ENERGY

SMART METERS

MODIFICATIONS TO THE SMART ENERGY CODE AND THE SMART METER COMMUNICATION LICENCES (SMART METERS No 2 of 2014)

The Secretary of State makes the following licence and code modifications in exercise of the powers conferred by section 88(1) of the Energy Act 2008 (“the Act”).

The Secretary of State has consulted the holders of any licence being modified, the Gas and Electricity Markets Authority and such other persons as the Secretary of State considered appropriate in accordance with section 89(1) of the Act.

A draft of these licence modifications has been laid before Parliament in accordance with section 89(3) of the Act. Neither House of Parliament resolved, within the 40-day period referred to in section 89(4) of the Act, that the Secretary of State should not make the licence modifications.

Interpretation

1 In these modifications–

(a) "smart meter communication licences" means–

(i) the licence granted to Smart DCC Limited on 20th September 2013 under section 7AB(2) of the Gas Act 1986; and

(ii) the licence granted to Smart DCC Limited on 20 September 2013 under section 6(1A) of the Electricity Act 1989; and

(b) "Smart Energy Code" means the document of that title required to be maintained and in force in accordance with condition 21 of the smart meter communication licences.

Modifications to smart meter communication licences

2 The conditions of the smart meter communication licences are modified, in accordance with paragraphs 3 to 6 below, with effect from the day after the day on which this instrument is made.

3 In condition 36, in paragraph 36.8, after "where RPIt means the" insert "percentage".

4 In condition 36, in paragraph 36.15, after "For the purposes of the Principal Formula, the correction factor (K)" delete "is" and insert "shall in the Regulatory Year 2013/2014 have the value of 0, and in each subsequent Regulatory Year shall be".

5 In Appendix 1 of condition 36, replace the existing table in Appendix 1 with the following table–

“

2013/14 **1.769**	2014/15 **3.194**	2015/16 **2.724**	2016/17 **2.041**	2017/18 **2.008**	2018/19 **2.059**	2019/20 **2.443**
2020/21 **1.959**	2021/22 **1.869**	2022/23 **1.875**	2023/24 **2.035**	2024/25 **1.840**	2025/26 **0.762**	2026/27 **n/a**

”.

6 In Part F of Schedule 3–

(a) renumber the second paragraph that is numbered 3.4 (the first of which appears in Part E of Schedule 3) as paragraph 3.5;

(b) renumber existing paragraphs 3.5 to 3.9 as paragraphs 3.6 to 3.10 respectively;

(c) in the renumbered new paragraph 3.5 delete "paragraph 3.5 or paragraph 3.8" and insert "paragraph 3.6 and 3.9";

(d) in the renumbered new paragraph 3.6 delete "paragraph 3.4" and insert "paragraph 3.5";

(e) in the renumbered new paragraph 3.7 delete "paragraph 3.5" and insert "paragraph 3.6";

(f) in the renumbered new paragraph 3.9 delete "paragraph 3.4" and insert "paragraph 3.5";

(g) in the renumbered new paragraph 3.10 delete "paragraphs 3.5 and 3.6" and insert "paragraphs 3.6 and 3.7"; and

(h) in the renumbered new paragraph 3.10 delete "paragraph 3.8" and insert "paragraph 3.9".

Modifications to the Smart Energy Code

7 The Smart Energy Code is modified, in accordance with paragraphs 8 to 15 below, with effect from the day after the day on which this instrument is made.

8 In Section A1.1–

(a) insert, in alphabetical order in the existing definitions set out in section A1.1, the definitions set out in Part A of Schedule 1 of this instrument; and

(b) replace, the existing definitions in section A1.1 of the terms set out in Part B of Schedule 1 of this instrument with the definitions set out in Part B of Schedule 1.

9 In Section A2–

(a) after existing Section A2.1(l) insert new Section A2.1(m) as follows–

"(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);";

(b) re-number existing Sections A2.1(m) and A2.1(n) as Sections A2.1(n) and A2.1(o) respectively;

(c) after existing Section A2.5 insert new Sections A2.6 and A2.7 as follows –

"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.".

10 After Section E insert new Section F comprising Sections F1 to F4 as set out in Schedule 2 of this instrument.

11 After Section H13 insert new Section H14 as set out in Schedule 3 of this instrument.

12 After Section K insert new Section L comprising Sections L1 to L10 as set out in Schedule 4 of this instrument.

13 After Section S insert new Section T comprising Sections T1 to T7 as set out in Schedule 5 of this instrument.

14 In Section X replace the existing Section X3 with the following:

"**X3** **<u>PROVISIONS TO BECOME EFFECTIVE FOLLOWING DESIGNATION</u>**

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:

(i) set out or otherwise described in this Section X3; or

(ii) 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) Section F1 (Technical Sub-Committee) shall have effect from the date on which this Code is first modified to include that Section;

(b) 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 commencement of SMKI and Repository Testing;

(C) in respect of Device and User System Testing, from the commencement of End-to-End Testing; and

(D) in respect of all other Testing Services, from the end of End-to-End Testing;

(c) 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;

(d) Section T (Testing During Transition) shall have effect from the date on which this Code is first modified to include that Section; and

(e) 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.

Provisions to be Effective Subject to Variations

X3.3 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).

X3.4 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.

X3.5 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:

(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).

General

X3.6 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).".

15 After Schedule 6 of the Smart Energy Code insert the following appendices–

(a) Appendix A – SMKI Device Certificate policy, as set out in Schedule 6 of this instrument;

(b) Appendix B – SMKI Organisation Certificate Policy, as set out in Schedule 7 of this instrument; and

(c) Appendix C – SMKI Compliance Policy, as set out in Schedule 8 of this instrument.

Sandy Verma

Verma
Parliamentary Under Secretary of State
Department of Energy and Climate Change

Date 30|07|14

SCHEDULE 1

NEW AND REPLACEMENT DEFINITIONS FOR SECTION A1.1 OF THE SMART ENERGY CODE

Part A: New definitions to be inserted in alphabetical order in Section A1.1 of the Smart Energy Code

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 Subscriber means a Party which is an Authorised Subscriber for the purposes (and in accordance with the meaning given to that expression in Annex A) of either or both of the Certificate Policies.

Authority Revocation List (or ARL) has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Auxiliary Load Control means, in respect of a premises, a device installed for the purposes of the Supply of Energy to that premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of,

[Section 5, Part D of the Smart Metering Equipment Technical Specification] that is applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

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.

Batched Certificate Signing Request has the meaning given to that expression in Section L8.2 (SMKI Services: Target Response Times).

Certificate means a Device Certificate, DCA Certificate, Organisation Certificate or OCA Certificate.

Certificate Policy means either the Device Certificate Policy or the Organisation Certificate Policy.

Certificate Revocation List (or CRL) has the meaning given to that expression in Annex A of the Organisation Certificate Policy.

Certificate Signing Request means a request for a Certificate submitted by an Eligible Subscriber in accordance with the 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.

Code Performance Measures means the performance measures set out in Section H13.1 (Code Performance Measures) or L8 (SMKI Performance Standards and Demand Management).

Communications Hub Function means, in respect of a premises, a device installed for the purposes of the Supply of Energy to that premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of,

the Communications Hub Technical Specification (excluding those provisions that apply only to ‘Gas Proxies’) that is applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

Communications Hub Technical Specification means the document of that name set out in Schedule [TBC].

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; and

(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 “Compromise” and “Compromising” are to be interpreted accordingly).

Contingency Key Pair has the meaning given to that expression in Section L10.6(c) (Recovery Procedure: Definitions).

Contingency Private Key has the meaning given to that expression in Section L10.6(c)(i) (Recovery Procedure: Definitions).

Contingency Public Key has the meaning given to that expression in Section L10.6(c)(ii) (Recovery Procedure: Definitions).

CPA Assurance Maintenance Plan means the document of that name issued by CESG with each CPA Certificate.

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

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.

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

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 Total System means the DCC Systems together with any and all Communications Hubs provided by the DCC as part of the Communications Hub Service.

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 Model means, in respect of a Device, the Device's manufacturer, model, hardware version and firmware version, including, where applicable, the Meter Variant (as defined in the SMETS).

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:

(a) in respect of a Service Request to be sent by a User, a digital signature generated by the User in accordance with the DCC User Gateway Interface Specification;

(b) in respect of a Pre-Command to be sent by a User, a digital signature generated by the User in accordance with the GB Companion Specification;

(c) in respect of Service Responses and Alerts to be signed by the DCC and sent to an Unknown Remote Party, a digital signature generated by the DCC in accordance with the GB Companion Specification (and sent to Users as documented in the DCC User Gateway Interface Specification);

(d) in respect of Pre-Commands to be sent by the DCC to a User, a digital signature generated by the DCC in accordance with the DCC User Gateway Interface Specification;

(e) in respect of a Service Response or Alert to be sent by a Device, any digital signature generated by the Device in accordance with the GB Companion

Specification; and

(f) in respect of a Certificate, a digital signature generated by the relevant Certification Authority in accordance with the relevant Certificate Policy and included within that Certificate.

Digitally Signed means, in respect of a communication, that such communication has had the necessary Digital Signatures applied to it (and "**Digitally Sign**" and "**Digitally Signing**" are to be interpreted accordingly).

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).

Electricity Smart Meter means, in respect of a premises, a device installed for the purposes of the Supply of Energy to the premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of,

[Section 5, Parts A, B or C] of the Smart Metering Equipment Technical Specification that is applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

Eligible Subscriber has the meaning given to that expression in Section L3.6 (Eligible Subscribers).

End-to-End Technical Architecture means the DCC Systems and the Smart Metering Systems together, including as documented in the Technical

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).

EUI-64 Compliant means a 64-bit globally unique identifier governed by the Institute of Electrical and Electronics Engineers.

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.

Gas Proxy Function means, in respect of a premises, a device installed for the purposes of the Supply of Energy to the premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of,

those sections of the Communications Hub Technical Specification that apply to 'Gas Proxies' and that are applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

Gas Smart Meter means, in respect of a premises, a device installed for the purposes of the Supply of Energy to the premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of, [Section 4] of the Smart Metering Equipment Technical Specification that is applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

GB Companion Specification means the document of that name set out in Schedule [TBC].

IHD means, in respect of a premises, a device installed for the purposes of the Supply of Energy to the premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of,

[Section 6 of the Smart Metering Equipment Technical Specification] that is applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

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).

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).

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.

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.

Lead Supplier means, in respect of any Device or Devices forming, or intended to form, part of one or more Smart Metering Systems:

(a) where one of those Smart Metering Systems relates to an MPAN, the Import Supplier (whether or not one of those Smart Metering Systems also relates to an MPRN); or

(b) where one of those Smart Metering Systems relates to a MPRN but none relate to an MPAN, the Gas Supplier.

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 Release Notes means, in respect of any hardware version or firmware version in a Device Model, the Manufacturer’s notes regarding:

(a) for new Device Models: the description of the features provided by that model; and

(b) for Device Models that differ from previous Device Models only by virtue of having new versions of hardware and/or firmware: the reasons for the new version(s), a description of any enhancements to the features provided by the new version(s), a description of any fixes to existing features, and a statement on backwards and forwards compatibility of any new firmware version.

Notification means, in respect of a Modification Proposal, notification of that modification to the EU Commission pursuant to EU Directive 98/34/EC.

OCA Certificate 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 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).

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:

(a) set out in Section H13.1 (Code Performance

Measure);

(b) published in accordance with Section H13.2 (Service Provider Performance Measure); or

(c) set out in Section L8 (SMKI Performance Standards and Demand Management).

Pre-Payment Interface means, in respect of a premises, a device installed for the purposes of the Supply of Energy to the premises that, on the date on which it is installed, as a minimum:

(a) consists of the apparatus identified in;

(b) has the functional capability specified by; and

(c) complies with the other requirements of,

[Section [TBC] of the Smart Metering Equipment Technical Specification] that is applicable at that date and was published on or after [SMETS2 date] (or, in the context of a device that has not yet been installed, means a device that is intended to meet the foregoing requirements once it has been installed).

Private Key means the private part of an asymmetric Key Pair used for the purposes of public key encryption techniques

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 wholly or partly for 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.

Recovery Certificate has the meaning given to that expression in Section L10.3(b)(ii) (Recovery Procedure: Definitions).

Recovery Key Pair has the meaning given to that expression in Section L10.6(b) (Recovery Procedure: Definitions).

Recovery Private Key has the meaning given to that expression in Section L10.6(b)(i) (Recovery Procedure: Definitions).

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

Registration Authority Policies and Procedures (or **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).

Relevant Private Key has the meaning given to that expression in Section L10.6(a) (Recovery Procedure: Definitions).

Relying Party means a person who, pursuant to the Code, receives and relies upon a Certificate.

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

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 for the purposes of complying with its obligations under, or in relation to, this Code, but excluding:

(a) any Digital Signature; and

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

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.

Separate means, in relation to any System or software, to establish controls which are appropriately designed to ensure that no communication may take place between it and any other System or software (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 or software (and "**Separated**", and "**Separation**" are to be interpreted accordingly).

Service Level means, in respect of each Performance Measure:

(a) the number of occasions during the Performance Measurement Period on which the DCC performed the activity that is the subject of the Performance Measure in accordance with the Service Level Requirements,

expressed as a percentage of:

(b) the number of occasions during the Performance Measurement Period on which the DCC performed the activity that is the subject of the Performance Measure; provided that 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 or the Target Resolution Time (as applicable in accordance with the table in Section H13 (Performance Standards and Reporting) or L8 (SMKI Performance Standards and Demand Management)); 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.

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.

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.

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

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 [TBC], which is originally to be developed pursuant to Section T6 (Development of Test Scenario Documents).

SMKI and Repository Testing means the testing described in Section T5 (SMKI and Repository Testing).

SMKI Code of Connection means the SEC Subsidiary Document of that name set out in Appendix [TBC], which:

(a) has the purpose described in Section L4.5 (SMKI Code of Connection); and

(b) is originally to be developed pursuant to Sections L4.6 to L4.7 (SMKI Interface Document Development).

SMKI Compliance Policy means the SEC Subsidiary Document of that name set out in Appendix C.

SMKI Document Set has the meaning given to that expression in Section L9.3 (the SMKI Document Set).

SMKI Independent Assurance Scheme has the meaning given to that expression in Part 2.1 of the SMKI Compliance Policy (DCC: Duty to Submit to an SMKI Independent Assurance Scheme).

SMKI Interface Design Specification means the SEC Subsidiary Document of that name set out in Appendix [TBC], which:

(a) has the purpose described in Section L4.4 (SMKI Interface Design Specification); and

(b) is originally to be developed pursuant to Sections L4.6 to L4.7 (SMKI Interface Document Development).

SMKI Participants means the DCC (acting in its capacity as the provider of the SMKI Services), all Authorised Subscribers and all Relying Parties.

SMKI PMA means the Sub-Committee of that name established pursuant to Section L1 (SMKI Policy Management Authority).

SMKI PMA (Network) Member has the meaning given to that expression in Section L1.8 (Membership of the SMKI PMA).

SMKI PMA (Supplier) Members has the meaning given to that expression in Section L1.6 (Membership of the SMKI PMA).

SMKI PMA Chair has the meaning given to that expression in Section L1.5 (Membership of the SMKI PMA).

SMKI PMA Member has the meaning given to that expression in Section L1.3 (Membership of the SMKI PMA).

SMKI Recovery Procedure means the SEC Subsidiary Document of that name set out in Appendix [TBC], which:

(a) has the purpose described in Section L10.1 (The SMKI Recovery Procedure); and

(b) is originally to be developed pursuant to Sections L10.4 to L10.5 (Recovery Procedure: Document Development).

SMKI Repository has the meaning given to that expression in Section L5.1 (the SMKI Repository).

SMKI Repository Code of Connection means the SEC Subsidiary Document of that name set out in Appendix [TBC], which:

(a) has the purpose described in Section L6.5 (SMKI Repository Code of Connection); and

(b) is originally to be developed pursuant to Sections L6.6 to L6.7 (SMKI Repository Interface Document Development).

SMKI Repository Interface has the meaning given to that expression in Section L6.3 (the SMKI Repository Interface).

SMKI Repository Interface means the SEC Subsidiary Document of that name set out in

Design Specification Appendix [TBC], which:

(a) has the purpose described in Section L6.4 (SMKI Repository Interface Design Specification); and

(b) is originally to be developed pursuant to Sections L6.6 to L6.7 (SMKI Repository Interface Document Development).

SMKI Repository Service has the meaning given to that expression in Section L5.2 (the SMKI Repository Service).

SMKI SEC Documents has the meaning given to that expression in Section L9.4 (the SMKI SEC Documents).

SMKI Service Interface has the meaning given to that expression in Section L4.3 (the SMKI Service Interface).

SMKI Services has the meaning given to that expression in Section L3.1 (the SMKI Services).

SMKI Specialist means an individual (rather than a body corporate, association or partnership) to be appointed and remunerated under a contract with SECCo, who:

(a) has experience and expertise in public key infrastructure arrangements;

(b) is sufficiently independent of any particular Party or class of Parties and of the Independent SMKI Assurance Service Provider; and

(c) is chosen by the SMKI PMA Chair from time to time.

Solution Architecture Information means a description of the overall technical architecture of the DCC Systems (or any part thereof) in more detail than the Technical Architecture Document so as to describe the individual components of the DCC Systems (including hardware and software) and how they interface with the User Systems.

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).

Symmetric Key means any key derived from a Shared Secret in accordance with the GB Companion Specification

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

Target Response Time has the meaning given to that expression in Section H3.20 (Target Response Times) or L8 (SMKI Performance Standards and Demand Management).

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

(a) set out in Section H13.1 (Code Performance Measure);

(b) published in accordance with Section H13.2 (Service Provider Performance Measure); or

(c) set out in Section L8 (SMKI Performance Standards and Demand Management).

Technical Architecture Document means a document setting out a representation of the End-to-End Technical Architecture.

Technical Specifications means the SMETS, the CHTS, the DCC User Gateway Code of Connection, the DCC User Gateway Interface Specification, the Self-Service Interface Design Specification, the Self-Service Code of Connection, the Electricity Registration Data Interface Documents, the Gas Registration Data Interface Documents, the Error Handling Strategy, the User Mapping Catalogue, the Incident Management Policy, the Registration Data 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 Sub-Committee means the Sub-Committee established pursuant to Section F1 (Technical Sub-Committee).

Test Certificate means a certificate that simulates the function of a Certificate for the purpose of testing pursuant to this Code.

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).

Type 1 Device means a Device that is capable of operating as a 'Type 1 Device' (as defined in the SMETS).

Type 2 Device means a Device that is not capable of operating as a 'Type 1 Device' (as defined in the SMETS).

User Entry Process Tests means the tests described in Section H14.13 (User Entry Process Tests).

Volume Scenarios means the capacity levels to which the DCC Systems will be tested.

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).

Part B: Definitions replacing existing definitions in Section A1.1 of the Smart Energy Code

Communications Hub means a Communications Hub Function together with a Gas Proxy Function.

DCC Systems means the Systems used by the DCC and/or the DCC Service Providers in relation to the Services and/or this Code, including the SM WAN but excluding the Communications Hubs.

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 Interface; (f) an Auxiliary Load Control; and (g) any Type 2 Device.

Other Enabling Services means the Services described in Section H (DCC Services) or L (Smart Metering Key Infrastructure), but excluding the Enrolment Services, the Communications Hub Services and the Communication Services.

Services means the services provided, or to be provided, by the DCC pursuant to Section H (DCC Services) or Section L (Smart Metering Key Infrastructure), including pursuant to Bilateral Agreements.

Smart Metering System means either:

(a) an Electricity Smart Meter together with the Communications Hub Function with which it is Associated; or

(b) a Gas Smart Meter together with the Communications Hub Function with which it is Associated and an Associated Gas Proxy Function,

together (in each case) with the Type 1 Devices that may from time to time be Associated with that Smart Meter.

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 and Data associated therewith.

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 Gateway;

(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 Gateway; and

(e) generating or receiving Data communicated by means of the Self-Service Interface.

SCHEDULE 2

NEW SECTION F TO BE INSERTED INTO THE SMART ENERGY CODE

“SECTION F: SMART METERING SYSTEM REQUIREMENTS

F1 TECHNICAL SUB-COMMITTEE

Establishment of the Technical 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 Sub-Committee”.

F1.2 Save as expressly set out in this Section F1, the Technical Sub-Committee shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

F1.3 Membership of the Technical Sub-Committee shall be determined by the Panel:

(a) having regard to the need to provide an appropriate level of technical expertise in the matters that are the subject of the Technical Sub-Committee’s duties; and

(b) otherwise in accordance with Section C6.7 (Membership).

Duties of the Technical Sub-Committee

F1.4 The Technical Sub-Committee shall undertake the following duties on behalf of the Panel:

(a) 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 Technical Specifications (or variations to other parts of this Code that affect the End-to-End Technical Architecture);

(b) to provide the Panel, the Change Board and Working Groups with 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;

(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 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 Specifications;

(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 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 Sub-Committee considers appropriate);

(f) to support the Panel in the technical aspects of the annual report which the Panel is required to prepare and publish under Section C2.3(h) (Panel Duties);

(g) to develop and thereafter maintain the Technical Architecture Document, and arrange for its publication on the Website;

(h) to provide the Panel with support and advice in respect of any other matter concerned with the End-to-End Technical Architecture which is not expressly referred to in this Section F1.4; and

(i) perform any other duties expressly ascribed to the Technical Sub-Committee elsewhere in this Code.

F1.5 The Technical Sub-Committee shall establish a process whereby the Code Administrator monitors Modification Proposals with a view to identifying (and bringing to the Technical Sub-Committee's attention) those proposals that are likely to affect the End-to-End Technical Architecture. The Code Administrator shall comply with such process.

DCC Obligations

F1.6 The DCC shall provide all reasonable assistance and information to the Technical Sub-Committee in relation to the performance of its duties as it may reasonably request, including by providing the Technical Sub-Committee with any requested Solution Architecture Information.

F2 CERTIFIED PRODUCTS LIST

Certified Products List

F2.1 The Panel shall establish and maintain a list of Device Models for which it has received Assurance Certificates (the "Certified Products List").

F2.2 The Panel shall ensure that the Certified Products List identifies each Device Model by Device Type, and lists the following matters in respect of each Device Model:

(a) Manufacturer and model;

(b) hardware version (together with accompanying Manufacturer Release Notes);

(c) firmware version (together with accompanying Manufacturer Release Notes);

(d) a Firmware Hash of the firmware image provided pursuant to Section F2.8 or F2.10 (as applicable);

(e) the version (or effective date) of the SMETS or the CHTS for which the Device Model has one or more Assurance Certificates;

(f) the identification numbers for each of the Device Model's Assurance Certificates; and

(g) the expiry date of the Device Model's CPA Certificate.

Background to Assurance Certificates

F2.3 The SMETS or the CHTS (as applicable to the relevant Device Type) sets out which 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 Device Types (each being, as further described in the SMETS or the CHTS, 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").

Expiry of CPA Certificates

F2.5 Each CPA Certificate will expire 6 years after its issue. Accordingly, the following Parties shall ensure that a replacement CPA Certificate is issued in respect of Device Models for the following Devices before the expiry of such CPA Certificate (to the extent Device Models of the relevant Device Type require CPA Certificates in accordance with the SMETS or the CHTS):

(a) the DCC for Communications Hub Functions and Gas Proxy Functions; and

(b) the Import Supplier and/or Gas Supplier (as applicable) for Devices of all other Device Types.

F2.6 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.

Addition of Device Models to the List

F2.7 The Panel shall only add Device Models to the Certified Products List once the Panel has received all the Assurance Certificates required (under the SMETS or the CHTS) to be obtained in respect of Device Models of the relevant Device Type. Assurance Certificates may be provided to the Panel by a Party or any other person.

F2.8 The Panel shall only add a Device Model to the Certified Products List once the Panel has been provided with the Manufacturer Release Notes for the relevant firmware version and hardware version, and once (in respect of the Device Model's firmware version):

(a) the person seeking to add the Device Model associated with the firmware version to the Certified Products List has notified the Panel of the relevant Manufacturer's identity;

(b) the Panel has received a Firmware Hash of the firmware image for the firmware version that is digitally signed so as to reasonably enable the Panel to check that the Firmware Hash originates from the Manufacturer; and

(c) the Panel has successfully confirmed that the digital signature referred to in (b) above is that of the Manufacturer identified under (a) above (validated as necessary by reference to a trusted party).

Adding Device Models to CPA Certificates

F2.9 An existing CPA Certificate for a Device Model may allow one or more additional Device Models to be added under that existing CPA Certificate, provided that any additional Device Model differs from the Device Model for which the CPA Certificate was originally issued only by virtue of having new versions of hardware and/or firmware and subject to the terms of the CPA Assurance Maintenance Plan. Where this is the case:

(a) the DCC for Communications Hub Functions and Gas Proxy Functions; or

(b) a Supplier Party for Device Models of all other Device Types,

may notify the Panel of one or more additional Device Models to be added to the CPA Certificate.

F2.10 Where the DCC or a Supplier Party notifies the Panel of an additional Device Model pursuant to Section F2.9, the DCC or the Supplier Party shall:

(a) only do so in accordance with the terms of the relevant CPA Assurance Maintenance Plan;

(b) retain evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, such evidence to be provided to the Panel or the Authority on request; and

(c) ensure that the requirements of Section F2.8 have been met.

F2.11 The Panel shall not be required to check whether the DCC or a Supplier Party (as applicable) is entitled to add a Device Model under the terms of the CPA Certificate and the CPA Assurance Maintenance Plan.

Removal of Device Models from the List

F2.12 Where an Assurance Certificate for a Device Model is withdrawn or cancelled by the Assurance Certification Body or (in the case of CPA Certificates) expires, then the Panel shall remove that Device Model from the Certified Products List.

F2.13 The DCC and each Supplier Party shall notify the Panel of any withdrawal, expiry or cancellation of Assurance Certificates of which the DCC or Supplier Party becomes aware. The Panel shall only remove Device Models from the Certified Products List having confirmed with the relevant Assurance Certification Body that the Assurance Certificate for that Device Model has expired or has been withdrawn or cancelled.

Publication and Use by the DCC

F2.14 Within one Working Day after being required to add or remove Device Models to or from the Certified Products List in accordance with this Section F2, the Panel shall:

(a) provide a copy of the updated Certified Products List to the DCC that is digitally signed so as to reasonably enable the DCC to check that the updated Certified Product List originates from the Panel;

(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.

F2.15 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:

(a) the DCC shall first confirm that the digital signature referred to in Section F2.14(a) is that of the Panel (validated as necessary by reference to a trusted party); and

(b) 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 revised Certified Products List.

Deployed Products List

F2.16 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).

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 SMETS or the CHTS does not meet the applicable requirements of the SMETS or the CHTS, then that Party may refer the matter to the Panel for its determination.

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 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 SMETS 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 the SMETS or the CHTS do not meet the applicable requirements of the SMETS or the CHTS, 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 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).

F3.7 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).”

SCHEDULE 3

NEW SECTION H14 TO BE INSERTED INTO THE SMART ENERGY CODE

"SECTION H14: TESTING SERVICES

H14 TESTING SERVICES

General Testing Requirements

H14.1 The DCC shall provide the following testing services (the "**Testing Services**"):

(a) User Entry Process Tests;

(b) SMKI and Repository Entry Process Tests;

(c) Device and User System Tests;

(d) Modification Proposal implementation testing (as described in Section H14.34); and

(e) DCC Internal Systems change testing (as described in Section H14.36).

H14.2 The DCC shall make the Testing Services available, and shall provide the Testing Services:

(a) in accordance with 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. 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 Party 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) the DCC is to provide Testing Services to a person that is not a Party, the DCC shall only do so where that person has agreed to be bound by reasonable terms and conditions relating to the same, including terms and conditions equivalent to Sections H14.5, H14.33, J1 (Payment of Charges) and M2 (Limitations of Liability).

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 Service, including providing:

(a) for access to the Testing Services either at physical test laboratories and/or remotely; and

(b) a reasonable number of Devices for use by Testing Participants at the DCC's physical test laboratories which Devices are to be of the same Device Models as those selected pursuant to the Device Selection Methodology and/or such other Device Models as the

Panel approves from time to time (provided that, where Test Stubs (or other alternative arrangements) were used then such Tests Stubs (or other alternative arrangements) will be used in place of Devices until the DCC agrees with the Panel which Device Models to use).

H14.10 Without prejudice to Section H14.9(b), the DCC shall allow Testing Participants to use Devices they have procured themselves when using the Testing Services. The DCC shall make storage facilities available at the DCC's physical test laboratories for the temporary storage by Testing Participants of such Devices (for no more than 30 days before and no more than 30 days after completion of the Testing Service for which such Devices may be expected to be used). The DCC shall ensure that such storage facilities are secure and only capable of access by persons authorised by the relevant Testing Participant.

General: SMKI Test Certificates and Test Repository

H14.11 The following shall apply with respect to the Testing Services and the tests required pursuant to Section T (Testing During Transition):

(a) the DCC shall use and make available to Testing Participants such Test Certificates as are reasonably necessary for the purposes of such tests or any other tests that a Party undertakes for either the purpose of satisfying itself that its Devices are SMETS compliant or for the purpose of undertaking activities associated with its participation under this Code;

(b) the DCC shall establish and make available to Testing Participants a Test Repository for the purposes of such tests;

(c) the DCC shall keep the Test Repository separate from the SMKI Repository;

(d) the DCC and each Testing Participant shall only use Test Certificates for the purposes of such tests (and no Party shall use actual Certificates when providing or undertaking such tests); and

(e) no person shall use Test Certificates otherwise than for the purposes of such tests.

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 Gateway via the Party's chosen DCC User Gateway Means of Connection;

(b) can use the DCC User Gateway for the purposes set out in Section H3.2 (Communications to be sent via DCC User Gateway) 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 Tests Scenarios Document; and

(c) be undertaken using Devices selected and provided by the DCC as referred to in Section H14.9(b).

H14.15 Only Parties who the DCC considers meet any entry requirements (for a particular User Role) set out in the Common Tests 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 Tests 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.

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 Tests Scenarios Document for that User Role.

H14.20 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).

H14.21 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 Parties seeking to complete the entry process described in Section L7 (SMKI and Repository Entry Process Tests) are 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 Tests Scenarios Document.

H14.24 A Party 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 Parties who 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 Party meets such entry requirements, 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).

H14.26 Each Party 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 Party 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 Party will have the right to determine the sequencing of the tests that comprise the SMKI and Repository Entry Process Tests.

H14.28 A Party 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 Party has demonstrated that it has satisfied the requirements set out in the SMKI and Repository Tests Scenarios Document for those purposes.

H14.29 Where requested by a Party, the DCC shall provide written confirmation to the Party and the Panel confirming whether or not the DCC considers that the Party has successfully completed the SMKI and Repository Entry Process Tests (for the purposes described in Section H14.22(a) and/or (b), as applicable).

H14.30 Where the DCC is not satisfied that a Party 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 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).

Device and User System Tests

H14.31 The DCC shall provide a service to enable Testing Participants:

(a) to test the interoperability of Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs provided as part of the Testing Services, such that those Devices are able to respond to Commands received from or via the DCC in accordance with the requirements defined in the GB Companion Specification;

(b) to test the interoperability of User Systems with the DCC Systems, including via the DCC User Gateway and the Self-Service Interface; and

(c) to test simultaneously the interoperability of User Systems and Devices (other than those comprising Communications Hubs) with the DCC Systems and with the Communications Hubs provided as part of the Testing Services,

which Testing Services in respect of (a) and (c) above shall include the provision of a connection to the SM WAN for the purpose of such tests (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).

H14.32 Each Party is eligible to undertake Device and User System Tests. Any Manufacturer (whether or not a Party) is eligible to undertake the Device and User System Tests described in Section H14.31(a).

H14.33 The DCC shall, on request by a Testing Participant, offer reasonable additional support to that Testing Participant in understanding the DCC Total System and the results of such Testing Participant's Device and User System Tests (subject to such Testing Participant agreeing to pay any applicable Charges). Such additional Testing Services are without prejudice to the DCC's obligations in respect of Testing Issues.

Modification Implementation Testing

H14.34 Where the Panel determines, in accordance with Section D10 (Implementation), that testing is required in relation to the implementation of a Modification Proposal, then such testing shall be undertaken as a Testing Service pursuant to this Section H14.34 and the implementation timetable approved in accordance with Section D10 (Implementation).

H14.35 The persons eligible to participate in such testing shall be determined by the Panel in accordance with Section D10 (Implementation).

DCC Internal System Change Testing

H14.36 Where, pursuant to Section H8.8 (DCC Internal Systems Changes), a User is involved in testing of changes to the DCC Internal Systems, then such testing shall not be subject to the requirements of Section H14.3, Section H14.4 and Sections H14.6 to H14.11 (inclusive), but such a User may nevertheless raise a Testing Issue in respect of the tests.

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)."

SCHEDULE 4

NEW SECTION L TO BE INSERTED INTO THE SMART ENERGY CODE

“SECTION L – SMART METERING 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 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 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 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 and Organisation 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) to, as soon as reasonably practicable following the incorporation of the following documents into this Code, review those documents in accordance with paragraph (c) above:

(i) the SMKI Compliance Policy;

(ii) the RAPP;

(iii) the Device Certificate Policy;

(iv) the Organisation Certificate Policy; and

(v) the 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) 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;

(f) to exercise the functions allocated to it under the Recovery Procedure, and in particular to exercise the power to nominate Parties for such purposes (and in accordance with such procedures) as are set out in the Recovery Procedure;

(g) 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;

(h) to provide assurance in accordance with Section L2 (SMKI Assurance);

(i) 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;

(j) to provide the Panel and Sub-Committees with general advice and support with respect to the SMKI Services and SMKI Repository Service;

(k) 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

(l) 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

L.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).

L2.16 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.

L2.17 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 either:

(a) the Device Certification Authority; or

(b) the Organisation Certification Authority,

in each case in accordance with the applicable requirements of the Code.

Authorised Subscribers

L3.2 Any Party which has successfully completed the SMKI and Repository Entry Process Tests may apply to become an Authorised Subscriber in accordance with, and by following the relevant procedures set out in, the relevant Certificate Policy and the RAPP.

L3.3 The DCC shall authorise any Party to submit a Certificate Signing Request, and so to become an Authorised Subscriber, where that Party has successfully completed the relevant procedures set out in the relevant Certificate Policy and the 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 must ensure that in the provision of the SMKI Services it acts in accordance with Good Industry Practice.

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, 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) specifies the technical details of the SMKI Service Interface;

(b) includes the protocols and technical standards that apply to the SMKI Service Interface; and

(c) bases those technical standards on PKIX/IETF/PKCS open standards, where:

(i) PKIX is the Public Key Infrastructure for X.509 Certificates, being an IETF set of standards for certificate and certificate revocation list profiles as specified in RFC 5280;

(ii) the IETF is the Internet Engineering Task Force; and

(iii) PKCS is the Public Key Cryptography Standard.

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) specifies the procedure by which an Authorised Subscriber and the DCC may communicate over the SMKI Service Interface; and

(c) 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; 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.

L5 <u>THE SMKI REPOSITORY SERVICE</u>

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 the following:

(a) all Device Certificates;

(b) all DCA Certificates;

(c) all Organisation Certificates;

(d) all OCA Certificates;

(e) all versions of the Device Certificate Policy;

(f) all versions of the Organisation Certificate Policy;

(g) all versions of the RAPP;

(h) all versions of the Recovery Procedure;

(i) all versions of the SMKI Compliance Policy;

(j) all versions of the CRL;

(k) all versions of the ARL;

(l) such other documents or information as may be specified by the SMKI PMA from time to time; and

(m) 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 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; and

(c) 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 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 to:

(a) the Parties;

(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 Panel and the SMKI PMA may access the SMKI Repository Interface;

(b) specifies the procedure by which the Parties, the Panel and the SMKI PMA may communicate over the SMKI Repository Interface; and

(c) includes a description of the way in which the mutual 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; and

(ii) a summary of any disagreements that arose during consultation and that have not been resolved by reaching an agreed proposal;

(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 shall not be entitled to:

(a) apply to become an Authorised Subscriber for the purposes of the Device Certificate Policy or the Organisation Certificate Policy (or both); or

(b) access the SMKI Repository,

until that Party 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 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 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 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 a Party's application pursuant to Section L7.4, the DCC shall process the Party'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 wishing to:

(a) become an Authorised Subscriber for the purposes of the Device Certificate Policy or the Organisation Certificate Policy (or both) 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 will have successfully completed the SMKI and Repository Entry Process Tests for a particular purpose once that Party has received confirmation from the DCC that it has met the relevant requirements of Section L7.6.

L7.8 Once a Party has successfully completed the SMKI and Repository Entry Process Tests for a particular purpose, the DCC shall confirm the same to the Panel.

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, 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
6	Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.	monthly	99%	96%
7	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 By the 15th Working Day of the months of December, March, June and September, each Party which is an Authorised Subscriber in accordance with the Device Certificate Policy shall 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 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 use its reasonable endeavours to achieve the Target Response Times).

L9 THE SMKI DOCUMENT SET

Obligations on the SMKI PMA

L9.1 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the SMKI Document Set.

Obligations on SMKI Participants

L9.2 Each SMKI Participant shall (in so far as they apply to it) comply with the requirements of the SMKI SEC Documents.

The SMKI Document Set

L9.3 For the purposes of this Section L, the "**SMKI Document Set**" means:

(a) the SMKI SEC Documents;

(b) the Device CPS; and

(c) the Organisation 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 SMKI Compliance Policy;

(iv) the RAPP;

(v) the Recovery Procedure;

(vi) the SMKI Interface Design Specification;

(vii) the SMKI Code of Connection;

(viii) the SMKI Repository Interface Design Specification;

(ix) the SMKI Repository Code of Connection;

(x) the SMKI and Repository Test Scenarios Document;

(b) the provisions of this Section L; 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 RAPP:

(a) to make provision for such matters as are specified in the Certificate Policies as being matters provided for in the 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) in accordance with the process set out at Section L9.6; and

(d) 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 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 RAPP;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the RAPP, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the RAPP specified in Section L9.5;

(c) the DCC shall send a draft of the 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;

(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 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 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 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.

Enquiries in relation to the SMKI Document Set

L9.19 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party 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 Compromised:

(a) the mechanism by which Users may notify the DCC and the DCC may notify Users that the Relevant Private Key has been Compromised;

(b) procedures relating to:

(i) the establishment and re-generation of a Recovery Key Pair and Issue of an associated Recovery Certificate;

(ii) the establishment and re-generation of a Contingency Key Pair;

(iii) the establishment and re-generation of a Symmetric Key to encrypt and decrypt the Contingency Public Key;

(iv) the storage of the Recovery Private Key and Contingency Private Key;

(v) the use of the Recovery Private Key and Contingency Private Key (including the use of the Symmetric Key); and

(vi) the distribution of new Root OCA Certificates and Organisation Certificates to Devices;

(c) steps to be taken by the DCC, the Parties (or any of them, whether individually or by Party Category) and the SMKI PMA, including in particular in respect of:

(i) notification of the Compromise; and

(ii) the process for recovering from the Compromise (which may differ depending on the Relevant Private Key that has been Compromised, and the nature and extent of the Compromise and any adverse effect arising from it); and

(d) arrangements for periodic testing of the operation of the matters described in paragraphs (a) to (c) and the associated technical solutions employed by the DCC.

Recovery Procedure: Obligations

L10.2 The DCC, each Party and the SMKI PMA shall comply (in so far as they apply to it) with any requirements set out in the SMKI Recovery Procedure.

L10.3 The DCC shall reimburse the reasonable costs of any Party associated with supporting the maintenance and use of the procedures and arrangements set out in the SMKI Recovery Procedure.

Recovery Procedure: Document Development

L10.4 The DCC shall develop a draft of the SMKI Recovery Procedure:

(a) in accordance with the process set out at Section L10.5; 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.

L10.5 The process set out in this Section L10.5 for the development of a draft of the SMKI Recovery Procedure is that:

(a) the DCC shall, in consultation with Users, 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.

Recovery Procedure: Definitions

L10.6 For the purposes of this Section L10:

(a) a "**Relevant Private Key**" means a Private Key which is associated with a Public Key contained in:

(i) any Organisation Certificate or OCA Certificate that is held on 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;

(b) 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

(c) 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)."

SCHEDULE 5

NEW SECTION T TO BE INSERTED INTO THE SMART ENERGY CODE

“SECTION T – TESTING DURING TRANSITION

T1 DEVICE SELECTION METHODOLOGY

Overview

T1.1 The Device Selection Methodology is the methodology for determining the Devices that are to be used by the DCC for the purposes of Systems Integration Testing, Interface Testing and User Entry Process Tests.

Use of Devices

T1.2 Systems Integration Testing, Interface Testing and User Entry Process Tests are to be undertaken using (to the extent reasonably practicable) actual Devices (rather than Test Stubs or other alternative arrangements).

Device Selection Methodology

T1.3 The DCC shall develop, publish (including on the DCC Website) and comply with a methodology (the “Device Selection Methodology”) concerning the selection and de-selection of Devices for the purposes of Systems Integration Testing, Interface Testing and User Entry Process Tests. The DCC shall consult with the other Parties and Manufacturers prior to finalising the Device Selection Methodology. The Device Selection Methodology shall include provision for the DCC to:

(a) (save for Communications Hubs) select as many different Device Models as the DCC considers appropriate in order to demonstrate that the Testing Objectives have been achieved; provided that, when the DCC first selects Device Models, the DCC shall select at least the first two Gas Meter Device Models and at least the first two Electricity Meter Device Models offered in accordance with the Device Selection Methodology that meet the criteria set out in Sections T1.4 and T1.6 (as varied by Section T1.5);

(b) (save for Communications Hubs) select the Device Models in accordance with the selection criteria described in Sections T1.4 and T1.6 (as varied by Section T1.5);

(c) (save for Communications Hubs) publish an invitation to submit Device Models for selection (such publication to be in a manner likely to bring it to the attention of Parties and Manufacturers, including publication on the DCC Website), such invitation to require Devices to be offered for use on reasonable terms specified by the DCC and from a certain date;

(d) de-select a Device Model (for the purposes of the then current phase of testing and any future phases of testing pursuant to this Section T) if that Device Model is subsequently found to not comply with the criteria set out in Section T1.4(a), with respect to which the methodology shall describe the process to be followed by the DCC in such circumstances and provide for an appeal by a Party or a Manufacturer to the Panel. The Panel’s decision on such matter may then be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) for final determination of disputes regarding whether or not a Device Model does comply with the requirements of Section T1.4(a); and

(e) select Communications Hubs comprising Devices of the Device Models that the DCC first proposes to make available to Supplier Parties pursuant to the Communications Hub Services (which Device Models need not, at the start of Systems Integration Testing, have CPA Certificates or (where the Secretary of State so directs) a ZigBee Alliance Assurance Certificate).

T1.4 In selecting Devices (other than those comprising Communications Hubs), the DCC shall apply the following selection criteria:

(a) that the Device Models selected are SMETS compliant, provided that they need not (where the Secretary of State so directs) have a ZigBee Alliance Assurance Certificate or a DLMS Certificate and need not have a CPA Certificate until CPA Certificates are generally available for the relevant Device Type (and the DCC need only switch to a Device Model with those Assurance Certificates where it is reasonably practicable for it to do so, having regard to the timely achievement of the Testing Objectives);

(b) that Gas Meter Device Models and Electricity Meter Device Models are selected so that, in respect of each Communications Hub Device Model that the DCC first proposes to make available pursuant to the Communications Hub Services, there are at least two

Gas Meter Device Models and at least two Electricity Meter Device Models of a Manufacturer which is not the Manufacturer (or an Affiliate of the Manufacturer) of that Communications Hub Device Model; and

(c) that there will be sufficient Devices available for Systems Integration Testing, Interface Testing and User Entry Process Tests.

T1.5 Where the DCC is not able to select Devices that meet all the criteria set out in Section T1.4, it may relax the requirements in accordance with the Device Selection Methodology.

T1.6 The Device Selection Methodology must also include:

(a) in addition to the selection criteria set out in Section T1.4, any other reasonable criteria that the DCC considers appropriate and that are consistent with those set out in Section T1.4;

(b) an explanation of the level of assurance the DCC needs regarding the achievement of the Testing Objectives and of how the Device Selection Methodology will ensure that level of assurance; and

(c) any amendments to the process referred to in Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) for resolving Testing Issues which are to be applied by the DCC in respect of Testing Issues concerning Devices that arise during activities undertaken pursuant to this Section T.

Appeal of Methodology

T1.7 Within the 14 days after publication of the Device Selection Methodology under Section T1.3, any person that is a Party and/or a Manufacturer may refer the methodology to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the methodology meets the requirements of this Section T1 (which determination shall be final and binding for the purposes of this Code).

T1.8 Following a referral in accordance with Section T1.7, the DCC shall comply with any directions of the person making the determination thereunder to reconsider and/or amend the Device Selection Methodology. The DCC shall republish (including on the DCC Website) the methodology as so amended and the provisions of Section T1.7 and this Section T1.8 shall apply to any such amended methodology.

Compliance with Methodology

T1.9 Following its decision on which Device Models (or alternative arrangements) to select pursuant to the Device Selection Methodology, the DCC shall publish its decision on the DCC Website. The DCC shall not publish details of the Device Models (if any) which were proposed for selection but not selected. The DCC shall notify the Secretary of State, the Authority and the person which proposed any Device Models which were not selected of the DCC's decision (together with its reasons for selecting the Device Models (or other arrangements) that were selected, and for not selecting that person's proposed Device Models).

T1.10 Where any Party and/or Manufacturer believes that the DCC has not complied with the Device Selection Methodology as published from time to time in accordance with this Section T1, then such person may refer the matter to be determined by the Panel. The Panel's decision on such matter may be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code.

T2 <u>SYSTEMS INTEGRATION TESTING</u>

Overview

T2.1 Systems Integration Testing tests the capability of the DCC and the component parts of the DCC Systems together with the Communications Hubs selected pursuant to Section T1 to interoperate with each other and with the RDP Systems.

SIT Objective

T2.2 The objective of Systems Integration Testing (the "SIT Objective") is to demonstrate that the DCC and the component parts of the DCC Systems together with the Communications Hubs selected pursuant to Section T1 interoperate with each other and with the RDP Systems to the extent necessary in order that:

(a) the DCC is capable of complying with its obligations under Sections E (Registration Data), G (Security) and H (DCC Services); and

(b) the Registration Data Providers are capable of complying with the obligations under Section E (Registration Data) with which the Network Parties are obliged to procure that the Registration Data Providers comply,

in each case at levels of activity commensurate with the relevant Volume Scenarios.

T2.3 For the purposes of Section T2.2, the Sections referred to in that Section shall be construed by reference to:

(a) the decision or consultation document concerning the intended future content of those Sections most recently published by the Secretary of State prior to the date on which this Section T2.3 comes into force (regardless of whether the content of those documents has yet been incorporated into this Code, or whether those Sections are stated to not yet apply under Section X (Transition)); and

(b) to the extent not inconsistent with any document referred to in (a), any document regarding technical or procedural requirements which support those Sections which is published from time to time by the Secretary of State for the purposes of this Section T2.3.

T2.4 Systems Integration Testing is to be undertaken on a Region-by-Region basis and an RDP-System-by-RDP-System basis; such that the SIT Objective is to be achieved in respect of each Region and each RDP System separately.

SIT Approach Document

T2.5 The DCC shall develop a document (the "SIT Approach Document") which sets out:

(a) the reasonable entry criteria to be satisfied with respect to each Registration Data Provider prior to commencement of Systems Integration Testing in respect of that Registration Data Provider;

(b) the manner in which Systems Integration Testing is to be undertaken, including the respective obligations of the DCC, and each Registration Data Provider and the Volume Scenarios to be used;

(c) a reasonable timetable for undertaking and completing Systems Integration Testing;

(d) the frequency and content of progress reports concerning Systems Integration Testing to be provided by the DCC to the Panel (which the Panel shall make available to the Secretary of State, the Authority and Testing Participants), which reports must include details of Testing Issues identified and resolved and of any problems and solutions encountered with respect to Devices (the details of such Testing Issues to be anonymised and redacted as required in accordance with Section H14.44 (General: Testing Issue Resolution Process));

(e) (to the extent it is not reasonably practicable to use actual Devices) details of the alternative arrangements (which may include Test Stubs) to be used in their place (together with an explanation of how such arrangements will provide sufficient assurance that the SIT Objective has been met), in which case there must also be a process describing whether and how to switch to the use of actual Devices as they become available;

(f) where a Device Model is de-selected pursuant to the Device Selection Methodology, the process for switching to an alternate Device Model where practicable, or otherwise to Tests Stubs or an alternative arrangement;

(g) a Good Industry Practice methodology for determining whether the SIT Objective has been achieved in respect of each Region and each RDP System, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria; provided that one such exit criteria for each Region must include the successful use in that Region of each Communications Hub Device Model that the DCC first proposes to make available in that Region (save that such Communications Hub Device Models need not have CPA Certificates and need not (where the Secretary of State so directs) have a ZigBee Alliance Assurance Certificate);

(h) that the DCC will produce a report where the DCC considers that the exit criteria referred to in (g) above have been achieved for a Region or an RDP System (providing evidence of such achievement in such report), having consulted with each Registration Data Provider in relation to the exit criteria applicable to that Registration Data Provider; and

(i) how an auditor (that is sufficiently independent of the DCC, the DCC Service Providers and the Registration Data Providers) will be selected, and how such auditor will monitor the matters being tested pursuant to Systems Integration Testing, and confirm that the exit criteria referred to in (g) above have been achieved for a Region or an RDP System (such independent auditor to be appointed by the DCC on terms consistent with Good Industry Practice).

Approval of SIT Approach Document

T2.6 The DCC shall submit the SIT Approach Document to the Panel for the Panel’s approval as fit for the purposes envisaged by this Section T2.

T2.7 The DCC shall not submit the SIT Approach Document to the Panel under Section T2.6 until after the DCC has first published the Device Selection Methodology.

T2.8 Before submitting the SIT Approach Document to the Panel, the DCC shall consult with the Registration Data Providers regarding the SIT Approach Document. When submitting the SIT Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the Registration Data Providers. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T2.9 Where the Panel decides not to approve the SIT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the Registration Data Providers giving the reasons why it considers that it is not fit for the purposes envisaged in this Section T2. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the Registration Data Providers; and

(c) re-submit the document to the Panel for approval and comply with Section T2.8 (following which this Section T2.9 or Section T2.10 shall apply).

T2.10 Where the Panel decides to approve the SIT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the Registration Data Providers. In such circumstances, the DCC and each Registration Data Provider shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the SIT Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T2;

(b) is not fit for the purposes envisaged by this Section T2, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T2 and should be revised and re-submitted by the DCC in accordance with Section T2.9,

(and any such determination shall be final and binding for the purposes of this Code).

Commencement of Systems Integration Testing

T2.11 Subject to Section T2.12, once the SIT Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T2.10(b)), the DCC shall publish the approved document on the DCC Website and give notice to the Registration Data Providers of the date on which Systems Integration Testing is to commence. The SIT Approach Document must be published at least 3 months' (or such shorter period as the Secretary of State may direct) in advance of the date on which Systems Integration Testing is to commence.

T2.12 The DCC shall not publish the SIT Approach Document and give notice under Section T2.11 where the Panel's decision has been appealed under Section T2.10 (pending approval of the document thereunder or revision in accordance with a determination made under Section T2.10(b)), save that where:

(a) the Panel’s approval of the SIT Approach Document is appealed by one or more Registration Data Providers, the DCC shall nevertheless publish the document and give notice under Section T2.11 insofar as the document relates to the other Registration Data Providers; and/or

(b) the Panel’s approval of the SIT Approach Document is appealed by one or more Registration Data Providers or the DCC, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay notice under Section T2.11, in which case the DCC shall publish the document and give notice under Section T2.11 (noting the appeal).

T2.13 Prior to the commencement of Systems Integration Testing, the DCC shall assess whether or not each Registration Data Provider meets the entry criteria referred to in Section T2.5(a), and report to the Registration Data Provider and the Panel on the same. Each Network Party shall ensure that its Registration Data Provider:

(a) cooperates with the DCC in its assessment of whether the Registration Data Provider meets the entry criteria referred to in Section T2.5(a);

(b) takes all reasonable steps to meet those entry criteria by the date required in accordance with the SIT Approach Document; and

(c) notifies the Panel and the DCC as soon as reasonably practicable if the Registration Data Provider considers that it will not meet those criteria by that date.

T2.14 Systems Integration Testing in respect of each Registration Data Provider shall only commence once the Registration Data Provider meets the entry criteria referred to in Section T2.5(a). Any disagreement between the DCC and a Registration Data Provider as to whether the Registration Data Provider has met such entry criteria shall be determined by the Panel, provided that such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to the Registration Data Provider. The Panel’s decision on such matter may (within 14 days after the Panel’s decision) be appealed by the DCC or the affected Registration Data Provider to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code.

Systems Integration Testing

T2.15 The DCC shall comply with its obligations under the approved SIT Approach Document. The DCC shall use its reasonable endeavours to ensure that Systems Integration Testing is completed as soon as it is reasonably practicable to do so.

T2.16 Each Network Party shall ensure that its Registration Data Provider complies with its obligations under the approved SIT Approach Document.

T2.17 Where requested by the DCC and/or a Registration Data Provider, each Party shall take all reasonable steps to do all such things as are within its power and necessary or expedient in order to facilitate achievement of the SIT Objective.

T2.18 Where the DCC wishes to make amendments to the SIT Approach Document, the DCC shall consult with the Registration Data Providers regarding those amendments and submit those amendments to the Panel (in accordance with Section T2.8) for approval (following which Sections T2.9 to T2.12 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Sections T2.11 and T2.12 to giving notice were not included).

Completion of Systems Integration Testing

T2.19 Subject to Section T2.20, Systems Integration Testing shall end in respect of each Region or RDP System on the date notified as the end of Systems Integration Testing for that Region or RDP System by the DCC to the Secretary of State, the Authority, the Panel, the Parties and the Registration Data Providers.

T2.20 The DCC shall not notify the end of Systems Integration Testing in respect of each Region or RDP System before the following reports have been produced in respect of that Region or RDP System:

(a) the DCC’s report in accordance with the SIT Approach Document demonstrating that the exit criteria have been met in respect of that Region or RDP System (as envisaged by Section T2.5(h)); and

(b) the independent auditor’s report to the DCC in accordance with the SIT Approach Document confirming that the exit criteria have been met in respect of that Region or RDP System (as envisaged by Section T2.5(i)).

T2.21 On notifying the end of Systems Integration Testing for one or more Regions or RDP Systems, the DCC shall provide to the Authority and the Panel and (on request) to the Secretary of State:

(a) copies of the reports referred to in Section T2.20; and

(b) where relevant, a list of sections of the report or reports which the DCC considers should be redacted prior to circulation of the reports to the Parties, Registration Data Providers or Testing Participants where the DCC considers that those sections contain information which may pose a risk of Compromise to the DCC Total System or RDP Systems.

T2.22 Once directed to do so by the Panel, the DCC shall make copies of the reports referred to in Section T2.20 available to the Parties, the Registration Data Providers and the Testing Participants. Prior to making such copies available, the DCC shall redact those sections of the reports which it is directed to redact by the Panel where the Panel considers that those sections contain information which may pose a risk of Compromise to the DCC Total System or RDP Systems (which sections may or may not include those sections which the DCC proposed for redaction).

Testing Issues

T2.23 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of Systems Integration Testing. Each Registration Data Provider shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of Systems Integration Testing.

T2.24 During Systems Integration Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

T3 INTERFACE TESTING

Overview

T3.1 Interface Testing tests the capability of the DCC and the DCC Systems together with the Communications Hubs selected pursuant to Section T1 to interoperate with User Systems.

Interface Testing Objective

T3.2 The objective of Interface Testing (the "Interface Testing Objective") is to demonstrate that the DCC and the DCC Systems together with the Communications Hubs selected pursuant to Section T1 interoperate with User Systems to the extent necessary in order that the DCC is capable of complying with its obligations under Sections E (Registration Data), G (Security) and H (DCC Services) (in each case) at levels of activity commensurate with the relevant Volume Scenarios.

T3.3 For the purposes of Section T3.2, the Sections referred to in that Section shall be construed by reference to:

(a) the decision or consultation document concerning the intended future content of those Sections most recently published by the Secretary of State prior to the date on which this Section T3.3 comes into force (regardless of whether the content of those documents has yet been incorporated into this Code, or whether those Sections are stated to not yet apply under Section X (Transition)); and

(b) to the extent not inconsistent with any document referred to in (a), any document regarding technical or procedural requirements which support those Sections which is published from time to time by the Secretary of State for the purposes of this Section T3.3.

T3.4 Interface Testing is to be undertaken on a Region-by-Region basis; such that the Interface Testing Objective is to be demonstrated in respect of each Region separately. Interface Testing for a Region cannot be completed until Systems Integration Testing has been completed for that Region. For the avoidance of doubt, Interface Testing cannot be completed until Systems Integration Testing has been completed for each and every Region and RDP System.

T3.5 During Interface Testing, Parties who wish to do so, and who are ready to do so in accordance with the entry criteria for the User Entry Process Tests, shall be able to undertake the User Entry Process Tests (pursuant to Section H14 (Testing Services)).

Overlapping Provision of Systems Integration Testing and Interface Testing

T3.6 Prior to the start of Interface Testing, the DCC may propose to the Secretary of State, having regard to the overriding objective of completing Interface Testing in a timely manner, that Interface Testing should be commenced from some point during System Integration Testing for any or all Regions. The DCC's proposal must set out its analysis of the benefits and risks of doing so. Prior to submitting its proposal to the Secretary of State, the DCC shall consult with the other Parties regarding the proposal. The DCC shall also submit copies of the consultation responses received from Parties. Where it has submitted the proposal to the Secretary of State, the DCC shall publish the proposal and such consultation responses (to the extent that they are not marked confidential) on the DCC Website.

T3.7 Where the Secretary of State agrees with the DCC's recommendation pursuant to Section T3.6, then Interface Testing shall commence from the time recommended for the Regions included in the recommendation (notwithstanding anything to the contrary in the Interface Testing Approach Document or the SIT Approach Document).

Interface Testing Approach Document

T3.8 The DCC shall develop a document (the "Interface Testing Approach Document") which sets out:

(a) the reasonable entry criteria to be satisfied by the DCC with respect to the DCC Systems and the Communications Hubs selected pursuant to Section T1, and to be met by the Registration Data Providers with respect to the RDP Systems prior to commencement of Interface Testing in each Region;

(b) the entry criteria to be met by the Parties prior to their commencing the User Entry Process Tests (which criteria shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of Interface Testing);

(c) the manner in which Interface Testing is to be undertaken, including the respective obligations of the DCC, each other Party and each Registration Data Provider and the Volume Scenarios to be used;

(d) a reasonable timetable for undertaking and completing Interface Testing;

(e) the frequency and content of progress reports concerning Interface Testing to be provided by the DCC to the Panel (which the Panel shall make available to the Secretary of State, the Authority and Testing Participants), which reports must include details of Testing Issues identified and resolved and of any problems and solutions encountered with respect to Devices (the details of such Testing Issues to be anonymised and redacted as required in accordance with Section H14.44 (General: Testing Issue Resolution Process);

(f) (to the extent it is not reasonably practicable to use actual Devices) details of the alternative arrangements (which may include Test Stubs) to be used in their place (together with an explanation of how such arrangements will provide sufficient assurance that the Interface Testing Objective has been met), in which case there must also be a process describing whether and how to switch to the use of actual Devices as they become available;

(g) where a Device Model is de-selected pursuant to the Device Selection Methodology, the process for switching to an alternate Device Model where practicable, or otherwise to Tests Stubs or an alternative arrangement;

(h) the process by which the DCC will facilitate the Parties undertaking and completing the User Entry Process Tests (which process shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of Interface Testing);

(i) how, to the extent it is reasonably practicable to do so, the DCC will allow persons who are eligible to undertake User Entry Process Tests (pursuant to the Interface Testing Approach Document) to undertake those tests concurrently (provided that, where it is not reasonably practicable to do so, the DCC shall give priority to completion of the User Entry Process Tests by the Supplier Parties);

(j) a Good Industry Practice methodology for determining whether or not the Interface Testing Objective has been achieved in respect of each Region, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria (including, as described in Section T3.27, completion of User Entry Process Tests for that Region by two Large Supplier Parties and (where applicable pursuant to Section T3.21) by at least one Network Party in respect of the ‘Electricity Distributor’ User Role and/or at least one Network Party in respect of the ‘Gas Transporter’ User Role); and

(k) how the DCC will report to the Panel where the DCC considers that the exit criteria referred to in (j) above have been achieved in respect of a Region (providing evidence of such achievement), having consulted with the Registration Data Providers and the Parties who are obliged by this Section T3 to undertake the User Entry Process Tests.

Approval of Interface Testing Approach Document

T3.9 The DCC shall submit the Interface Testing Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T3.

T3.10 Before submitting the Interface Testing Approach Document to the Panel, the DCC shall consult with the other Parties, the Panel and the Registration Data Providers regarding the Interface Testing Approach Document. When submitting the Interface Testing Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the other Parties or the Registration Data Providers. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T3.11 Where the Panel decides not to approve the Interface Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the other Parties and the Registration Data Providers; and

(c) re-submit the document to the Panel for approval and comply with Section T3.10 (following which this Section T3.11 or Section T3.12 shall apply).

T3.12 Where the Panel decides to approve the Interface Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC, the other Parties and the Registration Data Providers giving reasons for such decision. In such circumstances, the DCC and each other Party and each Registration Data Provider shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the Interface Testing Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T3;

(b) is not fit for the purposes envisaged by this Section T3, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T3 and should be revised and re-submitted by the DCC in accordance with Section T3.11,

(which determination shall be final and binding for the purposes of this Code).

Commencement of Interface Testing

T3.13 Subject to Section T3.14, once the Interface Testing Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T3.12(b)), the DCC shall publish the approved document on the DCC Website and give at least 6 months' (or such shorter period as the Secretary of State may direct) notice to the other Parties of the date on which Interface Testing is to commence.

T3.14 Where the Panel's approval of the Interface Testing Approach Document is appealed by one or more persons under Section T3.12, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay publication and the giving of notice under Section T3.13, in which case the DCC shall publish the document and give notice under Section T3.13 (noting the appeal). Subject to the foregoing provisions of this Section T3.14, the DCC shall not publish the Interface Testing Approach Document and give notice under Section T3.13 where the Panel's decision has been appealed under Section T3.12 (pending the approval of the document thereunder or revision in accordance with a determination made under Section T3.12(b)).

T3.15 Prior to the commencement of Interface Testing and in accordance with the Interface Testing Approach document, the DCC shall assess whether or not each Large Supplier Party (and, where directed pursuant to Section T3.21, each Network Party) meets the entry criteria referred to in Section T3.8(b), and report to the Panel and that Party on the same. Each Large Supplier Party (and, where directed pursuant to Section T3.21, each Network Party) shall:

(a) take all reasonable steps to ensure that it meets the entry criteria referred to in Section T3.8(b) by the date required in accordance with the Interface Testing Approach Document; and

(b) notify the Panel and the DCC as soon as reasonably practicable if the Party considers that it will not meet those criteria by that date.

T3.16 Section H14.16 (User Entry Process Tests) shall apply where there is any disagreement between the DCC and a Party as to whether that Party has met the entry criteria for the User Entry Process Tests (as modified by the Interface Testing Approach Document), provided that:

(a) the Panel's decision on any such matter may be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code; and

(b) in the case of the Parties referred to in Section T3.15, any such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to that Party and any appeal must be brought within 14 days after the Panel's decision.

Interface Testing

T3.17 The DCC shall comply with its obligations under the approved Interface Testing Approach Document. The DCC shall use its reasonable endeavours to ensure that Interface Testing is completed as soon as it is reasonably practicable to do so.

T3.18 Each Network Party shall ensure that its Registration Data Provider complies with its obligations under the approved Interface Testing Approach Document.

T3.19 Each Party that undertakes the User Entry Process Tests prior to completion of Interface Testing shall do so in accordance with Section H14 (Testing Services) and the approved Interface Testing Approach Document.

T3.20 Each Large Supplier Party shall use its reasonable endeavours to commence the User Entry Process Tests as soon as reasonably practicable (in respect of the User Roles of 'Import Supplier' and/or 'Gas Supplier', depending on which Energy Supply Licence or Energy Supply Licences it holds). Each Large Supplier Party shall, on request, notify the Panel and the DCC of the Party's progress towards completing such User Entry Process Tests.

T3.21 Where directed to do so by the Secretary of State, each Network Party shall use its reasonable endeavours to commence the User Entry Process Tests as soon as reasonably practicable (in respect of the User Roles of 'Electricity Distributor' or 'Gas Transporter', as applicable). Following any such direction, each Network Party shall, on request, notify the Panel and the DCC of the Party's progress towards completing such User Entry Process Tests.

T3.22 Section H14.21 (User Entry Process Tests) shall apply where there is any disagreement between the DCC and a Party as to whether that Party has completed the User Entry Process Tests (as modified by the Interface Testing Approach Document), provided that:

(a) the Panel's decision on any such matter be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs), whose decision shall be final and binding for the purposes of this Code; and

(b) in the case of the Parties referred to in Section T3.15, any such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to that Party and any appeal must be brought within 14 days after the Panel's decision.

T3.23 Where the DCC wishes to make amendments to the Interface Testing Approach Document, the DCC shall consult with the other Parties regarding those amendments and submit those amendments to the Panel (in accordance with Section T3.10) for approval (following which Sections T3.11 to T3.14 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Sections T3.13 and T3.14 to giving notice were not included).

Completion of Interface Testing

T3.24 The DCC shall, once the DCC considers that the exit criteria (as envisaged by Section T3.8(j)) have been met in respect of any Region, in accordance with the Interface Testing Approach Document:

(a) provide to the Panel a report evidencing that such criteria have been met;

(b) where relevant, list those sections of the report which the DCC considers should be redacted prior to circulation of the report to the Parties, where the DCC considers that those sections contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems; and

(c) apply to the Panel to determine whether or not such exit criteria have been met,

and the DCC may either (as it reasonably considers appropriate in accordance with the Interface Testing Objective) do so in respect of individual Regions or some or all of the Regions collectively.

T3.25 On application of the DCC pursuant to Section T3.24, the Panel shall:

(a) determine whether or not the exit criteria have been met;

(b) notify its decision to the Secretary of State, the Authority and the Parties, giving reasons for its decision; and

(c) direct the DCC to publish its report, subject to the redaction of those sections of the report which the Panel considers to contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction).

T3.26 Where the DCC has provided a report to the Panel in accordance with Section T3.24, the Panel shall provide a complete copy on request to the Secretary of State and/or the Authority.

T3.27 Subject to Section T3.28, Interface Testing shall be completed once the Panel has confirmed that the exit criteria referred to Section T3.8(j) have been met in respect of each and every Region, which must include (in respect of each Region) that the following persons have completed User Entry Process Tests (for that Region):

(a) at least two Large Supplier Parties who are not an Affiliate of one another in respect of the ‘Import Supplier’ User Role, and at least two Large Supplier Parties who are not an Affiliate of one another in respect of the ‘Gas Supplier’ User Role; and

(b) (only where applicable pursuant to Section T3.21) at least one Network Party in respect of the ‘Electricity Distributor’ User Role and/or at least one Network Party in respect of the ‘Gas Transporter’ User Role.

T3.28 Each Party shall have the ability (within the 14 days after notification by the Panel) to refer each of the Panel’s decisions pursuant to Section T3.25 to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether or not the exit criteria have been met in respect of the Region in question (which determination shall be final and binding for the purposes of this Code).

T3.29 Where, following the application of the DCC pursuant to Section T3.24, the Panel or the person which determines a referral under Section T3.28 determines that one or more of the exit criteria have not been met, the DCC shall undertake further testing in order to demonstrate that the exit criteria have been met and shall resubmit its report under Section T3.24.

Testing Issues

T3.30 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of Interface Testing. Each Party participating in Interface Testing shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of Interface Testing.

T3.31 During Interface Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

T4 <u>END-TO-END TESTING</u>

Overview

T4.1 End-to-End Testing allows for provision of the User Entry Process Tests and Device and User System Tests, subject to any modifications necessary for the purposes of transition.

Overlapping Provision of Interface Testing and End-to-End Testing

T4.2 Prior to the start of End-to-End Testing, the DCC may recommend to the Panel, having regard to the overriding objective of completing Interface Testing in a timely manner, that End-to-End Testing should be provided from the commencement of or from some point during Interface Testing. Where the DCC so recommends, it must provide a report to the Panel on the benefits and risks of the DCC providing End-To-End Testing in parallel with Interface Testing (rather than following completion of Interface Testing). Prior to submitting its report to the Panel, the DCC shall consult with the other Parties regarding the recommendation. The DCC shall also submit copies of the consultation responses received from Parties. Where it has submitted its report to the Panel, the DCC shall publish the report and such consultation responses (to the extent that they are not marked confidential) on the DCC Website.

T4.3 Where the Panel agrees with the DCC's recommendation pursuant to Section T4.2, then End-to-End Testing shall commence from the time recommended (notwithstanding the notice period in Section T4.9). Otherwise, End-to-End Testing shall commence on completion of Interface Testing (or such later date as is necessary to allow compliance with Section T4.9).

End-to-End Testing Approach Document

T4.4 The DCC shall develop a document (the "End-to-End Testing Approach Document") which sets out:

(a) the manner in which User Entry Process Tests and Device and User System Tests are to be provided during End-to-End Testing, which shall be consistent with the relevant requirements of Section H14 (Testing Services) subject only to amendments reasonably required for the purposes of transition; and

(b) that, to the extent it is reasonably practicable to do so, the DCC shall allow persons who are eligible to undertake tests pursuant to the End-to-End Testing Approach Document to undertake those tests concurrently (provided that, where it is not reasonably practicable to do so, the DCC shall give priority to completion of the User Entry

Process Tests by the Supplier Parties during the period prior to the completion of Interface Testing and the DCC shall otherwise schedule Testing Participants as is reasonable for the purposes of transition).

Approval of End-to-End Testing Approach Document

T4.5 The DCC shall submit the End-to-End Testing Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T4.

T4.6 Before submitting the End-to-End Testing Approach Document to the Panel, the DCC shall consult with the other Parties, the Panel and those persons entitled to undertake Device and User System Tests regarding the End-to-End Testing Approach Document. When submitting the End-to-End Testing Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the other Parties and such persons. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T4.7 Where the Panel decides not to approve the End-to-End Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the other Parties and those persons entitled to undertake Device and User Systems Tests; and

(c) re-submit the document to the Panel for approval and comply with Section T4.6 (following which this Section T4.7 or Section T4.8 shall apply).

T4.8 Where the Panel decides to approve the End-to-End Testing Approach Document submitted for approval, the Panel shall notify such decision to the DCC, the other Parties and the other persons who provided consultation responses in accordance with Section T4.6, giving reasons for such decision. In such circumstances, the DCC and each other Party shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the End-to-End Testing Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T4;

(b) is not fit for the purposes envisaged by this Section T4, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T4 and should be revised and re-submitted by the DCC in accordance with Section T4.7,

(and any such determination shall be final and binding for the purposes of this Code).

Commencement of End-to-End Testing

T4.9 Subject to Section T4.10, once the End-to-End Testing Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T4.8(b)), the DCC shall publish the approved document on the DCC Website and (subject to Section T4.3) give at least 6 months' prior notice to Testing Participants of the date on which End-to-End Testing is to commence (or such shorter period as the Secretary of State may direct).

T4.10 Where the Panel's approval of the End-to-End Testing Approach Document is appealed by one or more persons, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay publication and the giving of notice under Section T4.9, in which case the DCC shall publish the document and give notice under Section T4.9 (noting the appeal). Subject to the foregoing provisions of this Section T4.10, the DCC shall not publish the End-to-End Testing Approach Document and give notice under Section T4.9 where the Panel's decision has been appealed under Section T4.8 (pending the approval of the document thereunder or revision in accordance with a determination made under Section T4.8(b)).

End-to-End Testing

T4.11 The DCC shall comply with its obligations under the approved End-to-End Testing Approach Document.

T4.12 Each Party that seeks to undertake User Entry Process Tests or Device and System Tests during End-to-End Testing shall do so in accordance with the approved End-to-End Testing Approach Document. Where the DCC is to provide Testing Services during End-to-End Testing to a person that is not a Party, the DCC shall act in accordance with any relevant provisions of the End-to-End Testing Approach Document.

T4.13 Where the DCC wishes to make amendments to the End-to-End Testing Approach Document, the DCC shall consult with the other Parties, the Panel and those persons entitled to undertake Device and User System Tests regarding those amendments and submit those amendments to the Panel (in accordance with Section T4.6) for approval (following which Sections T4.7 to T4.10 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Section T4.9 and T4.10 to giving notice were not included).

Disputes

T4.14 Section T3.16 shall apply during Interface Testing in respect of the entry criteria for the User Entry Process Tests. Otherwise, in the case of those disputes relating to User Entry Process Tests and Device and User System Tests that would ordinarily be subject to the Authority's determination pursuant to Section H14 (Testing Services), during End-to-End Testing, the Secretary of State may direct that such disputes are determined by the Secretary of State (or, where the Secretary of State so directs such other person as the Secretary of State directs), rather than the Authority. The determination of such disputes by the Secretary of State (or such other person as the Secretary of State directs) shall be final and binding for the purposes of this Code.

Completion of End-to-End Testing

T4.15 Subject to Section T4.17, End-to-End Testing shall cease on the date 12 months after it commenced.

T4.16 During the ninth month of End-to-End Testing (or at such other time as the DCC and the Panel may agree), the DCC shall submit a recommendation to the Panel as to whether or not the period of End-to-End Testing should be extended by an additional 6 months. Prior to submitting such recommendation to the Panel, the DCC shall consult the Testing Participants on the matter. When submitting such recommendation to the Panel, the DCC shall also submit copies of any consultation responses received from the Testing Participants. The DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T4.17 The Panel shall, after receipt of the DCC’s recommendation in accordance with Section T4.16, decide whether or not the period of End-to-End Testing should be extended by an additional 6 months. The Panel shall notify the Testing Participants of its decision, and of the reasons for its decision. Where the Panel decides that the period of End-to-End Testing should be extended by an additional 6 months, then End-to-End Testing shall end on the date 18 months after the date it started (which decision shall be final and binding for the purposes of this Code).

Testing Issues

T4.18 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of End-to-End Testing. Each Party participating in User Entry Process Tests or Device and System Tests during End-to-End Testing shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of Interface Testing.

T4.19 During End-to-End Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

T5 SMKI AND REPOSITORY TESTING

Overview

T5.1 SMKI and Repository Testing tests the capability of the DCC and the component parts of the DCC Systems to interoperate with the Systems of Parties to the extent necessary for the SMKI Services and the SMKI Repository Service.

SRT Objective

T5.2 The objective of SMKI and Repository Testing (the "SRT Objective") is to demonstrate that the DCC and the DCC Systems interoperate with each other and with Systems of Parties to the extent necessary in order that the DCC is capable of complying with its obligations under Section L (Smart Metering Key Infrastructure) at (during the period of Interface Testing) the levels of activity reasonably anticipated during the period of Interface Testing, and (thereafter) the levels of activity set out in Section L (Smart Metering Key Infrastructure).

T5.3 For the purposes of Section T5.2, the Sections referred to in that Section shall be construed by reference to:

(a) the decision or consultation document concerning the intended future content of those Sections most recently published by the Secretary of State prior to the date on which this Section T5.3 comes into force (regardless of whether the content of those documents has yet been incorporated into this Code, or whether those Sections are stated to not yet apply under Section X (Transition)); and

(b) to the extent not inconsistent with any document referred to in (a), any document regarding technical or procedural requirements which support those Sections which is published from time to time by the Secretary of State for the purposes of this Section T5.3.

T5.4 During SMKI and Repository Testing, Parties who wish to do so, and who are ready to do so in accordance with the entry criteria for the SMKI and Repository Entry Process Tests, shall be able to undertake the SMKI and Repository Entry Process Tests (pursuant to Section H14 (Testing Services)).

SRT Approach Document

T5.5 The DCC shall develop a document (the "SRT Approach Document") which sets out:

(a) the reasonable entry criteria to be satisfied by the DCC with respect to the DCC Systems and the Communications Hubs selected pursuant to Section T1 prior to commencement of SMKI and Repository Testing;

(b) the entry criteria to be met by each Party prior to its commencing the SMKI and Repository Entry Process Tests (which criteria shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of SMKI and Repository Testing);

(c) the manner in which SMKI and Repository Testing is to be undertaken, including the respective obligations of the DCC and each other Party;

(d) a reasonable timetable for undertaking and completing SMKI and Repository Testing;

(e) the frequency and content of progress reports concerning SMKI and Repository Testing to be provided by the DCC to the Panel (which the Panel shall make available to the Secretary of State, the Authority and Testing Participants), which reports must include details of Testing Issues identified and resolved and of any problems and solutions encountered with respect to Devices (the details of such Testing Issues to be anonymised and redacted as required in accordance with Section H14.44 (General: Testing Issue Resolution Process));

(f) the process by which the DCC will facilitate Parties undertaking and completing the SMKI and Repository Entry Process Tests (which process shall be consistent with the relevant requirements of Section H14 (Testing Services), subject only to amendments reasonably required for the purposes of SMKI and Repository Testing);

(g) a Good Industry Practice methodology for determining whether or not the SRT Objective has been achieved, including details of the exit criteria to be achieved and the level of assurance that will be delivered by achievement of those exit criteria (including completion of SMKI and Repository Entry Process Tests by two Large Supplier Parties as described in Section T5.20); and

(h) how the DCC will report to the Panel where the DCC considers that the exit criteria referred to in (g) above have been achieved (providing evidence of such achievement), having consulted with the Parties who have participated in SMKI and Repository Testing.

Approval of SRT Approach Document

T5.6 The DCC shall submit the SRT Approach Document to the Panel for the Panel's approval as fit for the purposes envisaged by this Section T5.

T5.7 Before submitting the SRT Approach Document to the Panel, the DCC shall consult with the other Parties, the Panel and the SMKI PMA regarding the SRT Approach Document. When submitting the SRT Approach Document to the Panel, the DCC shall also submit copies of the consultation responses received from the other Parties. In addition, the DCC shall publish such consultation responses (to the extent not marked confidential) on the DCC Website.

T5.8 The Panel shall consult with the SMKI PMA prior to deciding whether or not to approve the SRT Approach Document submitted for approval.

T5.9 Where the Panel decides not to approve the SRT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC shall:

(a) revise the document to address such reasons;

(b) re-consult with the other Parties; and

(c) re-submit the document to the Panel for approval and comply with Section T5.7 (following which Section T5.8 shall apply and this Section T5.9 or Section T5.10 shall apply).

T5.10 Where the Panel decides to approve the SRT Approach Document submitted for approval, the Panel shall notify such decision to the DCC and the other Parties giving reasons for such decision. In such circumstances, the DCC and each other Party shall have the ability (within the 14 days after notification by the Panel) to refer the matter to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether the SRT Approach Document:

(a) should be approved as fit for the purposes envisaged by this Section T5;

(b) is not fit for the purposes envisaged by this Section T5, but will be deemed to be approved if it is revised by the DCC in accordance with the determination; or

(c) is not fit for the purposes envisaged by this Section T5 and should be revised and re-submitted by the DCC in accordance with Section T5.9, (which determination shall be final and binding for the purposes of this Code).

Commencement of SMKI and Repository Testing

T5.11 Subject to Section T5.12, once the SRT Approach Document has been approved by the Panel (or deemed to be approved by the Panel under Section T5.10(b)), the DCC shall publish the approved document on the DCC Website and give at least 3 month's (or such shorter period as the Secretary of State may direct) notice to the other Parties of the date on which SMKI and Repository Testing is to commence. The SRT Approach Document must be published at least 3 months (or such shorter period as the Secretary of State may direct) in advance of the date on which Systems Integration Testing is to commence.

T5.12 Where the Panel's approval of the SRT Approach Document is appealed by one or more persons under Section T5.10, the Panel may nevertheless direct that the matter appealed is not of a nature that should delay publication and the giving of notice under Section T5.11, in which case the DCC shall publish the document and give notice under Section T5.11 (noting the appeal). Subject to the foregoing provisions of this Section T5.12, the DCC shall not publish the SRT Approach Document and give notice under Section T5.11 where the Panel's decision has been appealed under Section T5.10 (pending the approval of the document thereunder or revision in accordance with a determination made under Section T5.10(b)).

T5.13 Prior to the commencement of SMKI and Repository Testing and in accordance with the SRT Approach document, the DCC shall assess whether or not each Large Supplier Party meets the entry criteria referred to in Section T5.5(b), and report to the Panel and that Party on the same. Each Large Supplier Party shall:

(a) take all reasonable steps to ensure that it meets the entry criteria referred to in Section T5.5(b) by the date required in accordance with the SRT Approach Document; and

(b) notify the Panel and the DCC as soon as reasonably practicable if the Party considers that it will not meet those criteria by that date.

T5.14 Section H14.25 (SMKI and Repository Entry Process Tests) shall apply where there is any disagreement between the DCC and a Party as to whether that Party has met the entry criteria for the SMKI and Repository Entry Process Tests (as modified by the SRT Approach Document), provided that:

(a) the Panel's decision on any such matter may be appealed to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the

Secretary of State directs), whose decision shall be final and binding for the purposes of this Code; and

(b) in the case of the Parties referred to in Section T5.13, such disagreement must be notified to the Panel within 14 days of the DCC notifying its assessment to that Party and any appeal must be brought within 14 days after the Panel's decision.

SMKI and Repository Testing

T5.15 The DCC shall comply with its obligations under the approved SRT Approach Document. The DCC shall use its reasonable endeavours to ensure that SMKI and Repository Testing is completed as soon as it is reasonably practicable to do so.

T5.16 Each Party that undertakes the SMKI and Repository Entry Process Tests pursuant to the SRT Approach Document shall do so in accordance with Section H14 (Testing Services) and the approved SRT Approach Document.

T5.17 Each Large Supplier Party shall use its reasonable endeavours to commence the SMKI and Repository Entry Process Tests as soon as reasonably practicable (in respect of all the roles to which the SMKI and Repository Entry Process Tests apply). Each Large Supplier Party shall, on request, notify the Panel and the DCC of the Party's progress towards completing such SMKI and Repository Entry Process Tests.

T5.18 Where the DCC wishes to make amendments to the SRT Approach Document, the DCC shall consult with the other Parties regarding those amendments and submit those amendments to the Panel (in accordance with Section T5.7) for approval (following which Sections T5.8 to T5.12 shall apply as if the references in those Sections to approval of the document were to approval of the amendments and as if the references in Sections T5.11 and T5.12 to giving notice were not included).

Completion of SMKI and Repository Testing

T5.19 The DCC shall, once the DCC considers that the exit criteria (as envisaged by Section T5.5(g)) have been met, in accordance with the SRT Approach Document:

(a) provide to the Panel a report evidencing that such criteria have been met;

(b) where relevant, list those sections of the report which the DCC considers should be redacted prior to circulation of the report to the Parties, where the DCC considers that those sections contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems; and

(c) apply to the Panel to determine whether or not such exit criteria have been met.

T5.20 Such exit criteria must include a requirement that at least two Large Supplier Parties who are not an Affiliate of one another have each completed the SMKI and Repository Entry Process Tests to become:

(a) an Authorised Subscriber under the Organisation Certificate Policy;

(b) an Authorised Subscriber under the Device Certificate Policy; and

(c) eligible to access the SMKI Repository.

T5.21 On application of the DCC pursuant to Section T5.19, the Panel shall:

(a) determine whether or not the exit criteria have been met;

(b) notify its decision to the Secretary of State, the Authority and the Parties, giving reasons for its decision ; and

(c) direct the DCC to publish its report, subject to the redaction of those sections of the report which the Panel considers to contain information which may pose a risk of Compromise to the DCC Total System, RDP Systems and/or User Systems (which sections may or may not include those sections which the DCC proposed for redaction)

T5.22 Where the DCC has provided a report to the Panel in accordance with Section T5.19, the Panel shall provide a complete copy on request to the Secretary of State and/or the Authority.

T5.23 Subject to Section T5.24, SMKI and Repository Testing shall be completed once the Panel has determined that the exit criteria referred to Section T5.5(g) have been met in respect of the Parties referred to in Section T5.20.

T5.24 Each Party shall have the ability (within the 14 days after notification by the Panel) to refer the Panel’s decision pursuant to Section T5.21 to the Authority (or, where the Secretary of State so directs, to the Secretary of State or such other person as the Secretary of State directs) to determine whether or not the exit criteria have been met in respect of the Parties referred to in Section T5.20 (which determination shall be final and binding for the purposes of this Code).

T5.25 Where, on the application of the DCC pursuant to Section T5.19, it has been determined that one or more of the exit criteria have not been met, the DCC shall undertake further testing in order to demonstrate that the exit criteria have been met and shall resubmit its report in accordance with Section T5.19.

Testing Issues

T5.26 Sections H14.37 to H14.45 (General: Testing Issue Resolution Process) shall apply for the purposes of SMKI and Repository Testing. Each Party participating in SMKI and Repository Testing shall be deemed to be a Testing Participant for such purposes, and may raise a Testing Issue in respect of SMKI and Repository Testing.

T5.27 During SMKI and Repository Testing, the DCC shall provide the Secretary of State with copies of the reports which are generated by the DCC or the DCC Service Provider in respect of Testing Issues (without redacting those reports as ordinarily required by Sections H14.37 to H14.45).

T6 DEVELOPMENT OF TEST SCENARIOS DOCUMENTS

Overview

T6.1 The Common Test Scenarios Document and the SMKI and Repository Test Scenarios Document are to be developed by the DCC pursuant to this Section T6, and incorporated into this Code pursuant to Section X5 (Incorporation of Certain Documents into this Code).

Purpose of the Test Scenarios Documents

T6.2 The purpose of each of the Common Test Scenarios Document and the SMKI and Repository Test Scenarios Document is set out in Section H14 (Testing Services).

T6.3 The Common Test Scenarios Document must include test scenarios for testing use of the Self-Service Interface and the DCC User Gateway and any entry requirements (for particular User Roles) prior to execution of those tests. In respect of the DCC User Gateway, such tests must include (for each User Role) a requirement for the successful testing of Service Requests for each Service set out in the DCC User Gateway Services Schedule in respect of that User Role.

Process to Develop Documents

T6.4 The procedure by which the DCC is to develop each of the Common Test Scenarios Document and the SMKI and Repository Test Scenarios Document is as follows:

(a) the DCC shall produce draft documents by such date as is reasonably necessary to meet the applicable date under Section T6.4(d);

(b) in producing each draft document, the DCC must consult appropriately with the Parties;

(c) where disagreements with the Parties arise concerning the proposed content of either document, the DCC shall seek to reach an agreed solution with them, but without prejudice to the purposes of the document;

(d) having complied with (b) and (c) above, the DCC shall submit each draft document to the Secretary of State as soon as is reasonably practicable, and (in any case) by the date seven months prior to the expected commencement date of Interface Testing as set out in the Interface Testing Approach Document (or such later date as the Secretary of State may direct);

(e) when submitting a draft document under (d) above, the DCC shall indicate to the Secretary of State:

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

(ii) any areas of disagreement that arose during the consultation process and that have not been resolved;

(f) the DCC must comply with the requirements with respect to process and timeframe of any direction that is given by the Secretary of State to resubmit either document.

T7 ENDING OF THE APPLICATION OF THIS SECTION T

T7.1 This Section T shall cease to apply, and this Code shall automatically be modified so as to delete this Section T, on the last to occur of the following:

(a) completion of Interface Testing;

(b) completion of End-to-End Testing; and

(c) completion of SMKI and Repository Testing.”

SCHEDULE 6

NEW APPENDIX A FOR INSERTION INTO SMART ENERGY CODE

"APPENDIX A – SMKI DEVICE CERTIFICATE POLICY

CONTENTS

1 INTRODUCTION

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

- shall be known as the "**SMKI Device Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(A) This Policy sets out the arrangements relating to:

(i) Device Certificates; and

(ii) DCA Certificates.

(B) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been registered with the Internet Address Naming Authority and assigned an OID of 1.2.826.0.1. 8641679.1.2.1.2.

1.3 SMKI PARTICIPANTS

1.3.1 The Device Certification Authority

(A) The definition of Device Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The 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 RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code.

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of a Device Certificate must be a Device (other than a Type 2 Device) represented by the identifier in the subjectAltName field of the Device Certificate Profile in accordance with Annex B.

(B) The Subject of a DCA Certificate must be the entity named in the Subject field of the Root DCA Certificate Profile or Issuing DCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code.

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF DEVICE CERTIFICATES AND DCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The DCA shall ensure that Device Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Devices in accordance with or pursuant to the Code.

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

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

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

(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 shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the DCA or the SMKI PMA.

1.5.3 Person Determining Device CPS Suitability for the Policy

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the SMKI PMA to approve the Device CPS.

1.5.4 Device CPS Approval Procedures

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the procedure by which the SMKI PMA may approve the Device CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The Registration Authority Policies and Procedures (the **RAPP**) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

(A) Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The DCA shall lodge the following in the SMKI Repository:

(i) each Device Certificate that has been accepted by a Subscriber;

(ii) each DCA Certificate;

(iii) each version of the RAPP;

(iv) each version of the Recovery Procedure; and

(v) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

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

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The DCA shall ensure that:

(i) each Device Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each DCA Certificate is lodged to the SMKI Repository promptly on being Issued;

(iii) the RAPP is lodged in the SMKI Repository, and a revised version of the RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) the Recovery Procedure is lodged in the SMKI Repository, and a revised version of Recovery Procedure is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code; and

(v) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the RAPP to ensure that the name of the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the RAPP to ensure that the name of the Subject of each Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Provision is made in the RAPP to:

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

(ii) permit the DCA to Authenticate each Eligible Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of Organisation Identity

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

(i) procedure to be followed by a Party in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the DCA will determine whether a Party is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party shall be Authenticated by the DCA for that purpose.

(B) Provision is made in the RAPP for the purpose of ensuring that the criteria in accordance with which the DCA shall Authenticate a Party shall be set to Level 3 pursuant to GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.4 Authentication of Devices

(A) Provision is made in the RAPP in relation to the Authentication of Devices.

3.2.5 Non-verified Subscriber Information

(A) The DCA shall:

(i) verify all information in relation to DCA Certificates;

(ii) require each Eligible Subscriber to verify the information contained in any Certificate Signing Request in respect of a Device Certificate.

(B) Further provision on the content of DCA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.6 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.7 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The DCA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

[*Not applicable in this Policy*]

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

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

(i) in respect of a Device Certificate:

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

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

(ii) in respect of a DCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain a DCA Certificate.

4.1.2 Enrolment Process and Responsibilities

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

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

(ii) maintenance by the DCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the RAPP in relation to the establishment of an enrolment process in respect of DCA Personnel and DCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the DCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the RAPP in relation to the Authentication by the DCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the RAPP, this Policy or any other provision of the Code, the DCA:

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

(ii) may give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

(B) Where any Certificate Signing Request satisfies the requirements set out in the RAPP, this Policy or any other provision of the Code, the DCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the DCA is made in Section L8 of the Code (SMKI Performance Standards and Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 DCA Actions during Certificate Issuance

(A) The DCA may Issue a Certificate only:

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

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

(B) The DCA shall ensure that:

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

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

(C) A DCA Certificate may only be:

(i) Issued by the DCA; and

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

(D) A Device Certificate may only be:

(i) Issued by the DCA; and

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

(E) The DCA shall not Issue a Device Certificate which is signed using an Issuing DCA Private Key after the first in time of the following:

(i) the time which is three months after the time at which any element of the Issuing DCA Private Key first became operational;

(ii) the time at which the DCA Issues the 100,000th Device Certificate which is signed using that Issuing DCA Private Key.

(F) For the purposes of paragraph (E), the DCA shall ensure that the Device CPS incorporates:

(i) a procedure for determining:

(a) how the DCA will calculate when each of the times specified in that paragraph occurs; and

(b) for that purpose, when any element of the Issuing DCA Private Key first became operational; and

(ii) provisions for notifying the SMKI PMA when either of the times specified in that paragraph is approaching.

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

(A) Provision is made in the RAPP for the DCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the RAPP to:

(i) specify a means by which an Eligible Subscriber may clearly indicate to the DCA its acceptance of a Certificate which has been Issued to it; and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued indicates its acceptance of that Certificate in accordance with the specified means of doing so.

(B) A Certificate which has been Issued by the DCA shall not be treated as valid for any purposes of this Policy or the Code until it is accepted by the Eligible Subscriber to which it was Issued.

(C) The DCA shall maintain a record of all Certificates which have been Issued by it and accepted by a Subscriber.

(D) Further provision in relation to the acceptance of Certificates is made in Section L11 of the Code (Subscriber Obligations).

4.4.2 Publication of Certificates by the DCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy.

4.4.3 Notification of Certificate Issuance by the DCA to Other Entities

(A) The DCA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11 of the Code (Subscriber Obligations); and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates

(B) The DCA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

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

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to a DCA Private Key:

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

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

(c) promptly both notify the SMKI PMA and verifiably destroy the DCA Private Key Material.

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

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

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

(C) An Eligible Subscriber may request a replacement for a Certificate at any time by applying for the Issue of a new Device Certificate in accordance with this Policy.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the DCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the DCA to Other Entities

See Part 4.4.3 of this Policy

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The DCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated by a Device, the Eligible Subscriber which is responsible for that Device shall apply for the Issue of a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

4.7.6 Publication of the Re-Keyed Certificate by the DCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

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

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the DCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the DCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) This Policy does not support the revocation or suspension of Certificates.

(B) The DCA shall not provide any service of revoking or suspending a Certificate.

4.9.2 Who can Request Revocation

[*Not applicable in this Policy*]

4.9.3 Procedure for Revocation Request

[*Not applicable in this Policy*]

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which DCA must process the Revocation Request

[*Not applicable in this Policy*]

4.9.6 Revocation Checking Requirements for Relying Parties

[*Not applicable in this Policy*]

4.9.7 CRL Issuance Frequency (if applicable)

[*Not applicable in this Policy*]

4.9.8 Maximum Latency for CRLs (if applicable)

[*Not applicable in this Policy*]

4.9.9 On-line Revocation/Status Checking Availability

[*Not applicable in this Policy*]

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

[*Not applicable in this Policy*]

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The DCA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[*Not applicable in this Policy*]

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The DCA shall ensure that the DCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The DCA shall ensure that:

(i) all of the physical locations in which the DCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The DCA shall ensure that the DCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with:

(i) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(ii) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

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

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

5.1.2 Physical Access

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to DCA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposure

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the DCA.

5.1.7 Waste Disposal

(A) The DCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the DCA are disposed of only using secure methods of disposal in accordance with:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time.

5.1.8 Off-Site Back-Up

(A) The DCA shall regularly carry out a Back-Up of:

(i) all Data held on the DCA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the DCA shall ensure that the Device CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The DCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the Device CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise DCA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The DCA shall ensure that, where any elements of the DCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of DCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The DCA shall ensure that:

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

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

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

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

5.2.2 Number of Persons Required per Task

(A) The DCA shall ensure that the Device CPS incorporates provisions designed to establish:

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

(ii) the application of controls to the actions of all members of DCA Personnel who are Privileged Persons, identifying in particular any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions.

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

(i) DCA Systems administration;

(ii) DCA Systems operations;

(iii) DCA Systems security; and

(iv) DCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The DCA shall ensure that all DCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the DCA, not have been previously relieved of any past assignment (whether for the DCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The DCA shall ensure that all DCA Personnel have, as a minimum, passed a Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The DCA shall ensure that the Device CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of DCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorised Actions

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

(A) The DCA shall ensure that all DCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the Device CPS; and

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The DCA shall ensure that:

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

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

(a) the activities of DCA Personnel;

(b) the use of DCA equipment;

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

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the DCA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The DCA shall ensure that:

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

(ii) all DCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the DCA Systems in compliance with:

(a) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(b) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time;

(B) The DCA shall ensure that the Device CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The DCA shall ensure that the Device CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of DCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The DCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The DCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the

Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The DCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the DCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The DCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the Device CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the DCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The DCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The DCA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The DCA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The DCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the DCA's operations.

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

5.6 KEY CHANGEOVER

5.6.1 Device Certificate Key Changeover

(A) The DCA shall Issue a new Device Certificate in relation to a Device where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the RAPP and this Policy.

5.6.2 DCA Key Changeover

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

(i) verifiably destroy the Issuing DCA Private Key Material;

(ii) not revoke the related Issuing DCA Public Key (which may continue to be used for the purpose of validating Digital Signatures generated using the Issuing DCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any Device Certificate subsequently Issued by it is Issued using the Issuing DCA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(v) in its capacity as the Root DCA:

(a) Issue a new Issuing DCA Certificate; and

(b) promptly lodge that Issuing DCA Certificate in the SMKI Repository.

(B) The DCA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The DCA shall ensure that the Device CPS incorporates a business continuity plan which shall be designed to ensure continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the DCA Systems or major failure in the DCA processes.

(B) The DCA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) In the event of the Compromise of any DCA Private Key, the DCA shall:

(i) not revoke the related Issuing DCA Public Key;

(ii) not revoke any Device Certificates Issued using the Issuing DCA Private Key;

(iii) not issue any further Device Certificates using the Issuing DCA Private Key;

(iv) treat the event in the same manner as if it were a Major Security Incident in accordance with Section G2 of the Code (System Security: Obligations on the DCC); and

(v) immediately notify the SMKI PMA.

(D) The DCA shall ensure that the Device CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any Issuing DCA Private Key or any part of the DCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The DCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The DCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[*Not applicable in this Policy*]

6 TECHNICAL SECURITY CONTROLS

The DCA shall ensure that the Device CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root DCA, the Issuing DCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The DCA shall ensure that all DCA 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 DCA 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 DCA shall not generate any Private Key or Public Key other than a DCA Key.

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root DCA and Issuing DCA; and

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

6.1.4 DCA Public Key Delivery to Relying Parties

(A) The DCA shall ensure that the Device CPS incorporates provisions:

(i) in relation to the manner by which each DCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the DCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The DCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the following size and characteristics:

(i) Elliptic Curve on the NIST P-256 curve in its uncompressed form, as defined in RFC5480 and as further set out in the GB Companion Specification; and

(ii) Digital Signature verification with Elliptic Curve Digital Signature Authentication using SHA256 and as further set out in the GB Companion Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The DCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

(A) The DCA shall ensure that each Certificate that is Issued by it has a 'keyUsage' field in accordance with RFC5759 and RFC5280.

(B) The DCA shall ensure that each Device Certificate that is Issued by it has a 'keyUsage' of either:

(i) 'digitalSignature'; or

(ii) 'keyAgreement'.

(C) The DCA shall ensure that each DCA Certificate that is Issued by it has a 'keyUsage' of 'keyCertSign'.

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

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The DCA shall ensure that all DCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The DCA shall ensure that all DCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(C) The DCA shall ensure that no DCA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The DCA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Device CPS; and

(ii) require to be unblocked by an authorised member of DCA Personnel who has been Authenticated as such following a process which shall be set out in the Device CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The DCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The DCA may Back-Up DCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing DCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The DCA shall ensure that no DCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services;

(ii) in accordance with a level of protection which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The DCA shall ensure that the Cryptographic Module in which any DCA Private Key is stored may be accessed only by an authorised member of DCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The DCA shall ensure that any DCA Private Key shall be capable of being de-activated by means of the DCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the Device CPS.

6.2.10 Method of Destroying Private Key

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

(B) The DCA shall ensure that no DCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the DCA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The DCA shall ensure that it archives DCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The DCA shall ensure that:

(i) the Validity Period of each Certificate shall be an indefinite period; and

(ii) for this purpose, it uses the ‘notAfter’ value specified in Annex B.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The DCA shall ensure that any Cryptographic Module within which a DCA Key is held has Activation Data that are unique and unpredictable.

(B) The DCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the DCA Keys; and

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

6.4.2 Activation Data Protection

(A) The DCA shall ensure that the Device CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The DCA shall ensure that the Device CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the DCA;

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

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

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

(v) the audit of security related events; and

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

6.5.2 Computer Security Rating

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

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The DCA shall ensure that any software which is developed for the purpose of establishing a functionality of the DCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The DCA shall ensure that the Device CPS incorporates provisions which are designed to ensure that the DCA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root DCA

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

6.7.2 Protection Against Attack

(A) The DCA shall use its best endeavours to ensure that the DCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event;

(ii) any unauthorised attempt to connect to them.

(B) The DCA shall use its reasonable endeavours to ensure that the DCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing DCA

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

6.7.4 Health Check of DCA Systems

(A) The DCA shall ensure that, in relation to the DCA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

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

(B) The DCA shall ensure that the Device CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the DCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

The DCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

[*Not applicable in this Policy*]

7.2.2 CRL and CRL Entry Extensions

[*Not applicable in this Policy*]

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 Device Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of Device Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 Device Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Device Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Activation Data

means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.

Archive

means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).

Audit Log

means the audit log created in accordance with Part 5.4.1 of this Policy.

Authentication

means the process of establishing that an individual, organisation, System or Device is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).

Authorised Subscriber

means a Party which has successfully completed the procedures set out in the RAPP and has been authorised by the DCA to submit a Certificate Signing Request.

Certificate

means either a Device Certificate or a DCA Certificate.

Certificate Profile

means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.

Certificate Re-Key

means a change to the Public Key contained within a Certificate bearing a particular serial number.

Certificate Signing Request means a request for a Certificate submitted by an Eligible Subscriber in accordance with the RAPP.

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

DCA Personnel means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the DCA.

DCA Private Key means a DCA Key which is a Private Key.

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

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

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

Device Certification Authority (or **DCA**) means the DCC, acting in the capacity and exercising the functions of one or more of:

(a) the Root DCA;

(b) the Issuing DCA; and

(c) the Registration Authority.

Eligible Subscriber means:

(a) in relation to a Device Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.7 of the Code (Device Certificates); and

(b) in relation to a DCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.8 of the Code (DCA

Certificates).

Issue means the act of the DCA, in its capacity as the Root DCA or Issuing DCA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "**Issued**" and "**Issuing**" shall be interpreted accordingly).

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

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

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

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

Key Escrow means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.

Object Identifier (or **OID**) means an Object Identifier assigned by the Internet Address Naming Authority.

OCA has the meaning given to that expression in Appendix B of the Code (SMKI Organisation Certificate Policy).

OCA Systems has the meaning given to that expression in Appendix B of the Code (SMKI Organisation Certificate Policy).

Policy means this Device Certificate Policy.

Private Key Material in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.

Registration Authority means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the 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 RAPP.

Registration Authority Personnel means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.

Relying Party means a person who, pursuant to the Code, receives and relies upon a Certificate.

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

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

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

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

Subject means:

(a) in relation to a Device Certificate, the Device identified by the Device ID in the 'hwSerialNum' field of the Device Certificate Profile in Annex B; and

(b) in relation to a DCA Certificate, the Root DCA or Issuing DCA as identified in the 'Subject' field of the relevant Certificate Profile in Annex B.

Subscriber means, in relation to any Certificate, a Party which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

Time-Stamping means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the DCA that:

(a) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(b) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the DCA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the independent time source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: DCA Certificate and Device Certificate Profiles

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which DCA Certificates and Device Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5759 or IETF RFC5280.

Common requirements applicable to DCA Certificates and Device Certificates

All DCA Certificates and Device Certificates that are validly authorised within the SMKI for use within the scope of the GB Companion Specification and GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all DCA Certificates and Device Certificates shall:
  - contain the authorityKeyIdentifier extension, except where the Certificate is the Root DCA Certificate;
  - contain the keyUsage extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- only contain Public Keys of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
- contain a certificatePolicies extension containing at least one PolicyIdentifier which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Devices shall interpret this extension;
- contain a serialNumber of no more than 16 octets in length;
- contain a subjectKeyIdentifier which shall be marked as non-critical;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier which shall be marked as non-critical, except where the Certificate is the Root DCA Certificate. 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 and so which shall always be 8 octets in length;

- contain an IssuerName which MUST be identical to the signer's SubjectName
- have a valid notBefore field consisting of the time of issue encoded and a valid notAfter field for a not well-defined expiraton date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Device Certificates only

All Device Certificates that are issued by the DCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z;
- have an empty SubjectName;
- contain SubjectAlternativeName extension which contains a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-HardwareModuleName) as defined in RFC 4108. The hwSerialNum field shall be set to the Device’s Entity Identifier. In adherence to IETF RFC 5280, the SubjectAlternativeName shall be marked as critical;
- contain a single Public Key;
- contain a keyUsage extension marked as critical, with a value of only one of:
    - digitalSignature; or
    - keyAgreement.
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID applicable to the version of this Device Certificate Policy applicable at the time that the Device Certificate was issued.

Requirements applicable to the Root DCA and Issuing DCA

All DCA Certificates issued by the DCA shall:

- not have a well-defined expiration date and so the notAfter shall be assigned the GeneralizedTime value of 99991231235959Z;
- must have a Valid: notBefore field consisting of the time of issue encoded as per RFC5280;
- Per RFC5280, the IssuerName of any certificates MUST be identical to the signer’s SubjectName;
- have a globally unique SubjectName ;
- contain a single Public Key;
- contain a keyUsage extension marked as critical and defined as:

    - keyCertSign; and
    - cRLSign.
- For Issuing DCA Certificates contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID of the version of this Device Certificate Policy prevailing at the time.
- For the Root DCA Certificate contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for anyPolicy.
- For Issuing DCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical.
- For the Root DCA Certificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

Device Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 with ECDSA	
Issuer	Name	Globally unique name of Issuing DCA	
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	

		Device Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
Subject	Name	EMPTY	
subjectAltName	OtherName	contains a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-HardwareModuleName) as defined in RFC 4108. The hwSerialNum field shall be set to the Device's Entity Identifier	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Device Certificate signature	

Interpretation

Version

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

serialNumber

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

Signature

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

Issuer

The name of the signer of the Device Certificate. This will be the gloablly unique name of the Issuing DCA.

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 Device Certificates. The Device Certificate shall contain a authorityKeyIdentifier in the form [0] KeyIdentifier.

subjectKeyIdentifier

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

validity

The time period over which the Issuing DCA expects the Device Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Device Certificate may be used. This shall be the time the Device Certificate is created.

notAfter

The latest time a Device Certificate is expected to be used. Device Certificate are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Device Certificate are expected to accept this value indefinitely.

subject

This field must be EMPTY.

subjectAltName

The non-critical subjectAltName extension shall contain a single GeneralName of type OtherName that is further sub-typed as a HardwareModuleName (id-on-HardwareModuleName) as defined in RFC 4108. The hwSerialNum field shall be set to the Device ID.

subjectPublicKeyInfo

The Device Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-
62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Device Certificate extension (explained further under the next ‘**extensions**’ heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {

 namedCurve        OBJECT IDENTIFIER

 -- implicitCurve   NULL

 -- specifiedCurve  SpecifiedECDomain
```

}

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The namedCurve field in ECParameters uses object identifiers to name well-known curves.

The NIST recommended namedCurve is the P-256 curve. The object identifier for the curve choice to be used in Device Certificate is:

secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key. ECC Public Keys have the following syntax:

ECPoint ::= OCTET STRING

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The elliptic curve Public Key (a value of type ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

The first octet of the OCTET STRING indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

The signatureAlgorithm field shall indicate the Issuing DCA signature algorithm used to sign this Device Certificate is as defined under the next '**Signature Method (ECDSA)**' heading below.

signatureValue

The Issuing DCA's signature of the Device Certificate is computed using the Issuing DCA's private 256-bit ECC Device Certificate signing key using the algorithm identified under the next '**Signature Method (ECDSA)**' heading below.

When using the Elliptic Curve keys the Device Certificates shall be signed by the Issuing DCA using the ECDSA algorithm identified under the next '**Signature Method (ECDSA)**' heading below. The structure for ECDSA signatures is as per RFC 5480.

extensions

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

- certificatePolicy: critical; (applicable Device Certificate Policy OID).
- subjectAlternativeName: critical; one GeneralName of type OtherName of hardwareModuleName.
- keyUsage: critical; either keyAgreement or digitalSignature.
- authorityKeyIdentifier.
- subjectKeyIdentifier.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

> ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

SHA-256 hash algorithm

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

Root DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference

Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 with ECDSA	
Issuer	Name	Globally unique name of Root DCA	
subjectKeyIdentifier	KeyIdentifier	A unique value that matches the subjectKeyIdentifier of the issuer's credential	
notBefore	Time	Creation time of the Certificate	
notAfter	Time	shall be assigned the GeneralizedTime value of 99991231235959Z	
Subject	Name	Globally unique name of Root DCA (same as Issuer name)	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the Devices SMKI.

Version

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

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the DCA Certificate that signs the Certificate (self-signed by Root DCA). The serialNumber shall be unique in the scope of Certificates signed by the DCA Certificate.

Signature

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

Issuer

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

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

subjectKeyIdentifier

The Subject Key Identifier extension should 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 so which shall always be 8 octets in length.

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.

Root DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Root DCA certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

subject

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

subjectPublicKeyInfo

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall be use the following identifier:

id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next '**extensions**' heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {

  namedCurve       OBJECT IDENTIFIER

  -- implicitCurve   NULL

  -- specifiedCurve  SpecifiedECDomain

}
```

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular

set of elliptic curve domain parameters to be represented by an

object identifier.

The namedCurve field in ECParameters uses object identifiers to name well-known curves.

The NIST recommended namedCurve is the P-256 curve. The object identifier fo the curve choice to be used in DCA Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045)
curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key. ECC Public Keys have the following syntax:

```
ECPoint ::= OCTET STRING
```

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The elliptic curve Public Key (a value of type ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

The first octet of the OCTET STRING indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

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

signatureValue

The Root DCA's signature of the Certificate is computed using the Root DCA's private 256-bit ECC Device Certificate signing key using the algorithm identified under the next '**Signature Method (ECDSA)**' heading below.

When using the Elliptic Curve keys the Device Certificates shall be signed by the Issuing DCA using the ECDSA algorithm identified under the next '**Signature Method (ECDSA)**' heading below. The structure for ECDSA signatures is as per RFC 5480.

extensions

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

Extensions

- certificatePolicy: critical; 1:anyPolicy
- keyUsage: critical; keyCertSign, crlSign
- basicConstraints: critical; cA=true, pathLen absent (unlimited)
- subjectKeyIdentifer

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

> ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

SHA-256 hash algorithm

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

Issuing DCA Certificate Profile

Field Name	RFC 5759/5280 Type	Value	Reference

version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 with ECDSA	
Issuer	Name	Globally unique name of Root DCA	
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	shall be assigned the GeneralizedTime value of 99991231235959Z	
Subject	Name	Globally unique name of Issuing DCA	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject’s Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the Issuing DCA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root DCA.

Signature

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

issuer

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

subjectKeyIdentifier

The Subject Key Identifier extension should 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 so 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 device Certificates. The Certificates shall contain a authorityKeyIdentifier in the form [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.

Issuing DCA certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Issuing DCA certificate are expected to accept this value indefinitely.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time a Certificate may be used. This shall be the time the Certificate is created.

notAfter

The latest time a Certificate is expected to be used. Certificates are expected to operate indefinitely into the future and should use the value 99991231235959Z. Solutions verifying a Certificate are expected to accept this value indefinitely.

subject

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

subjectPublicKeyInfo

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall be use the following identifier:

```
id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-
62(10045) keyType(2) 1 }
```

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next '**extensions**' heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {

  namedCurve        OBJECT IDENTIFIER

  -- implicitCurve   NULL

  -- specifiedCurve  SpecifiedECDomain

}
```

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular

set of elliptic curve domain parameters to be represented by an

object identifier.

The namedCurve field in ECParameters uses object identifiers to name well-known curves.

The NIST recommended namedCurve is the P-256 curve. The object identifier fo the curve choice to be used in Certificates is:

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045)
curves(3) prime(1) 7 }
```

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key. ECC Public Keys have the following syntax:

```
ECPoint ::= OCTET STRING
```

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The elliptic curve Public Key (a value of type ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

The first octet of the OCTET STRING indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

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

signatureValue

The Root DCA's signature of the Certificate is computed using the Root DCA's private signing key using the algorithm identified under the next '**Signature Method (ECDSA)**' heading below.

When using the Elliptic Curve keys the Certificates shall be signed by the Root DCA using the ECDSA algorithm identified under the next '**Signature Method (ECDSA)**' heading below. The structure for ECDSA signatures is as per RFC 5480.

extensions

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

- certificatePolicy: critical; 1:at least one policyIdentifier in the certificatePolicies extension that refers to the OID(s) valid for usage in the GBSM environments
- keyUsage: critical; keyCertSign, crlSign
- basicConstraints: critical; cA=true, pathLen=0
- subjectKeyIdentifer
- authorityKeyIdentifier

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

> ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

SHA-256 hash algorithm

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

SCHEDULE 7

NEW APPENDIX B FOR INSERTION INTO SMART ENERGY CODE

"APPENDIX B – SMKI ORGANISATION CERTIFICATE POLICY

CONTENTS

Part **Heading** **Page**

1 INTRODUCTION

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

- shall be known as the "**SMKI Organisation Certificate Policy**" (and in this document is referred to simply as the "**Policy**"),
- is a SEC Subsidiary Document related to Section L9 of the Code (The SMKI Document Set).

1.1 OVERVIEW

(B) This Policy sets out the arrangements relating to:

(i) Organisation Certificates; and

(ii) OCA Certificates.

(C) This Policy is structured according to the guidelines provided by IETF RFC 3647, with appropriate extensions, modifications and deletions.

1.2 DOCUMENT NAME AND IDENTIFICATION

(A) This Policy has been registered with the Internet Address Naming Authority and assigned an OID of 1.2.826.0.1. 8641679.1.2.1.1.

1.3 SMKI PARTICIPANTS

1.3.1 The Organisation Certification Authority

(A) The definition of Organisation Certification Authority is set out in Annex A.

1.3.2 Registration Authorities

(A) The definition of Registration Authority is set out in Annex A.

1.3.3 Subscribers

(A) In accordance with Section L3 of the Code (The SMKI Services), certain Parties may become Authorised Subscribers.

(B) In accordance with Section L3 of the Code (The SMKI Services), an Authorised Subscriber shall be an Eligible Subscriber in relation to certain Certificates.

(C) The 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 RAPP and Section L11 of the Code (Subscriber Obligations).

(E) Obligations on the DCC acting in the capacity of an Eligible Subscriber are set out in Section L11 of the Code (Subscriber Obligations).

(F) The definitions of the following terms are set out in Section A of the Code (Definitions and Interpretation):

(i) Authorised Subscriber;

(ii) Eligible Subscriber;

(iii) Subscriber.

1.3.4 Subjects

(A) The Subject of an Organisation Certificate must be an Organisation and be identified in the 'Subject' field of the Organisation Certificate Profile in accordance with Annex B.

(B) The Subject of an OCA Certificate must be the entity named in the Subject field of the Root OCA Certificate Profile or Issuing OCA Certificate Profile (as the case may be) in accordance with Annex B.

(C) The definition of Subject is set out in Annex A.

1.3.5 Relying Parties

(A) In accordance with Section L12 of the Code, certain Parties may be Relying Parties.

(B) Relying Parties are subject to the applicable requirements of Section L12 of the Code (Relying Party Obligations).

(C) Obligations on the DCC acting in the capacity of a Relying Party are set out in Section L12 of the Code (Relying Party Obligations).

(D) The definition of Relying Party is set out in Annex A.

1.3.6 SMKI Policy Management Authority

(A) Provision in relation to the SMKI PMA is made in Section L1 of the Code (SMKI

Policy Management Authority).

1.3.7 SMKI Repository Provider

(A) Provision in relation to the SMKI Repository Service is made in Section L5 of the Code (The SMKI Repository Service).

1.4 USAGE OF ORGANISATION CERTIFICATES AND OCA CERTIFICATES

1.4.1 Appropriate Certificate Uses

(A) The OCA shall ensure that Organisation Certificates are Issued only:

(i) to Eligible Subscribers; and

(ii) for the purposes of the creation, sending, receipt and processing of communications to and from Organisations in accordance with or pursuant to the Code.

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

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

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

(C) Further provision in relation to the use of Certificates is made in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code.

1.4.2 Prohibited Certificate Uses

(A) No Party shall use a Certificate other than for the purposes specified in Part 1.4.1 of this Policy.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

(A) This Policy is a SEC Subsidiary Document and is administered as such in accordance with the provisions of the Code.

1.5.2 Contact Person

(A) Questions in relation to the content of this Policy should be addressed to the OCA or the SMKI PMA.

1.5.3 Person Determining Organisation CPS Suitability for the Policy

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the SMKI PMA to approve the Organisation CPS.

1.5.4 Organisation CPS Approval Procedures

(A) Provision is made in Section L9 of the Code (The SMKI Document Set) for the procedure by which the SMKI PMA may approve the Organisation CPS.

1.5.5 Registration Authority Policies and Procedures

(A) The Registration Authority Policies and Procedures (the **RAPP**) are set out at Appendix D of the Code.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

(A) Definitions of the expressions used in this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

1.6.2 Acronyms

(A) Any acronyms used for the purposes of this Policy are set out in Section A of the Code (Definitions and Interpretation) and Annex A.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

(A) Provision is made in Section L5 of the Code (The SMKI Repository Service) for the establishment, operation and maintenance of the SMKI Repository.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

(A) The OCA shall lodge the following in the SMKI Repository:

(i) each Organisation Certificate that has been accepted by a Subscriber;

(ii) each OCA Certificate;

(iii) each version of the RAPP;

(iv) each version of the Recovery Procedure;

(v) each version of the CRL;

(vi) each version of the ARL; and

(vii) any other document or information that may from time to time be specified, for the purposes of this provision, by the SMKI PMA.

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

(C) Further provision on the lodging of documents and information in the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

2.3 TIME OR FREQUENCY OF PUBLICATION

(A) The OCA shall ensure that:

(i) each Organisation Certificate is lodged in the SMKI Repository promptly on its acceptance by a Subscriber;

(ii) each OCA Certificate is lodged to the SMKI Repository promptly on being Issued;

(iii) the RAPP is lodged in the SMKI Repository, and a revised version of the RAPP is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(iv) the Recovery Procedure is lodged in the SMKI Repository, and a revised version of Recovery Procedure is lodged in the SMKI Repository promptly following each modification to it made in accordance with the Code;

(v) the CRL is lodged in the SMKI Repository, and a revised version of the CRL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy;

(vi) the ARL is lodged in the SMKI Repository, and a revised version of the ARL is lodged in the SMKI Repository within such time as is specified in Part 4.9.7 of this Policy; and

(vii) any other document that may from time to time be specified by the SMKI PMA is lodged in the SMKI Repository within such time as may be directed by the SMKI PMA.

2.4 ACCESS CONTROLS ON REPOSITORIES

(A) Provision in relation to access controls for the SMKI Repository is made in Section L5 of the Code (The SMKI Repository Service).

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

(A) Provision is made in the RAPP to ensure that the name of the entity that is the Subject of each Certificate is in accordance with the relevant Certificate Profile at Annex B.

3.1.2 Need for Names to be Meaningful

(A) Provision is made in the RAPP to ensure that the name of the Subject of each OCA Certificate is meaningful and consistent with the relevant Certificate Profile in Annex B.

3.1.3 Anonymity or Pseudonymity of Subscribers

(A) Provision is made in the RAPP to:

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

(ii) permit the OCA to Authenticate each Eligible Subscriber.

3.1.4 Rules for Interpreting Various Name Forms

(A) Provision in relation to name forms is made in Annex B.

3.1.5 Uniqueness of Names

(A) Provision in relation to the uniqueness of names is made in Annex B.

3.1.6 Recognition, Authentication, and Role of Trademarks

(A) Provision in relation to the use of trademarks, trade names and other restricted information in Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

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

(i) the procedure to be followed by an Eligible Subscriber in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any Certificate that is the subject of a Certificate Signing Request; and

(ii) the procedure established for this purpose is in accordance with the procedure in PKCS#10 or an equivalent cryptographic mechanism.

3.2.2 Authentication of Organisation Identity

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

(i) procedure to be followed by a Party in order to become an Authorised Subscriber;

(ii) criteria in accordance with which the OCA will determine whether a Party is entitled to become an Authorised Subscriber; and

(iii) requirement that the Party shall be Authenticated by the OCA for that purpose.

(B) Provision is made in the RAPP to ensure that each Eligible Subscriber has an Organisation ID that is EUI-64 Compliant in respect of which the Organisation Unique Identifier is that of the Subject.

(C) Provision is made in the RAPP for the purpose of ensuring that the criteria in accordance with which the OCA shall Authenticate a Party shall be set to Level 3 pursuant to GPG 46 (Organisation Identity, v1.0, October 2013), or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.3 Authentication of Individual Identity

(A) Provision is made in the RAPP in relation to the Authentication of persons engaged by Authorised Subscribers, which provides for all such persons to have their identity and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

3.2.4 Non-verified Subscriber Information

(A) The OCA shall verify all information in relation to Certificates.

(B) Further provision on the content of OCA Certificates is made in Section L11 of the Code (Subscriber Obligations).

3.2.5 Validation of Authority

See Part 3.2.2 of this Policy.

3.2.6 Criteria for Interoperation

[*Not applicable in this Policy*]

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The OCA shall not provide a Certificate Re-Key service.

3.3.2 Identification and Authentication for Re-Key after Revocation

[*Not applicable in this Policy*]

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 Authentication for Certificate Revocation Requests

(A) Provision is made in the RAPP in relation to procedures designed to ensure the Authentication of persons who submit a Certificate Revocation Request and verify that they are authorised to submit that request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Submission of Certificate Applications

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

(i) in respect of an Organisation Certificate:

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

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

(ii) in respect of an OCA Certificate, the procedure to be followed by an Eligible Subscriber in order to obtain an OCA Certificate.

4.1.2 Enrolment Process and Responsibilities

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

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

(ii) maintenance by the OCA of a list of organisations, individuals, Systems and Devices enrolled in accordance with that process.

4.1.3 Enrolment Process for the Registration Authority and its Representatives

(A) Provision is made in the RAPP in relation to the establishment of an enrolment process in respect of OCA Personnel and OCA Systems:

(i) in order to Authenticate them and verify that they are authorised to act on behalf of the OCA in its capacity as the Registration Authority; and

(ii) including in particular, for that purpose, provision:

(a) for the face-to-face Authentication of all Registration Authority Personnel by a Registration Authority Manager; and

(b) for all Registration Authority Personnel to have their identify and authorisation verified to Level 3 (Verified) pursuant to the CESG GPG43 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

(A) Provision is made in the RAPP in relation to the Authentication by the OCA of Eligible Subscribers which submit a Certificate Signing Request.

4.2.2 Approval or Rejection of Certificate Applications

(A) Where any Certificate Signing Request fails to satisfy the requirements set out in the RAPP, this Policy or any other provision of the Code, the OCA:

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

(ii) may give notice to the Party 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 RAPP, this Policy or any other provision of the Code, the OCA shall Issue the Certificate which was the subject of the Certificate Signing Request.

4.2.3 Time to Process Certificate Applications

(A) Provision in relation to the performance of the SMKI Services by the OCA is made in Section L8 of the Code (SMKI Performance Standards and Demand Management).

4.3 CERTIFICATE ISSUANCE

4.3.1 OCA Actions during Certificate Issuance

(A) The OCA may Issue a Certificate only:

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

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

(B) The OCA shall ensure that:

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

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

(C) An OCA Certificate may only be:

(i) Issued by the OCA; and

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

(D) An Organisation Certificate may only be:

(i) Issued by the OCA; and

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

(E) The OCA shall not Issue:

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

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

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

(A) Provision is made in the RAPP for the OCA to notify an Eligible Subscriber where that Eligible Subscriber is Issued with a Certificate which was the subject of a Certificate Signing Request made by it.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

(A) Provision is made in the RAPP to:

(i) specify a means by which an Eligible Subscriber may clearly indicate to the OCA its acceptance of a Certificate which has been Issued to it; and

(ii) ensure that each Eligible Subscriber to which a Certificate has been Issued indicates its acceptance of that Certificate in accordance with the specified means of doing so.

(B) A Certificate which has been Issued by the OCA shall not be treated as valid for any purposes of this Policy or the Code until it is accepted by the Eligible Subscriber to which it was Issued.

(C) The OCA shall maintain a record of all Certificates which have been Issued by it and accepted by a Subscriber.

(D) Further provision in relation to the acceptance of Certificates is made in Section L11 of the Code (Subscriber Obligations).

4.4.2 Publication of Certificates by the OCA

(A) Provision in relation to the publication of Certificates is made in Part 2 of this Policy (Publication and Repository Responsibilities) and Section L5 of the Code (The SMKI Repository Service).

4.4.3 Notification of Certificate Issuance by the OCA to Other Entities

(A) The OCA shall give notice of the Issue of a Certificate only to the Eligible Subscriber which submitted a Certificate Signing Request in respect of that Certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

(A) Provision for restrictions on the use by Subscribers of Private Keys in respect of Certificates is made in:

(i) Section L11 of the Code (Subscriber Obligations); and

(ii) this Policy.

4.5.2 Relying Party Public Key and Certificate Usage

(A) Provision in relation to reliance that may be placed on a Certificate is made in

Section L12 of the Code (Relying Party Obligations).

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstances of Certificate Renewal

(A) This Policy does not support the renewal of Certificates

(B) The OCA may only replace, and shall not renew, any Certificate.

4.6.2 Circumstances of Certificate Replacement

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

(i) immediately notify the SMKI PMA;

(ii) provide the SMKI PMA with all of the information known to it in relation to the nature and circumstances of the event of Compromise or suspected Compromise; and

(iii) where the Compromise or suspected Compromise relates to an OCA Private Key:

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

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

(c) promptly both notify the SMKI PMA and, subject to the provisions of the Recovery Procedure, verifiably destroy the OCA Private Key Material.

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

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

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

(C) A Subscriber for an Organisation Certificate may request a replacement for that

Certificate at any time by applying for the Issue of a new Organisation Certificate in accordance with this Policy.

4.6.3 Who May Request a Replacement Certificate

See Part 4.1 of this Policy.

4.6.4 Processing Replacement Certificate Requests

See Part 4.2 of this Policy

4.6.5 Notification of Replacement Certificate Issuance to a Subscriber

See Part 4.3.2 of this Policy.

4.6.6 Conduct Constituting Acceptance of a Replacement Certificate

See Part 4.4.1 of this Policy.

4.6.7 Publication of a Replacement Certificate by the OCA

See Part 4.4.2 of this Policy.

4.6.8 Notification of Certificate Issuance by the OCA to Other Entities

See Part 4.4.3 of this Policy

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstances for Certificate Re-Key

(A) This Policy does not support Certificate Re-Key.

(B) The OCA shall not provide a Certificate Re-Key service.

(C) Where a new Key Pair has been generated for use by the Subject of an Organisation Certificate, the Subscriber for a Certificate which is associated with the previous Key Pair shall apply for the Issue of a new Certificate in accordance with this Policy.

4.7.2 Who may Request Certification of a New Public Key

[*Not applicable in this Policy*]

4.7.3 Processing Certificate Re-Keying Requests

[*Not applicable in this Policy*]

4.7.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

[*Not applicable in this Policy*]

4.7.6 Publication of the Re-Keyed Certificate by the OCA

[*Not applicable in this Policy*]

4.7.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstances for Certificate Modification

(A) This Policy does not support Certificate modification.

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

4.8.2 Who may request Certificate Modification

[*Not applicable in this Policy*]

4.8.3 Processing Certificate Modification Requests

[*Not applicable in this Policy*]

4.8.4 Notification of New Certificate Issuance to Subscriber

[*Not applicable in this Policy*]

4.8.5 Conduct Constituting Acceptance of Modified Certificate

[*Not applicable in this Policy*]

4.8.6 Publication of the Modified Certificate by the OCA

[*Not applicable in this Policy*]

4.8.7 Notification of Certificate Issuance by the OCA to Other Entities

[*Not applicable in this Policy*]

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

(A) A Subscriber shall ensure that it submits a Certificate Revocation Request in relation to a Certificate:

(i) (subject to the provisions of the Recovery Procedure) immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; or

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

(B) The OCA must revoke a Certificate upon:

(i) receiving a Certificate Revocation Request if the Certificate to which that request relates has been Authenticated in accordance with Part 3.4.1 of this Policy; or

(ii) being directed to do so by the SMKI PMA.

(C) The OCA must revoke a Certificate in relation to which it has not received a Certificate Revocation Request:

(i) (subject to the provisions of the Recovery Procedure) where it becomes aware that the Certificate has been Compromised, or is suspected of having been Compromised, due to the Compromise of the Private Key associated with the Public Key contained within that Certificate; 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 OCA may, on the receipt of a Certificate Revocation Request in relation to a Certificate which has not been Authenticated in accordance with Part 3.4.1 of this Policy, revoke that Certificate.

(E) Where the OCA revokes a Certificate in accordance with paragraph (D) it shall notify the SMKI PMA and provide a statement of its reasons for the revocation.

4.9.2 Who can Request Revocation

(A) Any Subscriber may submit a Certificate Revocation Request in relation to a Certificate for which it is the Subscriber, and shall on doing so:

(i) provide all the information specified in the RAPP (including all the information necessary for the Authentication of the Certificate); and

(ii) specify its reason for submitting the Certificate Revocation Request (which shall be a reason consistent with Part 4.9.1(A) of this Policy).

(B) The SMKI PMA may direct the OCA to revoke a Certificate.

(C) The OCA may elect to revoke a Certificate in accordance with Part 4.9.1(D) of this Policy.

4.9.3 Procedure for Revocation Request

(A) Provision is made in the RAPP in relation to the procedure for submitting and processing a Certificate Revocation Request.

(B) On receiving a Certificate Revocation Request, the OCA shall use its reasonable endeavours to:

(i) Authenticate the Subscriber making that request;

(ii) Authenticate the Certificate to which the request relates; and

(iii) confirm that a reason for the request has been specified in accordance with Part 4.9.2 of this Policy.

(C) Where the OCA, in accordance with Part 4.9.1(C) of this Policy, intends to revoke a Certificate in relation to which it has not received a Certificate Revocation Request, it shall use its best endeavours prior to revocation to confirm with the Subscriber for that Certificate the circumstances giving rise to the revocation.

(D) The OCA shall inform the Subscriber for a Certificate where that Certificate has been revoked.

4.9.4 Revocation Request Grace Period

[*Not applicable in this Policy*]

4.9.5 Time within which OCA must process the Revocation Request

(A) The OCA shall ensure that it processes all Certificate Revocation Requests promptly, and in any event in accordance with such time as is specified in the RAPP.

4.9.6 Revocation Checking Requirements for Relying Parties

(A) Provision in relation to the revocation checking requirements for Relying Parties is made in Section L12 of the Code (Relying Party Obligations).

4.9.7 CRL Issuance Frequency (if applicable)

(A) The OCA shall ensure that an up to date version of the ARL is lodged in the SMKI Repository:

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

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

(B) Each version of the ARL shall be valid until the date which is 12 months after the date on which that version of the ARL is lodged in the SMKI Repository.

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

(D) The OCA shall ensure that an up to date version of the CRL is lodged in the SMKI Repository:

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

(ii) within one hour on the revocation of an Organisation Certificate.

(E) Each version of the CRL shall be valid until 48 hours from the time at which it is lodged in the SMKI Repository.

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

(G) The OCA shall ensure that each up to date version of the ARL and CRL:

(i) continues to include each relevant revoked Certificate until such time as the Validity Period of that Certificate has expired; and

(ii) does not include any revoked Certificate after the Validity Period of that Certificate has expired.

(H) The OCA shall ensure that the 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).

4.9.8 Maximum Latency for CRLs (if applicable)

See Part 4.9.7 of this Policy.

4.9.9 On-line Revocation/Status Checking Availability

(A) This Policy does not support on-line revocation status checking.

(B) The OCA shall not provide any on-line revocation status checking service.

4.9.10 On-line Revocation Checking Requirements

[*Not applicable in this Policy*]

4.9.11 Other Forms of Revocation Advertisements Available

[*Not applicable in this Policy*]

4.9.12 Special Requirements in the Event of Key Compromise

See Part 4.6.2 of this Policy.

4.9.13 Circumstances for Suspension

[*Not applicable in this Policy*]

4.9.14 Who can Request Suspension

[*Not applicable in this Policy*]

4.9.15 Procedure for Suspension Request

[*Not applicable in this Policy*]

4.9.16 Limits on Suspension Period

[*Not applicable in this Policy*]

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

[*Not applicable in this Policy*]

4.10.2 Service Availability

(A) In circumstances in which:

(i) an up to date version of the ARL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(A) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the 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 CRL has not been lodged in the SMKI Repository in accordance with Part 4.9.7(C) of this Policy; or

(ii) the SMKI Repository Service is unavailable,

a Relying Party shall be entitled to rely on the CRL for the period during which it remains valid in accordance with the provisions of Part 4.9.7(D) of this Policy, but thereafter shall not rely on any Organisation Certificate.

4.10.3 Optional Features

[*Not applicable in this Policy*]

4.11 END OF SUBSCRIPTION

[*Not applicable in this Policy*]

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policies and Practices

(A) This Policy does not support Key Escrow.

(B) The OCA shall not provide any Key Escrow service.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

[*Not applicable in this Policy*]

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

(A) The OCA shall ensure that the OCA Systems are operated in a sufficiently secure environment, which shall at least satisfy the requirements set out at Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

(B) The OCA shall ensure that:

(i) all of the physical locations in which the OCA Systems are situated, operated, routed or directly accessed are in the United Kingdom;

(ii) all bespoke Security Related Functionality is developed, specified, designed, built and tested only within the United Kingdom; and

(iii) all Security Related Functionality is integrated, configured, tested in situ, implemented, operated and maintained only within the United Kingdom.

(C) The OCA shall ensure that the OCA Systems cannot be indirectly accessed from any location outside the United Kingdom.

(D) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that all physical locations in which the manufacture of Certificates and Time-Stamping take place are at all times manually or electronically monitored for unauthorised intrusion in accordance with:

(i) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(ii) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time.

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

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

5.1.2 Physical Access

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access control, including in particular provisions designed to:

(i) establish controls such that only appropriately authorised personnel may have unescorted physical access to OCA Systems or any System used for the purposes of Time-Stamping;

(ii) ensure that any unauthorised personnel may have physical access to such Systems only if appropriately authorised and supervised;

(iii) ensure that a site access log is both maintained and periodically inspected for all locations at which such Systems are sited; and

(iv) ensure that all removable media which contain sensitive plain text Data and are kept at such locations are stored in secure containers accessible only to appropriately authorised individuals.

5.1.3 Power and Air Conditioning

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

5.1.4 Water Exposure

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions as the OCA.

5.1.7 Waste Disposal

(A) The OCA shall ensure that all media used to store Data held by it for the purposes of carrying out its functions as the OCA are disposed of only using secure methods of disposal in accordance with:

(i) Information Assurance Standard No. 5:2011 (Secure Sanitisation); or

(ii) any equivalent to that Information Assurance Standard which updates or replaces it from time to time.

5.1.8 Off-Site Back-Up

(A) The OCA shall regularly carry out a Back-Up of:

(i) all Data held on the OCA Systems which are critical to the operation of those Systems or continuity in the provision of the SMKI Services; and

(ii) all other sensitive Data.

(B) For the purposes of paragraph (A), the OCA shall ensure that the Organisation CPS incorporates provisions which identify the categories of critical and sensitive Data that are to be Backed-Up.

(C) The OCA shall ensure that Data which are Backed-Up in accordance with paragraph (A):

(i) are stored on media that are located in physically secure facilities in different locations to the sites at which the Data being Backed-Up are ordinarily held;

(ii) are protected in accordance with the outcome of a risk assessment which is documented in the Organisation CPS, including when being transmitted for the purposes of Back-Up; and

(iii) to the extent to which they comprise OCA Private Key Material, are Backed-Up:

(a) using the proprietary Back-Up mechanisms specific to the relevant Cryptographic Module; and

(b) in a manner that is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The OCA shall ensure that, where any elements of the OCA Systems, any Data held for the purposes of providing the SMKI Services, or any items of OCA equipment are removed from their primary location, they continue to be protected in accordance with the security standard appropriate to the primary location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

(A) The OCA shall ensure that:

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

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

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

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

5.2.2 Number of Persons Required per Task

(A) The OCA shall ensure that the Organisation CPS incorporates provisions designed to establish:

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

(ii) the application of controls to the actions of all members of OCA Personnel who are Privileged Persons, in particular:

(a) identifying any controls designed to ensure that the involvement of more than one individual is required for the performance of certain functions; and

(b) providing that the revocation of any OCA Certificate is one such function.

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

(i) OCA Systems administration;

(ii) OCA Systems operations;

(iii) OCA Systems security; and

(iv) OCA Systems auditing.

5.2.3 Identification and Authentication for Each Role

See Part 5.2.2 of this Policy.

5.2.4 Roles Requiring Separation of Duties

See Part 5.2.2 of this Policy.

5.3 PERSONNEL CONTROLS

5.3.1 Qualification, Experience and Clearance Requirements

(A) The OCA shall ensure that all OCA Personnel must:

(i) be appointed to their roles in writing;

(ii) be bound by contract to the terms and conditions relevant to their roles;

(iii) have received appropriate training with respect to their duties;

(iv) be bound by contract not to disclose any confidential, sensitive, personal or security-related Data except to the extent necessary for the performance of their duties or for the purposes of complying with any requirement of law; and

(v) in so far as can reasonably be ascertained by the OCA, not have been previously relieved of any past assignment (whether for the OCA or any other person) on the grounds of negligence or any other failure to perform a duty.

(B) The OCA shall ensure that all OCA Personnel have, as a minimum, passed a

Security Check before commencing their roles.

5.3.2 Background Check Procedures

See Part 5.3.1 of this Policy.

5.3.3 Training Requirements

See Part 5.3.1 of this Policy.

5.3.4 Retraining Frequency and Requirements

(A) The OCA shall ensure that the Organisation CPS incorporates appropriate provisions relating to the frequency and content of retraining and refresher training to be undertaken by members of OCA Personnel.

5.3.5 Job Rotation Frequency and Sequence

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

5.3.6 Sanctions for Unauthorised Actions

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

5.3.7 Independent Contractor Requirements

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

5.3.8 Documentation Supplied to Personnel

(A) The OCA shall ensure that all OCA Personnel are provided with access to all documents relevant to their roles or necessary for the performance of their duties, including in particular:

(i) this Policy;

(ii) the Organisation CPS; and

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

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

(A) The OCA shall ensure that:

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

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

(a) the activities of OCA Personnel;

(b) the use of OCA equipment;

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

(d) communications and activities that are related to the Issue of Certificates (in so far as not captured by the OCA Systems audit log); and

(iii) it records in an audit log all the events specified in paragraph (ii).

5.4.2 Frequency of Processing Log

(A) The OCA shall ensure that:

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

(ii) all OCA Systems activity recorded in the Audit Log is recorded in a standard format that is compliant with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(iii) it monitors the OCA Systems in compliance with:

(a) CESG Good Practice Guide 13:2012 (Protective Monitoring); or

(b) any equivalent to that CESG Good Practice Guide which updates or replaces it from time to time;

(B) The OCA shall ensure that the Organisation CPS incorporates provisions which specify:

(i) how regularly information recorded in the Audit Log is to be reviewed; and

(ii) what actions are to be taken by it in response to types of events recorded in the Audit Log.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to access to the Audit Log, providing in particular that:

(i) Data contained in the Audit Log must not be accessible other than on a read-only basis; and

(ii) access to those Data must be limited to those members of OCA Personnel who are performing a dedicated system audit role.

5.4.3 Retention Period for Audit Log

(A) The OCA shall:

(i) retain the Audit Log so that it incorporates, on any given date, a record of all system events occurring during a period of at least twelve months prior to that date; and

(ii) ensure that a copy of the Audit Log incorporating a record of all system events occurring prior to the beginning of that period is archived in accordance with the requirements of Part 5.5 of this Policy.

5.4.4 Protection of Audit Log

(A) The OCA shall ensure that:

(i) to the extent to which the Audit Log is retained electronically, the Data stored in it cannot be accessed other than on a read-only basis, and are protected from unauthorised viewing, modification and deletion in accordance with:

(a) British Standard BS 10008:2008 (Evidential Weight and Legal

Admissibility of Electronic Information); or

(b) any equivalent to that British Standard which updates or replaces it from time to time; and

(ii) to the extent to which the Audit Log is retained in non-electronic form, the Data stored in it are appropriately protected from unauthorised viewing, modification and destruction in order to ensure that their integrity is maintained for evidential purposes.

5.4.5 Audit Log Back-Up Procedures

(A) The OCA shall ensure that the Data contained in the Audit Log are Backed-Up (or, to the extent that the Audit Log is retained in non-electronic form, are copied):

(i) on a daily basis; or

(ii) if activity has taken place on the OCA Systems only infrequently, in accordance with the schedule for the regular Back-Up of the Data held on those Systems.

(B) The OCA shall ensure that all Data contained in the Audit Log which are Backed-Up are, during Back-Up:

(i) held in accordance with the outcome of a risk assessment which is documented in the Organisation CPS; and

(ii) protected to the same standard of protection as the primary copy of the Audit Log in accordance with Part 5.4.4 of this Policy.

5.4.6 Audit Collection System (Internal or External)

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Audit Log.

5.4.7 Notification to Event-Causing Subject

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its notification of any person who is (or is responsible for any System which is) the direct cause of an event recorded in the Audit Log.

5.4.8 Vulnerability Assessments

(A) Provision is made in Sections G2.13 to G2.14 of the Code (Management of Vulnerabilities) in relation to the carrying out of vulnerability assessments in respect of the OCA Systems.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

(A) The OCA shall ensure that it archives:

(i) the Audit Log in accordance with Part 5.4.3 of this Policy;

(ii) its records of all Data submitted to it by Eligible Subscribers for the purposes of Certificate Signing Requests; and

(iii) any other Data specified in this Policy or the Code as requiring to be archived in accordance with this Part 5.5.

5.5.2 Retention Period for Archive

(A) The OCA shall ensure that all Data which are Archived are retained for a period of at least seven years from the date on which they were Archived.

5.5.3 Protection of Archive

(A) The OCA shall ensure that Data held in its Archive are:

(i) protected against any unauthorised access;

(ii) adequately protected against environmental threats such as temperature, humidity and magnetism; and

(iii) incapable of being modified or deleted.

5.5.4 Archive Back-Up Procedures

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its procedures for the Back-Up of its Archive.

5.5.5 Requirements for Time-Stamping of Records

(A) Provision in relation to Time-Stamping is made in Part 6.8 of this Policy.

5.5.6 Archive Collection System (Internal or External)

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to its system for collecting Data for the purpose of populating the Archive.

5.5.7 Procedures to Obtain and Verify Archive Information

(A) The OCA shall ensure that:

(i) Data held in the Archive are stored in a readable format during their retention period; and

(ii) those Data remains accessible at all times during their retention period, including during any period of interruption, suspension or cessation of the OCA's operations.

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

5.6 KEY CHANGEOVER

5.6.1 Organisation Certificate Key Changeover

(A) The OCA shall Issue a new Organisation Certificate in relation to an Organisation where a new Certificate Signing Request is submitted by an Eligible Subscriber in accordance with the requirements of the RAPP and this Policy.

5.6.2 OCA Key Changeover

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

(i) either:

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

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

(ii) not revoke the related OCA Public Key (which may continue to be used for the purpose of validating Digital Signatures generated using the OCA Private Key);

(iii) generate a new Key Pair;

(iv) ensure that any relevant Certificate subsequently Issued by it is Issued using the OCA Private Key from the newly-generated Key Pair:

(a) until the time determined in accordance with Part 4.3.1(E) of this Policy; and

(b) subject to the provisions of Part 5.7.1(C) of this Policy; and

(v) in its capacity as the Root OCA:

(a) Issue a new relevant OCA Certificate; and

(b) promptly lodge that OCA Certificate in the SMKI Repository.

(B) The OCA shall ensure that the actions taken by it in accordance with the requirements of paragraph (A) are managed so as to prevent any disruption to the provision of the SMKI Services.

5.6.3 Subscriber Key Changeover

(A) Where:

(i) a Certificate has been revoked in accordance with Part 4.9 of this Policy; and

(ii) the Subscriber for that Certificate submits to the OCA a Certificate Signing Request for the Issue of a replacement Certificate,

the OCA shall verify that the reasons for the revocation and replacement of the previous Certificate have been satisfactorily addressed, and may Issue a Certificate in accordance with the Certificate Signing Request only after it has done so.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

(A) The OCA shall ensure that the Organisation CPS incorporates a business continuity plan which shall be designed to ensure:

(i) continuity in, or (where there has been unavoidable discontinuity) the recovery of, the provision of the SMKI Services in the event of any Compromise of the OCA Systems or major failure in the OCA processes; and

(ii) that priority is given to maintain continuity in, or to recovering the capacity for, the revocation of Certificates and the making available of an up to date ARL and CRL.

(B) The OCA shall ensure that the procedures set out in the business continuity plan are:

(i) compliant with ISO 22301 and ISO 27031 (or any equivalent to those standards which update or replace them from time to time); and

(ii) tested periodically, and in any event at least once in each year, in order to ensure that they are operationally effective.

(C) The OCA shall ensure that the Organisation CPS incorporates provisions setting out the approach to be taken by it in circumstances in which it suspects (or has reason to suspect) that any OCA Private Key or any part of the OCA Systems is Compromised.

5.7.2 Computing Resources, Software and/or Data are Corrupted

(A) The OCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy incorporates provisions setting out the steps to be taken in the event of any loss of or corruption to computing resources, software or Data.

5.7.3 Entity Private Key Compromise Procedures

See Part 5.7.1 of this Policy.

5.7.4 Business Continuity Capabilities after a Disaster

(A) The OCA shall ensure that the business continuity plan established in accordance with Part 5.7.1 of this Policy is designed to ensure the recovery of the provision of the SMKI Services within not more than 12 hours of the occurrence of any event causing discontinuity.

5.8 CERTIFICATION AUTHORITY AND REGISTRATION AUTHORITY TERMINATION

[*Not applicable in this Policy*]

6 TECHNICAL SECURITY CONTROLS

The OCA shall ensure that the Organisation CPS incorporates detailed provision in relation to the technical controls to be established and operated for the purposes of the exercise of its functions as the Root OCA, the Issuing OCA and the Registration Authority.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(A) The OCA shall ensure that all OCA 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 OCA 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 OCA shall not generate any Private Key or Public Key other than an OCA Key.

6.1.2 Private Key Delivery to Subscriber

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

6.1.3 Public Key Delivery to Certificate Issuer

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

(i) in relation to the mechanism by which Public Keys of Subscribers are delivered to it for the purpose of the exercise of its functions as the Root OCA and Issuing OCA; and

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

6.1.4 OCA Public Key Delivery to Relying Parties

(A) The OCA shall ensure that the Organisation CPS incorporates provisions:

(i) in relation to the manner by which each OCA Public Key is to be lodged in the SMKI Repository; and

(ii) designed to ensure that the OCA Public Keys are securely lodged in the SMKI Repository in such a manner as to guarantee that their integrity is maintained.

6.1.5 Key Sizes

(A) The OCA and every Subscriber shall ensure that all Private Keys and Public Keys which each of them may use for the purposes of this Policy are of the following size and characteristics:

(i) Elliptic Curve on the NIST P-256 curve in its uncompressed form, as defined in RFC5480 and as further set out in the GB Companion Specification; and

(ii) Digital Signature verification with Elliptic Curve Digital Signature Authentication using SHA256 and as further set out in the GB Companion Specification.

6.1.6 Public Key Parameters Generation and Quality Checking

(A) The OCA shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

(B) Each Subscriber shall ensure that any Public Key used by it for the purposes of this Policy shall be of values and lengths that make the success of known attacks infeasible.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

(A) The OCA shall ensure that each Certificate that is Issued by it has a 'keyUsage' field in accordance with RFC5759 and RFC5280.

(B) The OCA shall ensure that each Organisation Certificate that is Issued by it has a 'keyUsage' of either:

(i) 'digitalSignature'; or

(ii) 'keyAgreement'.

(C) The OCA shall ensure that each OCA Certificate that is Issued by it has a ‘keyUsage’ of either:

(i) ‘keyCertSign’; or

(ii) ‘CRLSign’.

(D) The OCA shall ensure that no ‘keyUsage’ values may be set in an Organisation Certificate or OCA Certificate other than in accordance with this Part 6.1.7.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

(A) The OCA shall ensure that all OCA Private Keys shall be:

(i) protected to a high standard of assurance by physical and logical security controls; and

(ii) stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(B) The OCA shall ensure that all OCA Private Keys shall, where they affect the outcome of any Certificates Issued by it, be protected by, stored in and operated from within a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(C) The OCA shall ensure that no OCA Private Key shall be made available in either complete or unencrypted form except in a Cryptographic Module which is compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(D) The OCA shall ensure that any Cryptographic Module which is used for any purpose related to Certificate life-cycle management shall:

(i) operate so as to block access to itself following a number of failed consecutive attempts to access it using Activation Data, where that number shall be set out in the Organisation CPS; and

(ii) require to be unblocked by an authorised member of OCA Personnel who has been Authenticated as such following a process which shall be set out in the Organisation CPS.

6.2.2 Private Key (m out of n) Multi-Person Control

See Part 6.1.1 of this Policy.

6.2.3 Private Key Escrow

(A) This Policy does not support Key Escrow.

(B) The OCA shall not provide any Key Escrow service.

6.2.4 Private Key Back-Up

(A) The OCA may Back-Up OCA Private Keys insofar as:

(i) each Private Key is protected to a standard which is at least equivalent to that required in relation to the principal Private Key in accordance with this Policy; and

(ii) where more than one Private Key is Backed-Up within a single security environment, each of the Private Keys which is Backed-Up within that environment must be protected to a standard which is at least equivalent to that required in relation to an Issuing OCA Private Key in accordance with this Policy.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

(A) The OCA shall ensure that no OCA Private Key is transferred or copied other than:

(i) for the purposes of:

(a) Back-Up; or

(b) establishing an appropriate degree of resilience in relation to the provision of the SMKI Services;

(ii) in accordance with a level of protection which is compliant with FIPS 140-2

Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

6.2.7 Private Key Storage on Cryptographic Module

See Part 6.2.1 of this Policy.

6.2.8 Method of Activating Private Key

(A) The OCA shall ensure that the Cryptographic Module in which any OCA Private Key is stored may be accessed only by an authorised member of OCA Personnel who has been Authenticated following an Authentication process which:

(i) has an appropriate level of strength to ensure the protection of the Private Key; and

(ii) involves the use of Activation Data.

6.2.9 Method of Deactivating Private Key

(A) The OCA shall ensure that any OCA Private Key shall be capable of being de-activated by means of the OCA Systems, at least by:

(i) the actions of:

(a) turning off the power;

(b) logging off;

(c) carrying out a system reset; and

(ii) a period of inactivity of a length which shall be set out in the Organisation CPS.

6.2.10 Method of Destroying Private Key

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

(B) The OCA shall ensure that no OCA Key (whether in active use, existing as a copy for the purposes of resilience, or Backed-Up) is destroyed except in accordance with a positive decision by the OCA to destroy it.

6.2.11 Cryptographic Module Rating

See Part 6.2.1 of this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

(A) The OCA shall ensure that it archives OCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The OCA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

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

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

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

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

(C) The OCA shall ensure that no OCA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

(A) The OCA shall ensure that any Cryptographic Module within which an OCA Key is held has Activation Data that are unique and unpredictable.

(B) The OCA shall ensure that:

(i) these Activation Data, in conjunction with any other access control, shall be of an appropriate level of strength for the purposes of protecting the OCA Keys; and

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

6.4.2 Activation Data Protection

(A) The OCA shall ensure that the Organisation CPS incorporates provision for the use of such cryptographic protections and access controls as are appropriate to protect against the unauthorised use of Activation Data.

6.4.3 Other Aspects of Activation Data

[*Not applicable in this Policy*]

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

(A) The OCA shall ensure that the Organisation CPS incorporates provisions in relation to the identification and implementation, following the conclusion of any threat assessment, of security measures which make provision for at least the following:

(i) the establishment of access controls in relation to the activities of the OCA;

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

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

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

(v) the audit of security related events; and

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

6.5.2 Computer Security Rating

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

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

(A) The OCA shall ensure that any software which is developed for the purpose of establishing a functionality of the OCA Systems shall:

(i) take place in a controlled environment that is sufficient to protect against the insertion into the software of malicious code;

(ii) be undertaken by a developer which has a quality system that is:

(a) compliant with recognised international standards (such as ISO 9001:2000 or an equivalent standard); or

(b) available for inspection and approval by the SMKI PMA, and has been so inspected and approved.

6.6.2 Security Management Controls

(A) The OCA shall ensure that the Organisation CPS incorporates provisions which are designed to ensure that the OCA Systems satisfy the requirements of Section G2 (System Security: Obligations on the DCC) and Section G5 (Information Security: Obligations on the DCC and Users) of the Code.

6.6.3 Life-Cycle Security Controls

See Part 6.6.2 of this Policy.

6.7 NETWORK SECURITY CONTROLS

6.7.1 Use of Offline Root OCA

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

6.7.2 Protection Against Attack

(A) The OCA shall use its best endeavours to ensure that the OCA Systems are not Compromised, and in particular for this purpose that they are designed and operated so as to detect and prevent:

(i) any Denial of Service Event; and

(ii) any unauthorised attempt to connect to them.

(B) The OCA shall use its reasonable endeavours to ensure that the OCA Systems cause or permit to be open at any time only those network ports, and allow only those protocols, which are required at that time for the effective operation of those Systems, and block all network ports and protocols which are not so required.

6.7.3 Separation of Issuing OCA

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

6.7.4 Health Check of OCA Systems

(A) The OCA shall ensure that, in relation to the OCA Systems, a vulnerability assessment in accordance with Section G2.13 of the Code (Management of Vulnerabilities) is carried out with such frequency as may be specified from time to time by the Independent SMKI Assurance Service Provider.

6.8 TIME-STAMPING

6.8.1 Use of Time-Stamping

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

(B) The OCA shall ensure that the Organisation CA incorporates provisions in relation to the time source and mechanisms used by any Time-Stamping Authority which carries out Time-Stamping on behalf of the OCA.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

The OCA shall use only the Certificate Profiles in Annex B.

7.1.1 Version Number(s)

[*Not applicable in this Policy*]

7.1.2 Certificate Extensions

[*Not applicable in this Policy*]

7.1.3 Algorithm Object Identifiers

[*Not applicable in this Policy*]

7.1.4 Name Forms

[*Not applicable in this Policy*]

7.1.5 Name Constraints

[*Not applicable in this Policy*]

7.1.6 Certificate Policy Object Identifier

[*Not applicable in this Policy*]

7.1.7 Usage of Policy Constraints Extension

[*Not applicable in this Policy*]

7.1.8 Policy Qualifiers Syntax and Semantics

[*Not applicable in this Policy*]

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

[*Not applicable in this Policy*]

7.2 CRL PROFILE

7.2.1 Version Number(s)

(A) The OCA shall ensure that the ARL and CRL conform with X.509 v2 and IETF RFC 5280.

7.2.2 CRL and CRL Entry Extensions

(A) The OCA shall notify Parties of the profile of the CRL and of any CRL extensions.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

[*Not applicable in this Policy*]

7.3.2 OCSP Extensions

[*Not applicable in this Policy*]

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.3 ASSESSOR’S RELATIONSHIP TO ASSESSED ENTITY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.4 TOPICS COVERED BY ASSESSMENT

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

8.6 COMMUNICATION OF RESULTS

Provision in relation to this is made in Appendix C of the Code (SMKI Compliance Policy).

9 OTHER BUSINESS AND LEGAL MATTERS

In so far as provision is made in relation to all the matters referred to in this Part, it is found in the DCC Licence and the provisions of the Code (including in Section L11 (Subscriber Obligations) and Section L12 (Relying Party Obligations) of the Code).

9.1 FEES

See the statement at the beginning of this Part.

9.1.1 Certificate Issuance or Renewal Fees

See the statement at the beginning of this Part.

9.1.2 Organisation Certificate Access Fees

See the statement at the beginning of this Part.

9.1.3 Revocation or Status Information Access Fees

See the statement at the beginning of this Part.

9.1.4 Fees for Other Services

See the statement at the beginning of this Part.

9.1.5 Refund Policy

See the statement at the beginning of this Part.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

See the statement at the beginning of this Part.

9.2.2 Other Assets

See the statement at the beginning of this Part.

9.2.3 Insurance or Warranty Coverage for Subscribers and Subjects

See the statement at the beginning of this Part.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.2 Information not within the Scope of Confidential Information

See the statement at the beginning of this Part.

9.3.3 Responsibility to Protect Confidential Information

See the statement at the beginning of this Part.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

See the statement at the beginning of this Part.

9.4.2 Information Treated as Private

See the statement at the beginning of this Part.

9.4.3 Information not Deemed Private

See the statement at the beginning of this Part.

9.4.4 Responsibility to Protect Private Information

See the statement at the beginning of this Part.

9.4.5 Notice and Consent to Use Private Information

See the statement at the beginning of this Part.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

See the statement at the beginning of this Part.

9.4.7 Other Information Disclosure Circumstances

See the statement at the beginning of this Part.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the statement at the beginning of this Part.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 Certification Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.2 Registration Authority Representations and Warranties

See the statement at the beginning of this Part.

9.6.3 Subscriber Representations and Warranties

See the statement at the beginning of this Part.

9.6.4 Relying Party Representations and Warranties

See the statement at the beginning of this Part.

9.6.5 Representations and Warranties of Other Participants

See the statement at the beginning of this Part.

9.7 DISCLAIMERS OF WARRANTIES

See the statement at the beginning of this Part.

9.8 LIMITATIONS OF LIABILITY

See the statement at the beginning of this Part.

9.9 INDEMNITIES

See the statement at the beginning of this Part.

9.10 TERM AND TERMINATION

9.10.1 Term

See the statement at the beginning of this Part.

9.10.2 Termination of Organisation Certificate Policy

See the statement at the beginning of this Part.

9.10.3 Effect of Termination and Survival

See the statement at the beginning of this Part.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

9.11.1 Subscribers

See the statement at the beginning of this Part.

9.11.2 Organisation Certification Authority

See the statement at the beginning of this Part.

9.11.3 Notification

See the statement at the beginning of this Part.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

See the statement at the beginning of this Part.

9.12.2 Notification Mechanism and Period

See the statement at the beginning of this Part.

9.12.3 Circumstances under which OID Must be Changed

See the statement at the beginning of this Part.

9.13 DISPUTE RESOLUTION PROVISIONS

See the statement at the beginning of this Part.

9.14 GOVERNING LAW

See the statement at the beginning of this Part.

9.15 COMPLIANCE WITH APPLICABLE LAW

See the statement at the beginning of this Part.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

See the statement at the beginning of this Part.

9.16.2 Assignment

See the statement at the beginning of this Part.

9.16.3 Severability

See the statement at the beginning of this Part.

9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights)

See the statement at the beginning of this Part.

9.16.5 Force Majeure

See the statement at the beginning of this Part.

9.17 OTHER PROVISIONS

9.17.1 Organisation Certificate Policy Content

See the statement at the beginning of this Part.

9.17.2 Third Party Rights

See the statement at the beginning of this Part.

Annex A: Definitions and Interpretation

In this Policy, except where the context otherwise requires -

- expressions defined in Section A of the Code (Definitions and Interpretation) have the same meaning as is set out in that Section,
- the expressions in the left hand column below shall have the meanings given to them in the right hand column below,
- where any expression is defined in Section A of the Code (Definitions and Interpretation) and in this Annex, the definition in this Annex shall take precedence for the purposes of the Policy.

Activation Data means any private Data (such as a password or the Data on a smartcard) which are used to access a Cryptographic Module.

Archive means the archive of Data created in accordance with Part 5.5.1 of this Policy (and "**Archives**" and "**Archived**" shall be interpreted accordingly).

Audit Log means the audit log created in accordance with Part 5.4.1 of this Policy.

Authentication means the process of establishing that an individual, Certificate, System or Organisation is what he or it claims to be (and "**Authenticate**" shall be interpreted accordingly).

Authorised Subscriber means a Party which has successfully completed the procedures set out in the RAPP and has been authorised by the OCA to submit a Certificate Signing Request.

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

Certificate means either an Organisation Certificate or an OCA Certificate.

Certificate Profile means a table bearing that title in Annex B and specifying certain parameters to be contained within a Certificate.

Certificate Re-Key means a change to the Public Key contained within a Certificate bearing a particular serial number.

Certificate Revocation List (or **CRL**)

means a list, produced by the OCA, of all Organisation Certificates that have been revoked in accordance with this Policy.

Certificate Revocation Request

means a request for the revocation of a Certificate by the OCA, submitted by the Subscriber for that Certificate to the OCA in accordance with the RAPP and this Policy.

Certificate Signing Request

means a request for a Certificate submitted by an Eligible Subscriber in accordance with the RAPP.

DCA

has the meaning given to that expression in Appendix A of the Code (SMKI Device Certificate Policy).

DCA Systems

has the meaning given to that expression in Appendix A of the Code (SMKI Device Certificate Policy).

Eligible Subscriber

means:

(a) in relation to an Organisation Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.9 of the Code (Organisation Certificates); and

(b) in relation to an OCA Certificate, an Authorised Subscriber which is identified as an Eligible Subscriber in accordance with Section L3.10 of the Code (OCA Certificates).

Issue

means the act of the OCA, in its capacity as the Root OCA or Issuing OCA, and acting in accordance with this Policy, of creating and signing a Certificate which is bound to both a Subject and a Subscriber (and "**Issued**" and "**Issuing**" shall be interpreted accordingly).

Issuing Organisation Certification Authority (or **Issuing OCA**)

means the DCC exercising the function of Issuing Organisation Certificates to Eligible Subscribers and of storing and managing the Private Keys associated with that function.

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

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

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

Key Escrow means the storage of a Private Key by a person other than the Subscriber or Subject of the Certificate which contains the related Public Key.

Object Identifier (or **OID**) means an Object Identifier assigned by the Internet Address Naming Authority.

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

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

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

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

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

Organisation Certification Authority (or **OCA**) means the DCC, acting in the capacity and exercising the functions of one or more of:

(d) the Root OCA;

(e) the Issuing OCA; and

(f) the Registration Authority.

Private Key Material in relation to a Private Key, means that Private Key and the input parameters necessary to establish, use and maintain it.

Registration Authority means the DCC exercising the function of receiving and processing Certificate Signing Requests made in accordance with the 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 RAPP.

Registration Authority Personnel means those persons who are engaged by the DCC, in so far as such persons carry out, or are authorised to carry out, any function of the Registration Authority.

Relying Party means a person who, pursuant to the Code, receives and relies upon a Certificate.

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

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

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

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

Subject means:

(a) in relation to an Organisation Certificate, the Organisation identified in the 'Subject Name' field of the Organisation Certificate Profile in Annex B; and

(b) in relation to an OCA Certificate, the globally unique name of the Root OCA or Issuing OCA as identified in the ‘Subject’ field of the relevant Certificate Profile in Annex B.

Subscriber means, in relation to any Certificate, a Party which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the Certificate.

Time-Stamping means the act that takes place when a Time-Stamping Authority, in relation to a Certificate, stamps a particular datum with an accurate indicator of the time (in hours, minutes and seconds) at which the activity of stamping takes place.

Time-Stamping Authority means that part of the OCA that:

(c) where required, provides an appropriately precise time-stamp in the format required by this Policy; and

(d) relies on a time source that is:

(i) accurate;

(ii) determined in a manner that is independent of any other part of the OCA Systems; and

(iii) such that the time of any time-stamp can be verified to be that of the independent time source at the time at which the time-stamp was applied.

Validity Period means, in respect of a Certificate, the period of time for which that Certificate is intended to be valid.

Annex B: OCA Certificate and Organisation Certificate Profiles

End Entity Certificate Structure and Contents

This Annex lays out requirements as to structure and content with which OCA Certificates and Organisation Certificates shall comply. All terms in this Annex shall, where not defined in the Code, this Policy, or the GB Companion Specification, have the meanings in IETF RFC 5759 and IETF RFC5280.

Common requirements applicable to OCA Certificates and Organisation Certificates

All OCA Certificates and Organisation Certificates that are validly authorised within the SMKI for use within the scope of GB Companion Specification and GB Smart Metering:

- shall be compliant with IETF RFC 5759 and so with IETF RFC5280.
- for clarity and in adherence with the requirements of IETF RFC5759, all OCA Certificates and Organisation Certificates shall:
  - contain the authorityKeyIdentifier extension, except where the Certificate is the Root OCA Certificate;
  - contain the keyUsage extension which shall be marked as critical;
- be X.509 v3 certificates as defined in IETF RFC 5280, encoded using the ASN.1 Distinguished Encoding Rules;
- only contain Public Keys of types that are explicitly allowed by the GBCS. This means all Public Keys shall be elliptic curve Public Keys on the NIST P-256 curve;
- only contain Public Keys in uncompressed form i.e. contain an elliptic curve point in uncompressed form as detailed in Section 2.2 of IETF RFC5480;
- only provide for signature methods that are explicitly allowed within the GBCS. This means using P-256 Private Keys with SHA 256 and ECDSA;
- contain a certificatePolicies extension containing at least one PolicyIdentifier which shall be marked as critical. For clarity and in adherence with IETF RFC 5280, Certification Path Validation undertaken by Parties and Devices shall interpret this extension;
- contain a serialNumber of no more than 16 octets in length;
- contain a subjectKeyIdentifier which shall be marked as non-critical;
- contain an authorityKeyIdentifier in the form [0] KeyIdentifier which shall be marked as non-critical, except where the Certificate is the Root OCA Certificate. Note this exception only applies where RemotePartyRole as specified in the X520OrganizationalUnitName field = root;

  - only contain KeyIdentifiers generated as per method (2) of Section 4.2.1.2 of IETF RFC 5280 and so which shall always be 8 octets in length;
  - contain an IssuerName which MUST be identical to the signer's SubjectName
  - have a valid notBefore field consisting of the time of issue encoded and a valid notAfter field expiration date as per IETF RFC 5280 Section 4.1.2.5.

Requirements applicable to Organisation Certificates only

All Organisation Certificates that are issued by the OCA shall:

- contain a subjectUniqueID whose value shall be the 8 octet Entity Identifier of the subject of the Certificate;
- contain a non-empty subject field which contains an X520 OrganizationalUnitName whose value shall be set to the RemotePartyRole that this Certificate allows the subject of the certificate to perform;
- contain a single Public Key;
- contain a keyUsage extension marked as critical, with a value of only one of:
  - digitalSignature; or
  - keyAgreement.
- contain a single policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is issued.

Requirements applicable to the Root OCA and Issuing OCA

All OCA Certificates issued by the OCA shall:

  - be such that, per RFC5280, the IssuerName MUST be identical to the signer’s SubjectName;
  - have a globally unique SubjectName;
  - contain a single public key except for the Root-CA where there shall be two public keys. The second public key shall be referred to as the Contingency Key and shall be present in the WrappedApexContingencyKey extension with the meaning of IETF RFC5934. The Contingency Key shall be encrypted as per the requirements of the GBCS;
  - contain a keyUsage extension marked as critical and defined as:
    - keyCertSign; and

    - cRLSign;
- for Issuing OCA Certificates, contain at least one policyIdentifier in the certificatePolicies extension that refers to the OID of this Policy under which the Certificate is issued;
- for the Root OCA Certificate, contain a single policyIdentifier in the certificatePolicies extension that refers to the OID for any Policy;
- for Issuing OCA Certificates, contain the basicConstraints extension, with values cA=True, and pathLen=0. This extension shall be marked as critical;
- for the Root OCA Certificate, contain the basicConstraints extension, with the value cA=True and pathLen absent (unlimited). This extension shall be marked as critical.

Organisation Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 with ECDSA	
Issuer	Name	Globally unique name of Issuing OCA	
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 Organisation Certificate	

notAfter	Time	Expiry time of the Certificate	
Subject	Name	Name of the Subject	
OrganisationalUnitName	Sub-type of Name	Remote Party Role Code of the subject of the Certificate	
subjectUniqueID	UniqueIdentifier	The 64 bit Entity Identifier of the subject of the Certificate	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Organisation Certificate signature	

Interpretation

Version

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

serialNumber

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

Signature

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

Issuer

The name of the signer of the Organisation Certificate. This will be the gloablly unique name of the Issuing OCA.

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 Organisation Certificates. The Organisation Certificate shall contain a authorityKeyIdentifier in the form [0] KeyIdentifier.

subjectKeyIdentifier

The Subject Key Identifier extension shall be included and marked as non-critical in the Organisation Certificate. The Organisation 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 OCA expects the Organisation Certificate to be valid. The validity period is the period of time from notBefore through notAfter, inclusive.

All times shall be stated in the Universal Coordinated Time (UTC) time zone. Times up to and including 23:59:59 December 31, 2049 UTC shall be encoded as UTCTime as YYMMDDHHmmssZ.

Times later than 23:59:59 December 31, 2049 UTC shall be encoded as GeneralizedTime as YYYYMMDDHHmmssZ.

notBefore

The earliest time an Organisation Certificate may be used. This shall be the time the Organisation Certificate is created.

notAfter

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

subject

The formatting of this field shall contain a unique X.500 Distinguished Name (DN). This should be the unique trading name of the Organisation.

OrganizationalUnitName

The OrganisationalUnitName attribute of subject shall be populated with the RemotePartyRole code that the Certificate allows the subject of the Certificate to perform. See the GB Companion Specification for details of RemotePartyRole codes.

subjectUniqueID

This shall be populated with the 64 bit Entity Identifier (compliant with EUI-64 standard – see Great Britain Companion Specification) of the subject of the Certificate

subjectPublicKeyInfo

The Organisation Certificate subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall be use the following identifier:

> id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Organisation Certificate extension (explained further under the next ‘**extensions**’ heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {

  namedCurve       OBJECT IDENTIFIER

  -- implicitCurve   NULL

  -- specifiedCurve  SpecifiedECDomain

}
```

Only the following field in ECParameters shall be used:

> o namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The namedCurve field in ECParameters uses object identifiers to name well-known curves.

The NIST recommended namedCurve is the P-256 curve. The object identifier fo the curve choice to be used in Organisation Certificate is:

> secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key. ECC Public Keys have the following syntax:

> ECPoint ::= OCTET STRING

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The elliptic curve Public Key (a value of type ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

The first octet of the OCTET STRING indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

The signatureAlgorithm field shall indicate the Issuing OCA signature algorithm used to sign this Organisation Certificate is as defined under the next ‘**Signature Method (ECDSA)**’ heading below.

signatureValue

The Issuing OCA’s signature of the Organisation Certificate is computed using the Issuing OCA’s private 256-bit ECC Organisation Certificate signing key using the algorithm identified under the next ‘**Signature Method (ECDSA)**’ heading below.

When using the Elliptic Curve keys the Organisation Certificates shall be signed by the Issuing OCA using the ECDSA algorithm identified under the next ‘**Signature Method (ECDSA)**’ heading below. The structure for ECDSA signatures is as per RFC 5480.

extensions

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

- certificatePolicy: critical; OID as a policyIdentifier (the OID of the applicable Organisation Certificate Policy).
- keyUsage: critical; either keyAgreement or digitalSignature.
- authorityKeyIdentifier.
- subjectKeyIdentifier.

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

> ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

SHA-256 hash algorithm

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

Root OCA Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
Version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	

Signature	AlgorithmIdentifier	SHA256 with ECDSA	
Issuer	Name	Globally unique name of Root OCA	
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	Globally unique name of Root OCA (same as Issuer name)	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject's Public Key	
WrappedApexContingencyKey	ApexContingencyKey	The subject's protected (encrypted) Public Key used for recovery purposes	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject Certificate signature	

These certificates are the root of trust for the Organisations SMKI.

Version

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

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the OCA Certificate that signs the Certificate (self-signed by Root OCA). The serialNumber shall be unique in the scope of Certificates signed by the OCA Certificate.

Signature

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

Issuer

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

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 so which shall always be 8 octets in length.

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 OCA.

subjectPublicKeyInfo

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall be use the following identifier:

> id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next '**extensions**' heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {

 namedCurve        OBJECT IDENTIFIER

 -- implicitCurve   NULL

 -- specifiedCurve  SpecifiedECDomain

}
```

Only the following field in ECParameters shall be used:

o namedCurve - identifies all the required values for a particular set of elliptic curve domain parameters to be represented by an object identifier.

The namedCurve field in ECParameters uses object identifiers to name well-known curves.

The NIST recommended namedCurve is the P-256 curve. The object identifier fo the curve choice to be used in OCA Certificates is:

secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key. ECC Public Keys have the following syntax:

ECPoint ::= OCTET STRING

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The elliptic curve Public Key (a value of type ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

The first octet of the OCTET STRING indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

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

signatureValue

The Root OCA's signature of the Certificate is computed using the Root OCA's private 256-bit ECC Organisation Certificate signing key using the algorithm identified under the next '**Signature Method (ECDSA)**' heading below.

When using the Elliptic Curve keys the Organisation Certificates shall be signed by the Issuing OCA using the ECDSA algorithm identified under the next '**Signature Method (ECDSA)**' heading below. The structure for ECDSA signatures is as per RFC 5480.

extensions

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

Extensions

- certificatePolicy: critical; 1:anyPolicy
- keyUsage: critical; keyCertSign, crlSign
- basicConstraints: critical; cA=true, pathLen absent (unlimited)
- subjectKeyIdentifer

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

> ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

SHA-256 hash algorithm

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

Issuing OCA Certificate Profile

Field Name	**RFC 5759/5280 Type**	**Value**	**Reference**
version	Integer	V3	
serialNumber	Integer	Positive Integer of up to 16 Octets	
Signature	AlgorithmIdentifier	SHA256 with ECDSA	
Issuer	Name	Globally unique name of Root OCA	

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	Globally unique name of Issuing OCA	
subjectPublicKeyInfo	SubjectPublicKeyInfo	The subject’s Public Key	
Extensions	Extensions	Critical and non-critical extensions	
signatureAlgorithm	AlgorithmIdentifier	SHA256 with ECDSA	
signatureValue	BIT STRING	Subject certificate signature	

Version

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

serialNumber

Certificate serial number, a positive integer of up to 16 octets. The serialNumber identifies the Certificate, and shall be created by the Root OCA that signs the Certificate. The serialNumber shall be unique in the scope of Certificates signed by the Root OCA.

Signature

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

issuer

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

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 Organisation Certificates. The Certificates shall contain a authorityKeyIdentifier in the form [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 OCA.

subjectPublicKeyInfo

The Certificate's subjectPublicKeyInfo field shall indicate the Public Key algorithm identifier and the Public Key in the specified algorithm format as specified in RFC 3279 and RFC 5480.

The algorithm field in the subjectPublicKeyInfo structure shall be use the following identifier:

> id-ecPublicKey OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) keyType(2) 1 }

id-ecPublicKey indicates that the algorithms that can be used with the subject Public Key are unrestricted. The key is only restricted by the values indicated in the key usage Certificate extension (explained further under the next '**extensions**' heading below).

The parameter for id-ecPublicKey is as follows and shall always be present:

```
ECParameters ::= CHOICE {
  namedCurve        OBJECT IDENTIFIER
  -- implicitCurve   NULL
  -- specifiedCurve  SpecifiedECDomain
}
```

Only the following field in ECParameters shall be used:

```
   o namedCurve - identifies all the required values for a particular
     set of elliptic curve domain parameters to be represented by an
     object identifier.
```

The namedCurve field in ECParameters uses object identifiers to name well-known curves.

The NIST recommended namedCurve is the P-256 curve. The object identifier fo the curve choice to be used in Certificates is:

> secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 }

The subjectPublicKey from SubjectPublicKeyInfo is the ECC Public Key. ECC Public Keys have the following syntax:

> ECPoint ::= OCTET STRING

Implementations of Elliptic Curve Cryptography according to this document shall only support the uncompressed form.

The elliptic curve Public Key (a value of type ECPoint that is an OCTET STRING) is mapped to a subjectPublicKey (a value of type BIT STRING) as follows: the most significant bit of the OCTET STRING value becomes the most significant bit of the BIT STRING value, and so on; the least significant bit of the OCTET STRING becomes the least significant bit of the BIT STRING.

The first octet of the OCTET STRING indicates whether the key is compressed or uncompressed. The uncompressed form is indicated by 0x04 (the compressed form is indicated by either 0x02 or 0x03). The Public Key MUST be rejected if any value other than 0x04 is included in the first octet.

signatureAlgorithm

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

signatureValue

The Root OCA's signature of the Certificate is computed using the Root OCA's private signing key using the algorithm identified under the next '**Signature Method (ECDSA)**' heading below.

When using the Elliptic Curve keys the Certificates shall be signed by the Root OCA using the ECDSA algorithm identified in under the next '**Signature Method (ECDSA)**' heading below. The structure for ECDSA signatures is as per RFC 5480.

extensions

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

- certificatePolicy: critical; 1:at least one policyIdentifier in the certificatePolicies extension that refers to the OID(s) valid for usage in the GBSM environments
- keyUsage: critical; keyCertSign, crlSign
- basicConstraints: critical; cA=true, pathLen=0
- subjectKeyIdentifer
- authorityKeyIdentifier

Cryptographic Primitives for Signature Method

Signature Method (ECDSA)

The ECDSA signature method is defined in NIST FIPS 186-4. When implementing ECDSA, the SHA-256 message digest algorithm and the P-256 elliptic curve as defined in FIPS 186-4 Annex D, D.1.2.3, shall be used.

The signature algorithm shall be ecdsa-with-SHA256 as specified in RFC 5759 and 6318. The algorithm identifier is:

ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-sha2(3) 2 }

SHA-256 hash algorithm

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

SCHEDULE 8

NEW APPENDIX C FOR INSERTION INTO SMART ENERGY CODE

"APPENDIX C – SMKI COMPLIANCE POLICY

1 INTRODUCTION

1.1 The document comprising this Appendix C:

(a) shall be known as the "**SMKI Compliance Policy**" (and in this document is referred to simply as the "**Policy**"),

(b) is a SEC Subsidiary Document related to Section L2 of the Code (SMKI Assurance).

2 SMKI INDEPENDENT ASSURANCE SCHEME

DCC: Duty to Submit to an SMKI Independent Assurance Scheme

2.1 The DCC shall subject the SMKI Services to assessment against an assurance scheme which satisfies:

(a) the quality requirements specified in Part 2.2 of this Policy;

(b) the independence requirements specified in Part 2.3 of this Policy; and

(c) the approval requirements specified in Part 2.5 of this Policy,

and that scheme is referred to in this Policy as the "**SMKI Independent Assurance Scheme**".

Quality Requirements

2.2 The quality requirements specified in this Part 2.2 are that the SMKI Independent Assurance Scheme must be a scheme:

(a) which is recognised as an accreditation scheme for the purposes of Article 3(2) of Directive 1999/93/EC on a Community framework for electronic signatures;

(b) which is based on ISO 27001; and

(c) the provider of which:

(i) is used by the United Kingdom Government to provide assurance in relation to electronic trust services; and

(ii) requires all its scheme assessors to be UKAS certified.

Independence Requirements

2.3 The independence requirements specified in this Part 2.3 are that the provider of the SMKI Independent Assurance Scheme must be independent of the DCC and of each DCC Service Provider from which the DCC acquires capability for the purposes of the provision of the SMKI Services.

2.4 For the purposes of Part 2.3 of this Policy, the provider of the SMKI Independent Assurance Scheme is to be treated as independent of the DCC (and of 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 provider of the scheme;

(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 provider of the scheme; and

(c) the provider of the scheme does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC (or in any such DCC Service Provider).

Approval Requirements

2.5 Before entering into any agreement with the provider of the SMKI Independent Assurance Scheme, in accordance with its obligation under Section L2.2 of the Code (SMKI Compliance Policy), the DCC shall submit to the SMKI PMA for approval:

(a) its proposed choice of scheme; and

(b) the proposed terms and conditions of its agreement with the provider of that scheme,

and shall not enter into any such agreement unless the SMKI PMA has first approved the proposed SMKI Independent Assurance Scheme and the proposed terms and conditions of that agreement.

2.6 If the SMKI PMA does not approve either the proposed SMKI Independent Assurance Scheme or the proposed terms and conditions of the DCC's agreement with the provider of that scheme:

(a) the SMKI PMA shall provide the DCC with a statement of its reasons for not doing so; and

(b) the DCC shall submit to the SMKI PMA for approval, as soon as is reasonably practicable, a revised proposal in relation to the scheme.

3 INDEPENDENT ASSURANCE SERVICE PROVIDER

DCC: Duty to Procure Independent Assurance Services

3.1 For the purposes of complying with its obligation under Section L2.2 of the Code (SMKI Compliance Policy), the DCC shall procure the provision of assurance services:

(a) of the scope specified in Part 3.2 of this Policy;

(b) from a person who:

(i) is suitably qualified in accordance with Part 3.3 of this Policy; and

(ii) satisfies the independence requirements specified in Part 3.4 of this Policy,

and that person is referred to in this Policy as the "**Independent SMKI Assurance Service Provider**".

Scope of Independent Assurance Services

3.2 The assurance services specified in this Part 3.2 are services in accordance with which the Independent SMKI Assurance Service Provider shall:

(a) undertake an initial assessment of the SMKI Services against the SMKI Independent Assurance Scheme in accordance with Part 4 of this Policy;

(b) subsequently undertake further assessments of the SMKI Services against the SMKI Independent Assurance Scheme:

(i) at a frequency recommended by the provider of that scheme; or

(ii) where there is no such recommended frequency, or where the SMKI PMA otherwise determines, at a frequency specified by the SMKI PMA;

(c) at the request of, and to an extent determined by, the SMKI PMA, carry out an assessment of the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set;

(d) at the request of the SMKI PMA, provide to it advice in relation to the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set;

(e) at the request of the SMKI PMA, provide to it advice in relation to a review of this Policy, which shall include in particular:

(i) recommendations as to the scope and frequency of assessments carried out in accordance with this Policy; and

(ii) advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default), including where the Defaulting Party is the DCC in accordance with Section L2.6 of the Code (Events of Default); and

(f) at the request of the SMKI PMA Chair, provide a representative to attend and contribute to the discussion at any meeting of the SMKI PMA.

Suitably Qualified Service Provider

3.3 The Independent SMKI Assurance Service Provider shall be treated as suitably qualified in accordance with this Part 3.3 only if it is recognised by the provider of the SMKI Independent Assurance Scheme as being qualified to carry out assessments against that scheme.

Independence Requirements

3.4 The independence requirements specified in this Part 3.4 are that the Independent SMKI Assurance Service Provider must be independent of each SMKI Participant and of each service provider from whom that SMKI Participant acquires capability for any purpose related to its compliance with its obligations under the Code (but excluding any provider of corporate assurance services to that SMKI Participant).

3.5 For the purposes of Part 3.4 of this Policy, the Independent SMKI Assurance Service Provider is to be treated as independent of an SMKI Participant (and of a relevant service provider of that SMKI Participant) only if:

(a) neither that SMKI Participant nor any of its subsidiaries (or such a service provider or any of its subsidiaries) holds or acquires any investment by way of shares, securities or other financial rights or interests in the Independent SMKI Assurance Service Provider;

(b) no director of that SMKI Participant (or of any such service provider) is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the Independent SMKI Assurance Service Provider; and

(c) the Independent SMKI Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in that SMKI Participant (or in any such service provider).

4 INITIAL ASSURANCE ASSESSMENT

DCC: Duty to Procure Initial Assessment

4.1 The DCC shall ensure that an initial assurance assessment of the SMKI Services:

(a) against the SMKI Independent Assurance Scheme; and

(b) in respect of compliance by the DCC with the applicable requirements of the SMKI Document Set,

is undertaken by the Independent SMKI Assurance Service Provider in accordance with Parts 4.2 and 4.3 of this Policy.

Nature of the Initial Assessment

4.2 The initial assessment referred to in Part 4.1 of this Policy shall:

(a) be undertaken prior to the SMKI Services being provided for any purpose other than the issue of Test Certificates; and

(b) result in an assessment report in relation to the SMKI Services being produced by the Independent SMKI Assurance Service Provider at least one month prior to the anticipated start date of Interface Testing.

4.3 The assessment report referred to in Part 4.2 of this Policy shall:

(a) clearly identify any failure of the DCC to comply with the applicable requirements of the SMKI Document Set;

(b) recommend that the assurance status of the DCC in relation to the SMKI Services should be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved; and

(c) be provided to both the DCC and the SMKI PMA promptly upon completion.

PMA: Response to the Initial Assessment

4.4 On receiving an initial assessment report in accordance with Part 4.3 of this Policy, the SMKI PMA shall:

(a) promptly consider the report;

(b) determine that the assurance status of the DCC in relation to the SMKI Services is to be set at:

(i) approved;

(ii) approved with caveats; or

(iii) not approved;

(c) where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at 'approved with caveats', state in writing its reasons for considering that it is acceptable for the DCC to commence the provision of the SMKI Services for any purpose other than the issue of Test Certificates; and

(d) provide a copy of the report (being redacted only in so far as necessary for the purposes of security) and a statement of its determination (and of any reasons accompanying that determination) to all Parties.

4.5 Where the SMKI PMA has set the assurance status of the DCC in relation to the SMKI Services at 'approved with caveats' or 'not approved' it may:

(a) require that the DCC submit to it as soon as reasonably practicable a remedial action plan; and

(b) within one month of the submission of that plan, require the DCC to make any changes to it that the SMKI PMA may specify.

DCC: Duty in relation to Remedial Action Plan

4.6 Where the DCC is required to do so in accordance with Part 4.5(a) of this Policy, it shall as soon as reasonably practicable submit to the SMKI PMA a remedial action plan.

4.7 Where the DCC is required by the SMKI PMA in accordance with Part 4.5(b) of this Policy to make changes to the remedial action plan, it may appeal that decision to the Authority and:

(a) the Authority shall determine what changes (if any) shall be made to the remedial action plan; and

(b) the determination of the Authority shall be final and binding for the purposes of the Code.

4.8 The DCC shall implement any remedial action plan subject to any required changes to it specified by:

(a) the SMKI PMA in accordance with Part 4.6 of this Policy; or

(b) the Authority in accordance with Part 4.7 of this Policy.

5 **PMA: DUTY TO PROVIDE INFORMATION**

Initial Assurance Assessment

5.1 The SMKI PMA shall, on request, provide to the Secretary of State and the Authority a copy of:

(a) the initial assessment report received by it in accordance with Part 4.3 of this Policy; and

(b) any remedial action plan that the DCC is required to implement in accordance with Part 4.8 of this Policy.

Subsequent Assurance Assessments

5.2 Following any assessment carried out by the Independent SMKI Assurance Service Provider of the compliance of the DCC with the applicable requirements of the SMKI Document Set, the SMKI PMA's determination as to the extent to which the DCC is compliant with those requirements shall be made available by it to:

(a) all Parties;

(b) the Panel;

(c) the Authority; and

(d) on request, the Secretary of State."

GUIDANCE NOTE

(This note is not part of the modifications)

The purpose of these licence and code modifications is to place new obligations relating to the operation of smart meters on the holder of the smart meter communication licences and other energy licence holders through the Smart Energy Code, and to amend existing obligations on the smart energy communication licences holder in its licences.

A smart meter communication licence has been granted to Smart DCC Limited (a company registered in England and Wales with number 08641679) under each of section 7AB(2) of the Gas Act 1986 (c 44) and section 6(1A) of the Electricity Act 1989 (c 29). The two licences have uniform licence conditions. The licensee is required to maintain and keep in force the Smart Energy Code under condition 21 of the licences. Electricity and gas suppliers, electricity distributors and gas transporters are obliged to be a party to that code under the conditions of their licences.[1]

Smart meters are electricity and gas meters with enhanced functionalities, including the capability of providing consumption information to the consumer in near real-time, and to be remotely read by or on behalf of the supplier. Smart meters will promote energy saving by electricity and gas consumers, and will facilitate further efficiencies in the gas and electricity distribution and supply systems.

Paragraphs 3 and 4 make minor changes to the smart meter communication licences in order to ensure that their existing meaning is clear. Paragraph 5 replaces the table in appendix 1 to condition 36 of those licences. The changed table slightly alters the time period for payments to the licence holder by its customers, but does not change the total amount to be paid. Paragraph 6 amends a typographical error and makes consequential changes to cross-references.

Paragraphs 8 to 14 contain modifications to the smart energy code, primarily by adding content into the code.

Paragraph 10 and schedule 2 contain changes relating to the technology of smart meters, including introducing lists of products which will be available to detail devices which have passed an assurance regime. A sub-committee is also introduced to ensure that sufficient technical expertise will be available to support and advise various parties with roles in the governance of the technical design. Provision is made for the resolution of disputes concerning technology.

Paragraphs 11 and 13 and schedules 3 and 5 introduce a detailed testing regime, the various parts of which should ensure that the systems of the various parties involved in the operation of smart meters work together before the smart meter communication licence holder begins to provide communications to meters in consumer premises. Provision is made for testing of the systems required for the new security services to be provided by the licence holder (pursuant to paragraph 12 as detailed below). New obligations are put on that licence holder to provide services connected to the testing.

Paragraph 12 and schedule 4 contain new obligations and governance arrangements for a system of smart meters key infrastructure – a security system designed to ensure that messages to and from smart metering devices are properly authorised and are adequately protected from interference. Paragraph 15 and schedules 6 to 8 insert subsidiary documents into the SEC which support that security system by providing detailed obligations flowing from the granting of security accreditation certificates and a process for assurance of the security service.

[1] Copies of licences are available at www.ofgem.gov.uk, and the Smart Energy Code can be viewed at https://www.smartenergycodecompany.co.uk/.

Paragraphs 8, 9 and 14 make consequential changes related to the introduction of the above content to the code. They provide for new or modified defined terms, and make provision determining when the new content will have full effect.

The Secretary of State will publish the modifications on the website of the Department of Energy and Climate Change as soon as reasonably practicable.