RSA` Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

[1] The `extKeyUsage` extension is not used in IKI Certificates Issued by the IKI File Signing CA.

The hash algorithm used by the IKI Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Root ICA 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 RSA Encryption	
`issuer`	`Name`	Globally unique name of Root ICA	
`subjectKeyIdentifier`	`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	
`subject`	`Name`	Unique name of Root ICA (same as `issuer` name)	
`subjectPublicKeyInfo`	`SubjectPublicKeyInfo`	The subject's Public Key	
`extensions`	`Extensions`	Critical and non-critical extensions	

`signatureAlgorithm`	`AlgorithmIdentifier`	4096 bit RSA and SHA256	
`signatureValue`	`BIT STRING`	Subject Certificate signature	

These certificates are the root of trust for the IKI

`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 ICA Certificate that signs the Certificate (self-signed by Root ICA). The `serialNumber` shall be unique in the scope of Certificates signed by the ICA Certificate.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Root CA Certificate's `signatureAlgorithm` field explained further under the next '**Signature Method'** heading below.

`issuer`

The name of the signer of the Certificate. This will be the gloablly unique name of the Root ICA. This will be the same as the `subject` as it is self-signed by the Root ICA.

`subjectKeyIdentifier`

The Root ICA credentials contain the `subjectKeyIdentifier` extension. Adding `subjectKeyIdentifer` facilitates certificate path building, which is necessary to validate credentials.

The Subject Key Identifier extension shall be included and marked as non-critical in the Certificate. The Certificate shall contain a `subjectKeyIdentifier` with `KeyIdentifier` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280.

validity

The time period over which the issuer expects the Certificate to be valid for. 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

This field must be populated with the globally unique name of the Root ICA.

subjectPublicKeyInfo

The Root ICA Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280, where the key size shall be 4096-bit RSA. The object identifiers for the supported algorithms and the methods for encoding the public key materials (public key and parameters) are specified in RFC3279-, -RFC4055-, and -RFC4491-

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The `rsaEncryption` OID is intended to be used in the algorithm field of a value of type `algorithmIdentifier`. The parameters field MUST have ASN.1 type NULL for this algorithm identifier.

The RSA public key MUST be encoded using the ASN.1 type RSAPublicKey:

```
        RSAPublicKey ::= SEQUENCE {
```

```
                    modulus             INTEGER,     -- n
                    publicExponent      INTEGER  }   -- e
```

where modulus is the modulus n, and `publicExponent` is the public exponent e. The DER encoded `RSAPublicKey` is the value of the BIT STRING `subjectPublicKey`.

`signatureAlgorithm`

The `signatureAlgorithm` field shall indicate the Root ICA signature algorithm used to sign this Certificate as defined in section under the next '**Signature Method**' heading below.

`signatureValue`

The Root ICA's signature of the Certificate is computed using the Root ICA's private RSA 4096-bit Certificate signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The Root ICA Certificates shall be signed by the Root ICA using the RSA algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

`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`: critical; OID as a policyIdentifier
- `keyUsage`: critical; keyCertSign, crlSign
- `basicConstraints`: critical; cA=true, pathLen absent (unlimited)
- `subjectKeyIdentifer`: non-critical; Method 2

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57part1.

The signature algorithm shall be `SHA256-with-RSA` Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Issuing ICA 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 RSA Encryption.	
`issuer`	`Name`	Unique name of Root ICA	
`subjectKeyIdentifier`	`KeyIdentifier`	A unique value that matches the `subjectKeyIdentifier` of the issuer’s credential	

authorityKeyIdentifier	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	
subject	Name	Unique name of Issuing ICA within the Root ICA	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	2048-bit RSA and SHA256	
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 ICA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root ICA.

`signature`

The identity of the signature algorithm used to sign the Certificate. The field is identical to the value of the Issuing ICA Certificate's `signatureAlgorithm` field explained further under the next '**signatureAlgorithm**' heading below.

`issuer`

The name of the signer of the Certificate. This will be the gloablly unique name of the Root ICA.

`subjectKeyIdentifier`

The Issued credentials contain the `subjectKeyIdentifier` extension. Adding `subjectKeyIdentifer` facilitates certificate path building, which is necessary to validate credentials.

The Subject Key Identifier extension shall be included and marked as non-critical in the Certificate. The Certificate shall contain a `subjectKeyIdentifier` with `KeyIdentifier` generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and which shall always be 8 octets in length.

`authorityKeyIdentifier`

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 IKI Certificates. The Certificates shall contain a `authorityKeyIdentifier` in the form *option [0]* `KeyIdentifier`.

`validity`

The time period over which the issuer expects the Certificate to be valid for. 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

This field must be populated with the globally unique name of the Issuing ICA.

subjectPublicKeyInfo (RSA)

The Issuing ICA Certificate `subjectPublicKeyInfo` field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 5280, where the key size shall be 2048-bit RSA. The object identifiers for the supported algorithms and the methods for encoding the public key materials (public key and parameters) are specified in RFC3279, RFC4055, and RFC4491.

The algorithm field shall use the following identifier:

```
rsaEncryption ::= {iso(1) member-body(2) us(840)
rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}
```

The `rsaEncryption` OID is intended to be used in the algorithm field of a value of type `AlgorithmIdentifier`. The parameters field MUST have `ASN`.1 type `NULL` for this algorithm identifier.

The RSA public key MUST be encoded using the `ASN`.1 type `RSAPublicKey`:

```
RSAPublicKey ::= SEQUENCE {

   modulus            INTEGER,     -- n

   publicExponent     INTEGER  }   -- e
```

where `modulus` is the modulus n, and `publicExponent` is the public exponent e. The DER encoded `RSAPublicKey` is the value of the BIT STRING `subjectPublicKey`.

signatureAlgorithm

The `signatureAlgorithm` field shall indicate the Root ICA signature algorithm used to sign this Certificate as defined under the next '**Signature Method**' heading below.

signatureValue

The Root ICA's signature of the Certificate is computed using the Root ICA's private RSA 4096-bit private signing key using the algorithm identified under the next '**Signature Method (RSA)**' heading below.

The Certificates shall be signed by the Root ICA using the `RSA` algorithm identified under the next '**Signature Method (RSA)**' heading below. The structure for RSA signatures is as per RFC 5280.

extensions

Issuing ICA certificates MUST contain the extensions described below and MUST have the name form as described. They SHOULD NOT contain any additional extensions:

- `certificatePolicy`: critical; OID as a policyIdentifier
- `keyUsage`: critical; keyCertSign, crlSign
- `basicConstraints`: critical; cA=true, pathLen=0
- `subjectKeyIdentifer`: non-critical; Method 2
- `authorityKeyIdentifier`: non-critical; Option [0]
- `subjectAltName`: non-critical; pointer in the form of an X500 directory name for the associated Private Key on the relevant Cryptographic Module in which the Private Key is stored.
- `cRLDistributionPoint`: non-critical; URI string

Cryptographic Primitives for Signature Method

Signature Method (RSA)

The RSA signature method is defined in NIST FIPS 186-4. When implementing RSA, the SHA-256 message digest algorithm choice is identified based on section 5 of SP 800-57 part1.

The signature algorithm shall be `SHA256-with-RSA` Encryption as specified in RFC4055. The algorithm identifier is:

```
sha256WithRSAEncryption(11) ::= {iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
sha256WithRSAEncryption(11)}
```

SHA-256 hash algorithm

The hash algorithm used by the Certificate shall be the SHA-256 secure hash algorithm as defined in NIST FIPS 180-4.

Version X 1.0

APPENDIX X

Registration Data Interface Specification

(REGIS)

DEFINITIONS

In this document, 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; and
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below.

Data Transfer Catalogue	has the meaning given to that expression in the MRA.
DCC Service Flag	means a flag used to indicate the status recorded by DCC of each MPAN or Supply Meter Point with respect to whether a Smart Metering System is Enrolled, Suspended or Withdrawn.
DCC Status File	means the file produced by DCC and transferred to each Network Party's Registration Data Provider detailing the DCC Service Flag of each MPAN or Supply Meter Point registered to that Network Party.
Electricity Registration Data Provider	means a Registration Data Provider appointed by an Electricity Network Party.
FTP	means file transfer protocol, a standard protocol for transmitting files between computers on a network.
FTPS	means FTP with Transport Layer Security.
Gas Registration Data Provider	means a Registration Data Provider appointed by a Gas Network Party.
Internet Protocol (or IP)	means the commonly used communications protocol enabling the delivery of data packets based on the IP addresses in the packet headers, used in establishing internet communications.

Issuer	has the meaning given to that term in the ~~Organisation Certificate Policy~~DCCKI Interface Design Specification.
Network Address Translation	means the standard methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) headers while they are in transit across a traffic routing device.
Policy Enforcement Point (or PEP)	a logical entity that enforces policies for admission control and policy decisions in response to a request for access. It is the logical boundary between the DCC Systems and connecting systems, namely User Systems and RDP Systems. The PEP ensures that: (a) the policies in the applicable Code of Connection relevant to the applicable party are being enforced; (b) there is appropriate separation of the DCC Systems from the connecting systems of the applicable party; and (c) all the connections to the User Systems, RDP Systems, or DCC Systems are compliant with the same applicable Code of Connection .
Registration Data File	means the file or files containing Registration Data for one or more Network Parties, produced by (or on behalf of) each Network Party and transferred to the DCC detailing the Registration Data for that Network Party pursuant to Section E2 of the Code.
Registration Data Refresh File	means the Registration Data File containing Registration Data for a subset or full set of MPANs or Supply Meter Points.
Registration Data Update File	means the Registration Data File sent periodically that records changes to Registration Data.

Response File	means a file produced whilst processing a DCC Status File. For each record in the file being processed, the Response File contains either an acknowledgement that the record has been processed successfully or in the case of a failure in processing the record, the validation errors found.
Supported Version	means the latest version of the Data Transfer Catalogue data flow that the DCC supports for use with the Registration Data Interface as listed and as updated from time to time on the Website.
Transport Layer Security (or TLS)	means a protocol that provides for the privacy and integrity of data transferred between communicating applications and their users.

1. INTRODUCTION

Document Purpose

1.1 Pursuant to Section E2.8 (Registration Data Interface) of the Code, this document is the Registration Data Interface Specification.

2. REGISTRATION DATA INTERFACE

Establishment of the REGIS logical connection

2.1 The DCC shall make the Registration Data Interface available on an Internet Protocol version 4 (IPv4) address range.

2.2 Each Registration Data Provider shall use Network Address Translation to remap their internal Internet Protocol addresses to the DCC provided Internet Protocol addresses at the Registration Data Provider’s firewall prior to accessing the Registration Data Interface.

2.3 Each Registration Data Provider shall use Network Address Translation to remap incoming DCC traffic Internet Protocol addresses from the published Internet Protocol addresses at the Registration Data Provider’s firewall to the Internet Protocol addresses the Registration Data Provider has reserved within their subnet.

2.4 The DCC shall specify a range of ports and the DCC and each Registration Data Provider shall configure these ports to be open for the FTPS connection.

File Exchange Mechanism

2.5 The Registration Data Interface shall utilise FTPS.

2.6 The DCC and each Registration Data Provider shall implement FTP, in a standard format conforming to the following internet standards as defined in the referenced Request for Comments (RFC) as published by the Internet Engineering Task Force (IETF) and the Internet Society:

(a) RFC 959 - FTP; and

(b) RFC 2228 – FTP security extensions.

2.7 The DCC and each Registration Data Provider shall secure the FTP session using TLS, in a standard format conforming to the following internet standards as defined in the referenced RFC as published by the IETF and the Internet Society:

(a) RFC 4217 - Securing FTP with TLS; and

(b) RFC 5246 - TLS version 1.2.

2.8 In accordance with RFC 4217:

(a) each Registration Data Provider shall populate the "USER command" (as defined in RFC 4217) with the RDP Signifier issued to it by the Panel, in lower case; and

(b) the DCC shall populate the "USER command" with the Party Signifier issued to it by the Panel, in lower case.

2.9 The DCC and each Registration Data Provider shall ensure the session Transport Layer Security is achieved utilising:

(a) the cipher suite TLS_RSA_WITH_AES_128_GCM_SHA256 as catalogued and further defined by the Internet Assigned Numbers Authority within the Cipher Suite Registry; and

(b) DCCKI Certificates for mutual authentication.

2.10 The DCC and each Registration Data Provider shall ensure that the FTPS session is routed via the DCC's Policy Enforcement Point and the Policy Enforcement Point used by the Registration Data Provider.

2.11 When sending a Registration Data File or DCC Status File, the DCC and each Registration Data Provider shall follow steps (a) to (d) below, and when receiving a Registration Data File or DCC Status File the DCC and each Registration Data Provider shall follow steps (e) to (l) below:

(a) structure data files provided under Sections E2.1, E2.2 and E2.4 of the Code, in accordance with the structures defined in clauses 3.17, 3.18, 3.19, 3.26, 3.28 and 3.29 of this document and shall include a unique reference number in accordance with clauses 3.11 and 3.22;

(b) Digitally Sign the file in accordance with clause 2.13 of this document;

(c) connect to the recipient's FTPS server in accordance with clauses 2.7 to 2.9 of this document using a DCC Gateway Connection;

(d) initiate the transfer of the file to the relevant delivery directory on the recipient's FTPS server utilising FTP push mechanisms for all file exchanges;

(e) authenticate the source of the file through verifying that the file has been Digitally Signed in accordance with clause 2.13 of this document, and validate the file structure against the structure as defined in clauses 3.17, 3.18, 3.19, 3.26, 3.28 and 3.29 of this document;

(f) raise an Incident in accordance with the Incident Management Policy, where the recipient is unable to authenticate the file pursuant to clause 2.17 of this document;

(g) in the case of Electricity Registration Data Providers only, raise an Incident in accordance with the Incident Management Policy, where the Electricity Registration Data Provider is unable to confirm that the file conforms with clause 3.17 of this document;

(h) in the case of Registration Data Providers only, generate a Response File as defined in clause 3.18(d) or 3.28(b) of this document, where the Registration Data Provider is unable to validate the file structure pursuant to clauses 3.19 or 3.29 of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) immediately above and on receipt of the Response File containing validation errors the DCC shall raise an Incident as defined in the Incident Management Policy;

(i) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to validate the file structure pursuant to clause 2.11(e) of this document;

(j) process each record within the file and perform record level validation, where the Registration Data Provider or DCC is able to successfully authenticate and validate the file pursuant to clause 2.11(e) of this document;

(k) in the case of Registration Data Providers only, generate a Response File as defined in clauses 3.18(d) and 3.28(b) of this document, where the Registration Data Provider is unable to successfully validate and process each record within the file pursuant to clause 2.11(j) of this document. The Registration Data Provider shall send the Response File to the DCC using the steps outlined in clauses 2.11(b) to (d) and on receipt of the Response File containing validation errors the DCC shall raise an Incident in accordance with the Incident Management Policy; and

(l) in the case of the DCC only, raise an Incident in accordance with the Incident Management Policy, where the DCC is unable to successfully validate and process each record within the file pursuant to clause 2.11(j) of this document.

Security Requirements

2.12 The DCC shall allocate to each Registration Data Provider a separate directory within its FTPS server and permit access only to write files and obtain directory listings within their assigned directory, and not to read, modify or delete files.

2.13 The DCC and each Registration Data Provider shall Digitally Sign each file sent via the Registration Data Interface with a Private Key; for the Registration Data Provider this Private Key shall be associated with an SMKI Organisation Certificate issued to the Registration Data Provider.

2.14 The DCC and each Registration Data Provider shall ensure that the Digital Signature shall:

a) use, as the digital signature technique, Elliptic Curve Digital Signature Algorithm (ECDSA) (as specified in Federal Information Processing Standards Publications (FIPS PUB) 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the hash function;

b) be applied to the entirety of the file including header and trailer; and

c) be converted to Base64 and appended within the file itself to the trailer with a preceding "," separator.

2.15 Prior to Digitally Signing each file, the DCC and each Registration Data Provider shall append to the trailer of the file the Issuer, which shall be URL encoded (as specified in the IETF RFC 2253), and serial number of the SMKI Organisation Certificate with preceding "," separators.

2.16 The DCC and each Registration Data Provider may use the organisation identifier in the header of the file and the Issuer and serial number in the trailer of the file to retrieve the appropriate public key.

2.17 The DCC and each Registration Data Provider shall Check Cryptographic Protection on a file using ECDSA (as specified in FIPS PUB 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the hash function, and Confirm Validity of the Certificate used to Check Cryptographic Protection.

2.18 The DCC and each Registration Data Provider shall ensure that the Digital Signature calculation shall:

(a) be performed on the entire file including header and trailer except the Digital Signature and preceding field separator appended to the trailer;

(b) ensure that all line termination characters read from the file, except any termination characters in the trailer, shall be normalised to 0x0A; and

(c) exclude any line termination characters in the trailer.

2.19 Prior to verifying the Digital Signature, the DCC and each Registration Data Provider shall ensure that all line termination characters in the file, except the line termination characters in the trailer, shall be normalised to 0x0A.

Interface Error Handling

Data files not being received when expected

2.20 Identification of an Anomalous Event:

(a) the DCC shall perform a check to ensure that the Registration Data Update Files being sent by the Registration Data Provider are consistent with the schedules as described in Section E2.5 (Frequency of Data Exchanges); and

(b) in the event of the DCC or a Registration Data Provider identifying an exception to the agreed schedules, either organisation may raise an Incident in accordance with the Incident Management Policy.

2.21 Connection & Transfer Failures:

(a) in the event of connection failures or file transfer failures between the Registration Data Provider and the DCC, the originating organisation shall attempt to reconnect and/or resend the file on 3 further occasions at 5 minute intervals; and

(b) if the DCC cannot establish a connection with the Registration Data Provider after such number of retries, the DCC shall raise an Incident in accordance with the Incident Management Policy; or

(c) if the Registration Data Provider fails to establish a connection with the DCC after such number of retries, the Registration Data Provider shall first confirm that the issue does not exist within their own environment and once this has been completed they may raise an Incident in accordance with the Incident Management Policy.

2.22 Authentication Failure:

(a) In the event of a transport authentication failure where the DCC is trying to send a DCC Status File to a Registration Data Provider, a transport authentication failure will result in no connection or transmission of Registration Data. In such circumstances, the DCC shall raise an Incident in accordance with the Incident Management Policy; or

(b) In the event of a transport authentication failure where a Registration Data Provider is trying to send a file to the DCC, a transport authentication failure will result in no connection or transmission of Registration Data. In such circumstances the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

Data files not conforming to the Registration Interface Specification

2.23 Identification of an Anomalous Event:

(a) The DCC or Registration Data Provider shall perform a check of the conformity of files against the agreed standards set out in clause 3 of this Registration Data Interface Specification; or

(b) In the event of either the DCC or a Registration Data Provider being in receipt of a non-conforming file the respective organisation shall raise an Incident in accordance with the Incident Management Policy.

2.24 Validation Failure:

(a) where a validation failure is identified as a result of a Registration Data Provider file that has been sent to the DCC, the DCC shall raise an Incident in accordance with the Incident Management Policy; or

(b) where a validation failure is identified as a result of a DCC file that has been sent to the Registration Data Provider, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

2.25 Other Circumstances:

(a) in the event of an Incident arising that is not covered by clauses 2.20 to 2.24 above, a Registration Data Provider shall review its business processes; and

(b) following compliance with clause 2.24 2.24(a) above, and in the event a Registration Data Provider has reasonable grounds to expect the issue to reside within the DCC, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

Notification of Delays

2.26 In the event that a Registration Data Provider has a planned or unplanned delay to a Registration Data File transfer, the Registration Data Provider shall raise an Incident in accordance with the Incident Management Policy.

2.27 In the event that the DCC has a planned or unplanned delay to a DCC Status File transfer, the DCC shall raise an Incident in accordance with the Incident Management Policy.

3. INTERFACE FILES

General Obligations

3.1 The DCC shall maintain a separate unique reference number for each Network Party that it shall apply to all files corresponding to that Network Party that it sends through the Registration Data Interface to that Network Party's Registration Data Provider.

3.2 In the event that a file is suspected of being lost, each Registration Data Provider may raise an Incident in accordance with the Incident Management Policy.

3.3 Each Electricity Registration Data Provider shall, pursuant to clause 2.11(j), reject a record with a DCC Service Flag 'effective from date' for a Smart Metering System that is earlier than the DCC Service Flag 'effective from date' previously provided by the DCC for that Smart Metering System.

3.4 Each Gas Registration Data Provider shall detect duplicate files and where detected shall not process duplicate files.

3.5 Each Gas Registration Data Provider shall process files in the order they are received.

3.6 Each Registration Data Provider and the DCC shall not use file compression on files transferred through the Registration Data Interface.

3.7 The DCC shall maintain a minimum of 24 months of the required historic Registration Data within DCC Systems.

3.8 Each Electricity Registration Data Provider shall provide any files containing Registration Data utilising the FTPS connection or via an alternative means as agreed between the DCC and the Electricity Registration Data Provider (provided that any such alternative means must incorporate the use of security controls that are at least as robust as those that apply to the FTPS connection) .

3.9 Each Gas Registration Data Provider shall provide any files containing Registration Data utilising the FTPS connection or via an alternative means as agreed between the DCC and the Gas Registration Data Provider (provided that any such alternative means must incorporate the use of security controls that are at least as robust as those that apply to the FTPS connection) .

3.10 The DCC shall provide any DCC Status Files utilising the FTPS connection or via an alternative means as agreed between the DCC and the Gas Registration Data Provider or Electricity Registration Data Provider to whom the file is being sent, (provided that any such alternative means must incorporate the use of security controls that are at least as robust as those that apply to the FTPS connection) .

Electricity Registration Data File Structure and Data Formats

3.11 Each Electricity Registration Data Provider shall maintain a unique reference number for each Electricity Network Party that it shall apply to all files corresponding to that Electricity Network Party that it sends through the Registration Data Interface.

3.12 Each Electricity Registration Data Provider shall provide Registration Data Update Files in accordance with the schedule outlined in the Registration Data Interface Code of Connection irrespective of whether there are Registration Data updates to convey. Where there are no Registration Data updates, each Electricity Registration Data Provider shall provide a Registration Data Update File containing the standard header, trailer and unique sequence number record and no further data records.

3.13 The DCC and each Electricity Registration Data Provider shall use variable length delimited file format for exchanging files, which meet the following requirements:

(a) fields shall be separated with "|" (ASCII 124) characters

(b) only use ASCII characters;

(c) not exceed the field lengths shown in the flow definitions referenced in clause 3.18 of this document;

(d) values shall not be padded (with leading zeroes or trailing spaces) where less than the maximum field length;

(e) fields shall not be enclosed in double quotes;

(f) no characters shall be entered into fields that are intended to be blank; and

(g) records shall be terminated with a line feed (ASCII 10) character.

3.14 Each Electricity Registration Data Provider:

(a) shall provide a Registration Data Refresh File containing a subset of Registration Data where the DCC so requests in accordance with Section E2.7(b) (Frequency of Registration Data Exchange) of the Code;

(b) may provide an unsolicited Registration Data Refresh File, which shall not be considered an Anomalous Event, containing a subset of Registration Data; and

(c) where both Registration Data Refresh Files under clauses 3.14(a) and 3.14(b) are to be provided on the same day, the Registration Data Provider shall provide one Registration Data Refresh File to meet these combined requirements. The time by which these files need to be sent is set out in the Registration Data Interface Code of Connection.

3.15 Each Electricity Registration Data Provider shall employ a file naming convention that ensures that each of the files it sends through the Registration Data Interface has a unique name.

3.16 For electricity Registration Data Files, the DCC shall employ a file naming convention that ensures that each file sent through the Registration Data Interface has a unique name, using the following items separated by the underscore character, giving the overall naming layout: DCCO_D0123_123456 where:

(a) 'DCCO' is the organisation identifier (as defined by the MRA);

(b) 'D0123' is the flow reference (as defined by the MRA); and

(c) '123456' is a unique reference number (unique within DCC files for each Electricity Network Party).

3.17 Each Electricity Registration Data Provider and DCC shall ensure that all files contain header and trailer records that conform to the formats as specified below:

(a) File Header

Data Item	**Format**	**Optionality**	**Comment**
Group Header	CHAR(3)	Mandatory	'ZHV'
File Identifier	CHAR(10)	Mandatory	File identifier - unique within market participant
Data flow and Version Number	CHAR(8)	Mandatory	Dxxxxnnn Consists of 5 char data flow reference followed by 3 char flow version number - where 'n' has a range of 0-9 e.g. 001, 105....
From Market Participant Role Code	CHAR(1)	Mandatory	e.g. Registration systems have value P
From Market Participant Id	CHAR(4)	Mandatory	e.g. DCC has value DCCO
To Market Participant Role Code	CHAR(1)	Mandatory	e.g. DCC has value Z
To Market Participant Id	CHAR(4)	Mandatory	e.g. DCC has value DCCO
File creation timestamp	CHAR(14)	Mandatory	DATETIME (GMT) DCC is using UTC Formatted: YYYYMMDDHHMMSS
Sending Application Id	CHAR(5)	Optional	Application identifier. For possible future use
Receiving Application Id	CHAR(5)	Optional	Application identifier. For possible future use
Broadcast	CHAR(1)	Optional	For possible future use.

Test data flag	CHAR(4)	Optional	Indicates whether or not this file contains test data. All operational (non-test) files shall contain the value OPER

(b) File Trailer

Data Item	**Format**	**Optionality**	**Comment**
Group Name	CHAR(3)	Mandatory	'ZPT'
File identifier	CHAR(10)	Mandatory	File identifier - unique within market participant
Total Group Count	INT (10)	Mandatory	Total number of groups in file excluding header/trailer
Checksum	INT (10)	Optional	Checksum
Flow count	INT (8)	Mandatory	Number of flow instances excluding file header/trailer
File completion timestamp	CHAR(14)	Optional	DATETIME (GMT) DCC is using UTC Formatted: YYYYMMDDHHMMSS

3.18 Each Electricity Registration Data Provider shall provide the following files, which shall conform to the latest Supported Version of the specified data flow structures as defined in the Data Transfer Catalogue:

(a) Initial upload and full Registration Data Refresh File

To provide the DCC with an initial population of Registration Data and any subsequent full Registration Data refresh, each Electricity Registration Data Provider shall send a Registration Data Refresh File as specified in the Data Transfer Catalogue D0353 data flow;

(b) Registration Data Update File

To notify the DCC of any changes to relevant Registration Data, each Electricity Registration Data Provider shall send a Registration Data Update File as specified in the Data Transfer Catalogue D0348 data flow.

(c) Registration Data Refresh File - Partial refresh

To provide the DCC with a partial refresh of Registration Data, each Electricity Registration Data Provider shall send a Registration Data Refresh File as specified in the Data Transfer Catalogue D0349 data flow;

(d) Response File - DCC Service Flag update rejections

To notify the DCC of any data records rejected during processing of a DCC Status File due to validation errors, each Electricity Registration Data Provider shall send a Response File as specified in the Data Transfer Catalogue D0351 data flow; and

(e) Response File - DCC Service Flag update acknowledgement

To notify the DCC of successful processing of the DCC Status File, each Electricity Registration Data Provider shall send a Response File as specified in the Data Transfer Catalogue D0172 data flow.

3.19 The DCC shall provide the following files to each Electricity Registration Data Provider conforming to the data flow structures as defined in the Data Transfer Catalogue:

(a) DCC Status File

To notify Electricity Network Parties of DCC Service Flag updates and the identity of the person that the DCC believes to be registered in relation to an MPAN as set out in Section E2.4 of the Code, the DCC shall send a DCC Status File as specified in the Data Transfer Catalogue D0350 data flow.

3.20 Clauses 3.18(a), 3.18(b) and 3.18(c) constitute the Registration Data that is to be provided by Electricity Registration Data Providers to the DCC under Section E2.1 of the Code.

3.21 Clause 3.19 constitutes the data that is to be provided by the DCC to Registration Data Providers under Section E2.4 (a) of the Code.

Gas Registration Data File Structure and Data Formats

3.22 Each Gas Registration Data Provider shall maintain a unique reference number that it shall apply to each file it sends through the Registration Data Interface. Each file (with the exception of the multiple file confirmation file as defined in clause 3.28(c) of this document) shall include this unique reference number within the file header, taken from a monotonically increasing number generator. The DCC shall check this unique reference number in order to detect duplicate, missing or out of sequence files.

3.23 The DCC and each Gas Registration Data Provider shall use comma separated file format for exchanging files, and each shall ensure that all of the files that it sends meet the following requirements:

(a) fields shall be comma-separated;

(b) only use ASCII characters;

(c) do not exceed the field lengths shown below at clause 3.28 of this document and exclude any opening and closing double quotation marks or comma separators;

(d) values shall not be padded where less than the maximum field length;

(e) text fields shall be enclosed with opening and closing double quotation marks, but no quotation marks shall be used in date and numeric fields; and

(f) blank fields shall not contain characters other than opening and closing double quotation marks for text fields.

3.24 Each Gas Registration Data Provider shall employ the file naming convention described below in clauses (a) to (e), ensuring that each file sent through the DCC Gateway Connection has a unique name. Within the names shown in clauses (a) to (e) below: ‘PN’ indicates that the files are production (will be ‘TN’ for test); nnnnnn is be the sequence number of the file in question; and xxx is the file type (ERR, FRJ or DXR) as detailed in clause 3.30:

(a) Registration Data Update File:
XOS01.PNnnnnnn.XDO

(b) Registration Data Refresh File also used for initial population:
XOS02.PNnnnnnn.XDO

(c) Daily DCC Status Files:
DCC01.PNnnnnnn.DXI

(d) Response Files from Daily DCC Status File processing will be:
XOS01.PNnnnnnn.xxx

(e) Multiple file confirmation file where Registration Data has been split into multiple Registration Data Files:
XOS02.PNnnnnnn.TOK

3.25 In the circumstance where Registration Data Files need to be split into multiple files due to size limitations; each Gas Registration Data Provider shall additionally provide a multiple file confirmation file confirming the number of files within the set as defined in clause 3.28(c) of this document and with the file naming convention defined in clause 3.24(e) of this document.

3.26 Each Gas Registration Data Provider shall ensure that all files (with the exception of the multiple file confirmation file as defined in clause 3.28(c) of this document) contain header and trailer records that conform to the formats as detailed below:

(a) File Header

Field Name	**Type**	**Length**	**Description**
Transaction Type	Text	3	Value: A00
Organisation Id	Numeric	10	An reference which uniquely identifies the sending organisation For example: DCC is 10005989
File Type	Text	3	An application specific code used to identify the structure and the usage of the file. The allowable values are: XDO Registration Data File

			ERR Response File - record level validation failure FRJ Response File - file level validation failure DXI DCC Status File DXR Response File - DCC Service Flag update response
Creation Date	Date	8	The date on which the file was generated. Format : YYYYMMDD
Creation Time	Text	8	The time (UTC) at which the file was generated (within the Creation Date) Format : HHMMSS
Generation Number	Numeric	6	A sequence number which represents an issue of a file from the Registration Data Provider or DCC (indicated by the organisation id). Each file sent either from the Registration Data Provider to DCC or from DCC to the Registration Data Provider will have a unique consecutively increasing number.

(b) File Trailer

Field Name	**Type**	**Length**	**Description**
Transaction Type	Text	3	Value: Z99
Record Count	Numeric	10	The number of detail records contained within the file. This should not include the standard header and the standard trailer but should include any file specific headers if specified for this file i.e. only A00 and Z99 records are excluded.

3.27 Each Gas Registration Data Provider shall provide Registration Data Update Files to the schedule outlined in the Registration Data Interface Code of Connection irrespective of whether there are Registration Data updates to convey. Where there are no updates to provide the Registration Data Update File will contain the standard header, file sequence number and trailer and no data records.

3.28 Each Gas Registration Data Provider shall provide files to the DCC conforming to the following data flow structures:

(a) Registration Data Update Files

Registration Data updates shall be contained within a single file type (Ref XDO) and shall consist of up to 3 different types of data record per update as detailed below.

Where Registration Data needs to be split into multiple Registration Data Update Files due to size limitations, the data for a specific MPRN shall not be split between files.

(i) Data notifications (Ref E47, including data items for the Supply Meter Point such as address, postcode & UPRN)

Field Name	**Optionality**	**Type**	**Length**	**Description**	**Code reference**
Transaction Type	Mandatory	Text	3	Value: E47	Not applicable
Meter Point Reference (MPRN)	Mandatory	Number	10	A unique identifier for the point at which a meter is, has been or will be connected to the gas network.	Section E2.2 (c)
MPRN Status	Mandatory	Text	2	The current status of the operability of the meter.	Section E2.2 (d)
Source Registration Id	Mandatory	Text	3	Unique ID to identify the GT or iGT which has sent the data.	Not applicable

Field Name	**Optionality**	**Type**	**Length**	**Description**	**Code reference**
Meter Point Address	Optional	Text	250	Standard PAF format address for the Supply Meter Point. This field will be a concatenated form of the elements of the Supply Meter Point address available. The address will be separated within the text delimiters (double quotation marks) by commas. The address will be represented in a consistent manner in the following order: Plot Number, Building Number, Sub Building Name, Building Name, Principal Street, Dependent Locality Post Town. If no address field data has been provided, the field will be blank denoted as ",,,,,,"	Section E2.2 (g)
Meter Point Postcode	Optional	Text	9	Standard PAF post code as defined in the PAF digest. The postcode will comprise the concatenated outcode and incode, separated by a space.	Section E2.2 (g)
Market Sector Flag	Optional	Text	1	A code that specifies that the site is used for Domestic or Industrial purposes. The allowable values are: D – Domestic or I – Industrial.	Section E2.2 (h)
Unique Property Reference Number	Optional	Text	12	A unique property reference number. It is a unique reference number that can be linked to further address information that is collated and provided by the Ordnance Survey Group.	Section E2.2 (g)

(ii) Organisation Notifications (Ref. E48, including details of the various organisations associated with the MPRN such as Gas Supplier, Meter Asset Manager and Gas Transporter).

Field Name	**Optionality**	**Type**	**Length**	**Description**	**SEC reference**
Transaction Type	Mandatory	Text	3	Value: E48	Not applicable
Organisation Type	Mandatory	Text	3	A three character short code denoting the role performed by the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record. The allowable values are: SUP – Gas Supplier; MAM – Meter Asset Manager; NWO – Network Operator (Gas Transporter).	Section E2.2 (f)
Organisation Identifier	Mandatory	Text	3	A three character short code which is assigned by the Gas Transporter to denote the identity of the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record.	Section E2.2 (f)
Organisation Effective From Date	Mandatory	Date	8	The date from which the Organisation was effective from or appointed to the Supply Meter Point denoted in the parent record. Format : YYYYMMDD	Section E2.2 (f)
Organisation Effective To Date	Optional	Date	8	Organisation's Effective To Date. Format : YYYYMMDD N.B. Where the date is '00010101', this will be treated as Null This will not be provided for Meter Asset Manager and Network Operator.	Section E2.2 (f)

(iii) Organisation Deletions (Ref. E49, including details of the various organisations previously associated with the MPRN which are now to be deleted). This record type is used to delete future dated organisations which will no longer come into effect due to other data changes. For example where a new Meter Asset Manager is due to be associated with an MPRN, but a change of supplier occurs before the effective date and the supplier assigns their own Meter Asset Manager.

Field Name	**Optionality**	**Type**	**Length**	**Description**	**SEC reference**
Transaction Type	Mandatory	Text	3	Value: E49	Not applicable
Organisation Type	Mandatory	Text	3	A three character short code denoting the role performed by the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record. The allowable values are: SUP – Gas Supplier; MAM – Meter Asset Manager; NWO – Network Operator (Gas Transporter).	Section E2.2 (f)
Organisation Identifier	Mandatory	Text	3	A three character short code which is assigned by the Gas Transporter to denote the identity of the Organisation being notified as being effective at the Supply Meter Point denoted in the parent record.	Section E2.2 (f)
Organisation Effective From Date	Mandatory	Date	8	The date from which the Organisation was effective from or appointed to the Supply Meter Point denoted in the parent record. Format : YYYYMMDD	Section E2.2 (f)
Organisation Effective To Date	Optional	Date	8	Organisation's Effective To Date. Format : YYYYMMDD NB Where the date is '00010101', this will be treated as Null	

(b) Response File - DCC Service Flag update responses

Following the processing of the DCC Status File (file format described in clause 3.29(a) of this document) each Gas Registration Data Provider shall provide a Response File indicating whether each of the DCC Service Flag update records (record reference 'E45') was accepted or rejected. For each E45 record in the incoming "DXI" DCC Status File there will be a corresponding E46 record (as described immediately below) in the "DXR" Response File. If the E45 record is processed successfully, the outcome code in the E46 record will be "AC" and if unsuccessful the outcome code is "RJ".

Where the outcome is "RJ" the rejection reason will be notified to the DCC through an S72 record or records directly following the E46.

(i) The format of an E46 record is as follows:

Field Name	**Optionality**	**Type**	**Length**	**Description**
Transaction Type	Mandatory	Text	3	Value: E46
Outcome Code	Mandatory	Text	2	Details whether the request has been accepted or rejected. AC – Accepted RJ – Rejected.
Meter Point Reference	Mandatory	Number	10	
DCC Service Flag	Mandatory	Text	1	Service flag provided by the DCC. The allowable values are: A Active S Suspended W Withdrawn
DCC Service Effective From Date	Mandatory	Date	8	The date the DCC Service Flag (provided above) is effective from. Format : YYYYMMDD

(ii) The format of an S72 record is as follows:

Field Name	**Optionality**	**Type**	**Length**	**Description**
Transaction Type	Mandatory	Text	3	Value: S72
Rejection	Mandatory	Text	8	The unique reference number identifying

Code				the reason for the validation failure. One of the following two values: 'MPO00001' Supply Meter Point does not exist 'DCC00001' DCC Service Flag value is not recognised

(c) Multiple file confirmation file

Where Registration Data needs to be split into multiple files due to size limitations, each Gas Registration Data Provider shall provide an additional file confirming the number of files within the set.

Field Name	**Optionality**	**Type**	**Length**	**Description**
File Name	Mandatory	Text	18	
Record Count	Mandatory	Number	10	The number of detail records contained within the file. This should not include the standard header and the standard trailer but should include any file specific headers if specified for this file i.e. only A00 and Z99 records are excluded.

3.29 The DCC shall provide files to each Gas Registration Data Provider conforming to the following data flow structure:

(a) DCC Status File

To notify each Gas Registration Data Provider of DCC Service Flag updates the DCC shall send a single DCC Status File (Ref DXI) that shall consist of a single data record per update (Ref. E45). The format of an E45 record is as follows:

Field Name	Optionality	Type	Length	Description	SEC reference
Transaction Type	Mandatory	Text	3	Value: E45	Not applicable
Meter Point Reference	Mandatory	Number	10		Section E2.4 (b)
DCC Service Flag	Mandatory	Text	1	Service flag provided by the DCC. The allowable values are: A – Active S – Suspended W – Withdrawn	Section E2.4 (b)
DCC Service Effective From Date	Mandatory	Date	8	The date the DCC Service Flag (provided above) is effective from. Format : YYYYMMDD	Section E2.4 (b)

3.30 Each Gas Registration Data Provider shall create and send the Response Files as defined in clause 3.30 (a) and (b) below, in response to failures in validation of the DCC Status File. On receipt of the Response File DCC shall raise an Incident as defined in the Data Incident Management Policy.

(a) Record level format failure Response File

To record any record level format validation errors found in processing the DCC Status File, the Gas Registration Data Provider shall create a Response File with header and trailer as defined in clause 3.26 of this document and one or more record level error records as detailed below. The file name will be as defined in clause 3.24(d) of this document with suffix ‘ERR’.

Field Name	**Optionality**	**Type**	**Length**	**Description**
Transaction Type	Mandatory	Text	3	Value: E01
Rejection Code	Mandatory	Text	8	The unique reference number identifying the reason for the validation failure as defined in the Error Code under clause 3.30(c)
File Reference	Mandatory	Number	10	The unique reference number of the file that was received and processed.
Rejection Description	Mandatory	Text	250	Description of the error found and which record/field it occurred as defined in the Rejection Reason under clause 3.30(c).

(b) Response File - File level rejection

To record any file level format validation errors found in processing the DCC Status File, the Registration Data Provider shall create a Response File with header and trailer as defined in clause 3.26 of this document and the file name will be as defined in clause 3.24(d) of this document with suffix ‘FRJ’. File level validation failures will be contained within a single file and will consist of 2 different types of data record per file – Rejected File (record reference S71) and Rejection Details (record reference S72). There will be one S71 record followed by one or more S72 records.

(i) The format of an S71 record is as follows:

Field Name	**Optionality**	**Type**	**Length**	**Description**
Transaction Type	Mandatory	Text	3	Value: S71
File Reference	Mandatory	Text	30	The unique reference number of the file that was received and processed.

(ii) The format of an S72 record is as follows:

Field Name	**Optionality**	**Type**	**Length**	**Description**
Transaction Type	Mandatory	Text	3	Value: S72
Rejection Code	Mandatory	Text	8	The unique reference number identifying the reason for the validation failure as defined in the Error Code under clause 3.30(d)

(c) Record level - Error codes

Error Code	
CSV00010	Transaction type not recognized - <*Record identifier*>
CSV00011	Invalid character - <*Record identifier*>, <*Field number*>
CSV00012	Invalid numeric field , <*Record identifier*>, <*Field number*>
CSV00013	Premature end of record - <*Record identifier*>
CSV00014	Invalid record termination - <*Record identifier*>
CSV00015	Invalid text field - <*Record identifier*>, <*Field number*>
CSV00019	Record too short - <*Record identifier*>
CSV00020	Mandatory field expected - <*Record identifier*>, <*Field number*>
CSV00021	Invalid Date/Time field - <*Record identifier*>, <*Field number*>
CHK00036	Mandatory record not supplied - <*Record identifier*>

(d) File level - Error codes

Error Code	
FIL00013	Organisation ID on header cannot be found
FIL00014	Organisation ID on the header does not match the sender's ID
FIL00015	File type on the header is not the same as that in file name
FIL00016	Generation number on the header is not the same as that in file name
FIL00017	A file has previously been received & processed with this generation number
FIL00018	A count of detail records in the file does not match that held on the trailer
FIL00019	Invalid record type found