# SECTION L – SMART METERING KEY INFRASTRUCTURE AND DCC KEY INFRASTRUCTURE

## L1  SMKI POLICY MANAGEMENT AUTHORITY

**Establishment of the SMKI PMA**

L1.1  The Panel shall establish a Sub-Committee in accordance with the requirements of this Section L1, to be known as the "**SMKI PMA**".

L1.2  Save as expressly set out in this Section L1, the SMKI PMA shall be subject to the provisions concerning Sub-Committees set out in Section C6 (Sub-Committees).

**Membership of the SMKI PMA**

L1.3  The SMKI PMA shall be composed of the following persons (each an "**SMKI PMA Member**"):

(a)  the SMKI PMA Chair (as further described in Section L1.5);

(b)  four SMKI PMA (Supplier) Members (as further described in Section L1.6);

(c)  two SMKI PMA (Network) Member (as further described in Section L1.8);

(d)  one representative of the Security Sub-Committee and one representative of the Technical Architecture and Business Architecture Sub-Committee (in each case as further described in Section L1.10); and

(e)  one SMKI Specialist (appointed as described in the definition of that expression in Section A1 (Definitions)).

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 four "**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 four SMKI PMA (Supplier) Members shall be appointed in accordance with a process:

(a)     by which three 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 "SMKI 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 two "**SMKI PMA (Network) Members**" shall (subject to any directions to the contrary made by the Secretary of State for the purpose of transition on the incorporation of this Section 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) Members", 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 two SMKI PMA (Network) Members shall be appointed in accordance with a process:

(a)     by which one SMKI PMA (Network) Member will be elected by the Electricity Network Parties and one SMKI PMA (Network) Member will be elected by the Gas Network Parties and

(b)     that is otherwise the same as that by which Elected Members are elected under Sections C4.2 and C4.3 (as if references therein to "Panel" were to "SMKI PMA", to "Panel Chair" were to "PMA Chair", to "Panel Members" were to

"SMKI PMA Members", and to provisions of Section C or D were to the corresponding provisions set out in or applied pursuant to this Section L1).

L1.10 The Security Sub-Committee and the Technical Architecture and Business Architecture Sub-Committee shall each nominate one of their members to be an SMKI PMA Member by notice to the Secretariat from time to time. The Security Sub-Committee or the Technical Architecture and Business Architecture Sub-Committee (as applicable) may each replace its nominee from time to time by prior notice to the Secretariat. Such nomination or replacement shall be subject to compliance by the relevant person with Section C6.9 (Member Confirmation). Until each such Sub-Committee exists, the Panel shall nominate a person to act as a representative of that Sub-Committee (and may from time to time replace such person).

L1.11 Each SMKI PMA Member must ensure that he or she reads the SMKI Document Set when first appointed, and subsequently from time to time, so that he or she is familiar with its content.

**Proceedings of the SMKI PMA**

L1.12 Each SMKI PMA Member shall be entitled to appoint an Alternate in accordance with Section C5.19 (as it applies pursuant to Section L1.15); provided that:

(a) the SMKI PMA Chair will be deemed to have nominated the SMKI Specialist to act as Alternate for the SMKI PMA Chair; and

(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).

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)     a representative of the DCC shall be invited to attend each and every SMKI PMA meeting (which representative 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 in any circumstances and the SMKI Specialist shall have no rights under that Section.

**Duties of the SMKI PMA**

L1.17   The SMKI PMA shall undertake the following duties:

(a)     to approve the Device CPS, Organisation CPS and the IKI CPS, and any changes to those documents, in accordance with Sections L9;

(b)     to propose variations to the SMKI SEC Documents, as further described in Section L1.19;

(c)     to periodically review (including where directed to do so by the Panel) the effectiveness of the SMKI Document Set (including so as to evaluate whether the SMKI Document Set remains consistent with the SEC Objectives), and report to the Panel on the outcome of such review (such report to include any recommendations for action that the SMKI PMA considers appropriate);

(d)     as soon as reasonably practicable following the incorporation of each of the

following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (c) above:

(i)       the SMKI Compliance Policy;

(ii)      the SMKI RAPP;

(iii)     the Device Certificate Policy;

(iv)      the Organisation Certificate Policy;

(v)       the IKI Certificate Policy;

(vi)      the SMKI Recovery Procedure,

and (where the SMKI PMA considers it appropriate to do so) submit one or more Modification Proposals in respect of those documents (which Modification Proposals shall, notwithstanding Section X2.3(a), (b) and (c), be subject to Section D (Modification Process) as varied by Section X2.3(d));

(e)     to periodically review the effectiveness of the DCCKI Document Set and to:

(i)       notify DCC where it considers that changes should be made to the DCCKI Document Set in order to ensure that DCC meets its obligations under Section G (Security) (such notification to include any recommendation for action that the SMKI PMA considers appropriate); and

(ii)      copy any such notification to the Security Sub-Committee and, except to the extent that it is appropriate to redact information for security purposes, to other SEC Parties;

(f)     as soon as reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, to review that document in accordance with paragraph (e) above:

(i)       the DCCKI RAPP;

(ii)     the DCCKI Certificate Policy;

(g)     to review the DCCKI CPS, and any amendments proposed to be made to it by the DCC, in accordance with Section L13 (DCC Key Infrastructure);

(h)     as part of its review of the SMKI Compliance Policy pursuant to paragraph (d) above, to consider whether SMKI Participants which are subject to assurance assessments pursuant to the SMKI Compliance Policy should be liable to meet the costs (or a proportion of the costs) of undertaking such assessments, and (where the SMKI PMA considers it appropriate to do so) submit one or more Modification Proposals as referred to in paragraph (d) above;

(i)     in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, to decide, in accordance with the SMKI Recovery Key Guidance, whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key);

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

(k)     to provide the Panel, the Change Board and Working Groups with support and advice in respect of Modification Proposals that provide for variations to the SMKI SEC Documents or the DCCKI SEC Documents;

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

(m)     to provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the SMKI Document Set or the DCCKI Document Set;

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

(o)     to exercise such functions as are allocated to it under, and to comply with all the

applicable requirements of, the SMKI Document Set in accordance with Section L9.1; and

(p)     to perform any other duties expressly ascribed to the SMKI PMA elsewhere in this Code.

L1.18   The SMKI PMA shall establish a process whereby the Code Administrator monitors Modification Proposals with a view to identifying (and bringing to the SMKI PMA's attention) those proposals that are likely to affect the SMKI SEC Documents. The Code Administrator shall comply with such process.

**Modification of the SMKI SEC Documents by the SMKI PMA**

L1.19   Notwithstanding Section D1.3 (Persons Entitled to Submit Modification Proposals):

(a)     the SMKI PMA shall be entitled to submit Modification Proposals in respect of the SMKI SEC Documents where the SMKI PMA considers it appropriate to do so; and

(b)     any SMKI PMA Member shall be entitled to submit Modification Proposals in respect of the SMKI SEC Documents where he or she considers it appropriate to do so (where the SMKI PMA has voted not to do so).

## L2    SMKI ASSURANCE

**SMKI Compliance Policy**

L2.1    The SMKI PMA shall exercise the functions allocated to it by the SMKI Compliance Policy.

L2.2    The DCC shall procure all such services as are required for the purposes of complying with its obligations under the SMKI Compliance Policy.

**SMKI Participants: Duty to Cooperate in Assessment**

L2.3    Each SMKI Participant shall do all such things as may be reasonably requested by the SMKI PMA, or by any person acting on behalf of or at the request of the SMKI PMA (including in particular the Independent SMKI Assurance Service Provider), for the purposes of facilitating an assessment of that SMKI Participant's compliance with any applicable requirements of the SMKI Document Set.

L2.4    For the purposes of Section L2.3, an SMKI Participant shall provide the SMKI PMA (or the relevant person acting on its behalf or at its request) with:

(a)     all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified; and

(b)     all such other forms of cooperation as may reasonably be requested, including in particular access at all reasonable times to:

(i)     such parts of the premises of that SMKI Participant as are used for; and

(ii)    such persons engaged by that SMKI Participant as carry out, or are authorised to carry out,

any activities related to its compliance with the applicable requirements of the SMKI Document Set.

**Events of Default**

L2.5    In relation to an Event of Default which consists of a material breach by an SMKI Participant of any applicable requirements of the SMKI Document Set, the provisions

of Sections M8.2 (Notification of an Event of Default) to M8.4 (Consequences of an Event of Default) shall apply subject to the provisions of Sections L2.6 to L2.13.

L2.6    For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section L2.5, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any applicable requirements of the SMKI Document Set (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

L2.7    Where in accordance with Section M8.2 the Panel receives notification that an SMKI Participant is in material breach of any applicable requirements of the SMKI Document Set, it shall refer the matter to the SMKI PMA. On any such referral, the SMKI PMA may investigate the matter in accordance with Section M8.3 as if the references in that Section to the "Panel" were to the "SMKI PMA".

L2.8    Where the SMKI PMA has:

(a)     carried out an investigation in accordance with Section M8.3; or

(b)     received a report from the Independent SMKI Assurance Service Provider, following an assessment by it of the compliance of any SMKI Participant with the applicable requirements of the SMKI Document Set, concluding that the SMKI Participant has not complied with those requirements,

the SMKI PMA shall consider the information available to it and shall determine whether any non-compliance with the SMKI Document Set has occurred and, if so, whether that non-compliance constitutes an Event of Default.

L2.9    Where the SMKI PMA determines that an Event of Default has occurred, it shall:

(a)     notify the relevant SMKI Participant and any other Party it considers may have been affected by the Event of Default; and

(b)     refer the matter to the Panel for the Panel to determine the appropriate steps to take in accordance with Section M8.4.

L2.10   Where the Panel is considering what steps to take in accordance with Section M8.4, it shall request and consider the advice of the SMKI PMA.

L2.11 Where the Panel determines that an SMKI Participant is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the SMKI PMA.

L2.12 Where, in accordance with Section L2.11, the SMKI PMA has approved a remedial action plan in relation to the provision by the DCC of the SMKI Services, the Panel shall ensure that the approved plan (being redacted only in so far as necessary for the purposes of security) is made available to all Parties.

L2.13 Where, in accordance with Section L2.11, the SMKI PMA has approved a remedial action plan in relation to:

(a)     the DCC acting in a capacity other than as the provider of the SMKI Services, the Panel may arrange for a version of the approved plan (or parts of that plan) to be made available to all the Parties; or

(b)     any other SMKI Participant, the Panel may arrange for an anonymised version of the approved plan (or parts of that plan) to be made available to all the Parties,

but (in each case) only where the Panel considers that such dissemination is necessary for the purposes of security.

**Emergency Suspension of SMKI Services**

L2.14 Where the SMKI PMA has reason to believe that there is any immediate threat of the DCC Total System, any User Systems, any Smart Metering Systems or any RDP Systems being Compromised to a material extent by the occurrence of an event arising in relation to the SMKI Services, it may instruct the DCC immediately to suspend:

(a)     the provision (in whole or in part) of the SMKI Services and/or any other Services which rely on the use of Certificates;

(b)     the rights of any SMKI Participant to receive (in whole or in part) the SMKI Services and/or any other Services which rely on the use of Certificates,

and thereafter to retain that suspension in effect until such time as the SMKI PMA instructs the DCC to reinstate the provision of the relevant Services or the rights of the SMKI Participant (as the case may be).

L2.15  Where the SMKI PMA takes any steps under Section L2.14, it:

    (a)      shall immediately thereafter notify the Authority;

    (b)      shall comply with any direction given to it by the Authority in relation to such steps; and

    (c)      may notify all the Parties of some or all of such steps (without identifying the SMKI Participant), but only where the Panel considers that such notification is necessary for the purposes of security.

L2.16  Any Party which is affected by the SMKI PMA taking any steps under Section L2.14 may appeal the decision to do so to the Authority, and the DCC shall comply with any decision of the Authority in respect of the matter (which shall be final and binding for the purposes of this Code).

## L3    THE SMKI SERVICES

**The SMKI Services**

L3.1   For the purposes of this Section L3, the "**SMKI Services**" means all of the activities undertaken by the DCC in its capacity as:

(a)    the Device Certification Authority;

(b)    the Organisation Certification Authority; or

(c)    the IKI Certification Authority,

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

**Authorised Subscribers**

General Provisions

L3.2    For the purposes of this Section L3:

(a)    any Party which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of any of the Certificate Policies;

(b)    any RDP which has successfully completed the SMKI and Repository Entry Process Tests for the purposes of Section H14.22(a) in respect of the Organisation Certificate Policy; and

(c)    SECCo in respect of the IKI Certificate Policy,

may apply to become an Authorised Subscriber in accordance with, and by following the relevant procedures set out in, that Certificate Policy and the SMKI RAPP.

L3.3   The DCC shall authorise SECCo, any Party or any RDP to submit a Certificate Signing Request, and so to become an Authorised Subscriber, where SECCo, that Party or that RDP has successfully completed the relevant procedures and satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP.

L3.4   The DCC shall provide any SMKI Services that may be requested by an Authorised Subscriber where the request is made by that Authorised Subscriber in accordance with

the applicable requirements of the SMKI SEC Documents.

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

Registration Data Providers

L3.6    Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become an Authorised Subscriber, the Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L.

L3.7    Where a Registration Data Provider has been nominated as such by more than one Network Party:

(a)     that RDP shall not, by virtue of acting in the capacity of an RDP for different Network Parties, be required to become a Subscriber for different Organisation Certificates;

(b)     to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP;

(c)     to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP.

Determinations by the Panel

L3.8    Where the DCC has notified SECCo, a Party or an RDP that has applied to become an Authorised Subscriber that the DCC does not consider that it has satisfied the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, SECCo, that Party or that RDP (as the case may be) may refer the matter to the Panel for determination.

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

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

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

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

L3.11 Nothing in Sections L3.8 to L3.10 shall be taken to prevent SECCo, any Party or any RDP from making a new application to DCC to become an Authorised Subscriber, in accordance with Section L3.2, at any time.

Changes in Circumstance

L3.12 Where a SECCo, any Party or any RDP which is an Authorised Subscriber becomes aware of a change in circumstance which would be likely, if it were to make a new application to the DCC to become an Authorised Subscriber, to affect whether it would satisfy the criteria set out in the relevant Certificate Policy and the SMKI RAPP for that purpose, it shall as soon as is reasonably practicable notify the DCC of that change in circumstance.

L3.13 Where the DCC receives a notification from an Authorised Subscriber in accordance with Section L3.12, or otherwise becomes aware of a change in circumstance of the nature referred to in that Section, it shall:

(a) assess whether that Authorised Subscriber continues to satisfy the relevant criteria to be an Authorised Subscriber as set out in the relevant Certificate Policy and the SMKI RAPP; and

(b) where it determines that the Party or RDP does not continue to satisfy the relevant criteria, notify the Authorised Subscriber which, subject to Section L3.14, shall cease to be an Authorised Subscriber in accordance with the Certificate Policy.

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

(a)    the provisions of Section L3.8 to L3.11 shall apply as if the person notified had made an unsuccessful application to become an Authorised Subscriber in respect of the relevant Certificate Policy; and

(b)    where the relevant Certificate Policy is the Organisation Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, revoke any Organisation Certificates for which that person is the Subscriber;

(c)    where the relevant Certificate Policy is the IKI Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, take such steps in relation to any IKI Certificates for which that person is the Subscriber as may be set out in that Certificate Policy or in the SMKI RAPP.

**Eligible Subscribers**

L3.15    An Authorised Subscriber:

(a)    shall be known as an "**Eligible Subscriber**" in respect of a Certificate if it is entitled to become a Subscriber for that Certificate; and

(b)    will be entitled to become a Subscriber for a Certificate only if it is identified as an Eligible Subscriber in respect of that Certificate in accordance with the following provisions of this Section L3.

Device Certificates

L3.16    A Party which is an Authorised Subscriber in accordance with the Device Certificate Policy will be an Eligible Subscriber in respect of a Device Certificate only where that Subject of that Device Certificate is one that is identified with that Party in the table immediately below.

| **Party** | **Subject** |
|---|---|
| The DCC | Either: |

| | |
|---|---|
| | (a)     a Communications Hub Function; or<br><br>(b)     a Gas Proxy Function. |
| An Import Supplier | Either:<br><br>(a)     an Electricity Smart Meter; or<br><br>(b)     a Type 1 Device. |
| A Gas Supplier | Either:<br><br>(a)     a Gas Smart Meter;<br><br>(b)     a Gas Proxy Function; or<br><br>(c)     a Type 1 Device. |
| Any other Party | Either:<br><br>(a)     an Electricity Smart Meter<br><br>(b)     a Gas Smart Meter; or<br><br>(c)     a Type 1 Device,<br><br>but only in so far as the SMI Status of that Device is not set to 'commissioned' or 'installed not commissioned'. |

DCA Certificates

L3.17  Where the DCC (acting in its capacity as Root DCA or Issuing DCA) is an Authorised Subscriber in accordance with the Device Certificate Policy:

(a)     it (and only it) will be an Eligible Subscriber in respect of DCA Certificates;

(b)     (save for the purposes of the replacement of the Root DCA Certificate) it will be an Eligible Subscriber only in respect of a single Root DCA Certificate.

Organisation Certificates

L3.18 Where the DCC, a Network Party or another Party which is (or is to become) a User, or any RDP, is an Authorised Subscriber in accordance with the Organisation Certificate Policy, that person will be an Eligible Subscriber in respect of an Organisation Certificate only where:

(a)    if the Subject of that Certificate is:

(i)    either the DCC (acting pursuant to its powers or duties under the Code) or a DCC Service Provider, that person is the DCC; or

(ii)    not the DCC, that person is the Subject of the Certificate; and

(b)    if the value of the OrganizationalUnitName field in that Certificate is a Remote Party Role corresponding to that listed in the table immediately below, either:

(i)    that person is the DCC, and the Remote Party Role is not one in relation to which a Device may require to undertake processing in accordance with the GB Companion Specification; or

(ii)    that person is identified with that Remote Party Role in the second column of that table, and the value of the subjectUniqueID field in the Certificate is a User ID or RDP ID associated with any such User Role or with an RDP as may be identified in the third column of that table.

| **Remote Party Role** | **Party** | **User Role or RDP** |
|---|---|---|
| Root | The DCC | [Not applicable] |
| Recovery | The DCC | [Not applicable] |
| Transitional CoS | The DCC | [Not applicable] |
| wanProvider | The DCC | [Not applicable] |
| Access Control Broker | The DCC | [Not applicable] |

| Issuing Authority | The DCC | [Not applicable] |
|---|---|---|
| networkOperator | A Network Party | Either:<br><br>(a)    Electricity Distributor; or<br>(b)    Gas Transporter. |
| supplier | A Supplier Party | Either:<br><br>(a)    Import Supplier; or<br>(b)    Gas Supplier. |
| other | An RDP or any Party other than the DCC | Either:<br><br>(a)    Other User;<br>(b)    Registered Supplier Agent;<br>(c)    Registration Data Provider; or<br>(d)    Export Supplier. |

OCA Certificates

L3.19 Where the DCC (acting in its capacity as Root OCA or Issuing OCA) is an Authorised Subscriber in accordance with the Organisation Certificate Policy:

(a)    it (and only it) will be an Eligible Subscriber in respect of OCA Certificates;

(b)    (save for the purposes of the replacement of the Root OCA Certificate) it will be an Eligible Subscriber only in respect of a single Root OCA Certificate.

IKI Certificates

L3.20 Where SECCo or any Party or RDP is an Authorised Subscriber in accordance with the IKI Certificate Policy, it will be an Eligible Subscriber in respect of an IKI Certificate in the circumstances set out in the IKI Certificate Policy.

ICA Certificates

L3.21 Where the DCC (acting in its capacity as Root ICA or Issuing ICA) is an Authorised Subscriber in accordance with the IKI Certificate Policy:

(a)     it (and only it) will be an Eligible Subscriber in respect of ICA Certificates;

(b)     (save for the purposes of the replacement of the Root ICA Certificate) it will be an Eligible Subscriber only in respect of a single Root ICA Certificate.

**Certificates for Commissioning of Devices**

L3.22   The DCC shall:

(a)     prior to the commencement of Interface Testing, or by such later date as may be specified by the Secretary of State, establish and lodge in the SMKI Repository; and

(b)     subsequently maintain,

such of its Certificates as are necessary to facilitate the installation at premises of Devices that are capable of being Commissioned.

L3.23   For the purposes of Section L3.22, the DCC shall ensure that the Certificates which are established, lodged in the SMKI Repository and subsequently maintained include at least the following:

(a)     the Root OCA Certificate;

(b)     the Issuing OCA Certificate;

(c)     the Root DCA Certificate;

(d)     the Issuing DCA Certificate;

(e)     the Recovery Certificate;

(f)     the DCC (Access Control Broker) - digitalSignature Certificate;

(g)     the DCC (Access Control Broker) – keyAgreement Certificate;

(h)     the DCC (wanProvider) Certificate; and

(i)     the DCC (transitionalCoS) Certificate.

L3.24   For the purposes of Sections L3.23(e) - (i), the Certificates which are referred to in those

paragraphs mean Organisation Certificates in respect of which, in each case:

(a)     the value of the KeyUsage field is that identified in relation to the Certificate in the second column of the table immediately below;

(b)     the value of the OrganizationalUnitName field corresponds to the Remote Party Role identified in relation to the Certificate in the third column of that table; and

(c)     the Certificate is used for the purposes of discharging the obligations of the DCC in the role identified in relation to it in the fourth column of that table.

| Certificate | KeyUsage Value | Remote Party Role | DCC Role |
|---|---|---|---|
| Recovery Certificate | digitalSignature | Recovery | The role of the DCC under the SMKI Recovery Procedure. |
| DCC (Access Control Broker) - digitalSignature Certificate | digitalSignature | AccessControlBroker | AccessControlBroker |
| DCC (Access Control Broker) – keyAgreement Certificate | KeyAgreement | AccessControlBroker | AccessControlBroker |
| DCC (wanProvider) Certificate | digitalSignature | wanProvider | wanProvider |
| DCC (transitionalCoS) Certificate | digitalSignature | Transitional CoS | The role of the DCC as CoS Party. |

**Definitions**

L3.25   For the purposes of this Section L3:

(a)     "**KeyUsage**" means the field referred to as such in the Organisation Certificate Policy;

(b)     "**OrganizationalUnitName**" and "**subjectUniqueID**" mean those fields which are identified as such in the Organisation Certificate Profile at Annex B of the Organisation Certificate Policy; and

(c)     "**AccessControlBroker**" and "**wanProvider**", when used in relation to the roles of the DCC, mean those roles which are identified as such, and have the meanings given to them, in the GB Companion Specification.

**L4**     **THE SMKI SERVICE INTERFACE**

**DCC: Obligation to Maintain the SMKI Service Interface**

L4.1     The DCC shall maintain the SMKI Service Interface in accordance with the SMKI Interface Design Specification and make it available, for sending and receiving communications in accordance with the SMKI Code of Connection, via DCC Gateway Connections, to:

(a)     Authorised Subscribers; and

(b)     (where applicable) Parties for the purpose of undertaking SMKI Entry Process Testing.

L4.2     The DCC shall ensure that the SMKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a)     from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and

(b)     prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing.

**The SMKI Service Interface**

L4.3     For the purposes of this Section L4, the "**SMKI Service Interface**" means a communications interface designed to allow communications to be sent between an Authorised Subscriber and the DCC for the purposes of the SMKI Services.

**SMKI Interface Design Specification**

L4.4     For the purposes of this Section L4, the "**SMKI Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a)     shall specify the technical details of the SMKI Service Interface;

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

(c)     shall base those technical standards on PKIX/IETF/PKCS open standards,

where:

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

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

(iii)   PKCS is the Public Key Cryptography Standard;

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

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

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

(e)     may specify limits on the use of the SMKI Service Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent.

**SMKI Code of Connection**

L4.5    For the purposes of this Section L4, the "**SMKI Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a)     sets out the way in which an Authorised Subscriber may access the SMKI Service Interface;

(b)     may specify limits on the use of the SMKI Service Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent

(c)     specifies the procedure by which an Authorised Subscriber and the DCC may

communicate over the SMKI Service Interface; and

(d)    includes a description of the way in which the mutual authentication and protection of communications taking place over the SMKI Service Interface will operate.

**SMKI Interface Document Development**

L4.6    The DCC shall develop drafts of the SMKI Interface Design Specification and SMKI Code of Connection:

(a)    in accordance with the process set out at Section L4.7; and

(b)    so that the drafts are available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L4.7    The process set out in this Section L4.7 for the development of drafts of the SMKI Interface Design Specification and SMKI Code of Connection is that:

(a)    the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of each document;

(b)    where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c)    the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i)    a statement of the reasons why the DCC considers that draft document to be fit for purpose;

(ii)    copies of the consultation responses received; and

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

(d)     the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

   (i)     any requirement to produce and submit to the Secretary of State a further draft of either document; and

   (ii)    any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

**L5**    **THE SMKI REPOSITORY SERVICE**

**The SMKI Repository**

L5.1    For the purposes of this Section L5, the "**SMKI Repository**" means a System for storing and (subject to the provisions of this Section) making available copies of the following:

(a)    all Device Certificates;

(b)    all DCA Certificates;

(c)    all Organisation Certificates;

(d)    all OCA Certificates;

(e)    the IKI Certificates (to the extent required by the SMKI RAPP);

(f)    any other IKI Certificates, and any ICA Certificates, which the DCC may from time to time consider appropriate;

(g)    all versions of the Device Certificate Policy;

(h)    all versions of the Organisation Certificate Policy;

(i)    all versions of the IKI Certificate Policy;

(j)    all versions of the SMKI RAPP;

(k)    all versions of the SMKI Recovery Procedure;

(l)    all versions of the SMKI Compliance Policy;

(m)    the latest version of the Organisation CRL;

(n)    the latest version of the Organisation ARL;

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

(p)    such other documents or information as the DCC, in its capacity as the provider

of the SMKI Services, may from time to time consider appropriate.

**The SMKI Repository Service**

L5.2    The DCC shall establish, operate, maintain and make available the SMKI Repository in accordance with the provisions of this Section L5 (the "**SMKI Repository Service**").

L5.3    The DCC shall ensure that the documents and information described in Section L5.1 may be lodged in the SMKI Repository:

(a)    by itself, for the purpose of providing the SMKI Services or complying with any other requirements placed on it under the Code; and

(b)    (except in the case of Certificates, the CRL and the ARL) by the SMKI PMA, or by the Code Administrator acting on its behalf, for the purpose of fulfilling its functions under the Code.

L5.4    The DCC shall ensure that no person may lodge documents or information in the SMKI Repository other than in accordance with Section L5.3.

L5.5    The DCC shall ensure that the SMKI Repository may be accessed for the purpose of viewing and/or obtaining a copy of any document or information stored on it by:

(a)    any Party or RDP which reasonably requires such access in accordance, or for any purpose associated, with the Code;

(b)    the Panel (or the Code Administrator acting on its behalf); and

(c)    the SMKI PMA (or the Code Administrator acting on its behalf).

L5.6    The DCC shall ensure that no person may access documents or information in the SMKI Repository other than in accordance with Section L5.5.

**SMKI PMA: Role in relation to the SMKI Repository**

L5.7    The SMKI PMA shall lodge each of the following documents in the SMKI Repository promptly upon the SMKI Repository Service first becoming available or (if later) the incorporation of that document into the Code:

(a)     the Device Certificate Policy;

(b)     the Organisation Certificate Policy;

(c)     the IKI Certificate Policy; and

(d)     the SMKI Compliance Policy.

L5.8    The SMKI PMA shall lodge in the SMKI Repository the modified version of each document referred to in Section L5.7 promptly upon any modification being made to that document in accordance with the Code.

L5.9    The SMKI PMA may require the DCC to lodge in the SMKI Repository such other documents or information as it may from time to time direct.

L5.10   Subject to Section L5.3, the SMKI PMA may lodge in the SMKI Repository such other documents or information as it may from time to time consider appropriate.

**Parties: Duties in relation to the SMKI Repository**

L5.11   Neither any Party nor RDP, or the SMKI PMA, may access the SMKI Repository for the purpose of viewing and/or obtaining a copy of any document or information stored on it except to the extent that it reasonably requires such access in accordance, or for any purpose associated, with the Code.

**L6** **THE SMKI REPOSITORY INTERFACE**

**DCC: Obligation to Maintain the SMKI Repository Interface**

L6.1 The DCC shall maintain the SMKI Repository Interface in accordance with the SMKI Repository Interface Design Specification and make it available, via DCC Gateway Connections, to:

(a) the Parties and RDPs;

(b) the Panel (or the Code Administrator on its behalf); and

(c) the SMKI PMA (or the Code Administrator on its behalf),

to send and receive communications in accordance with the SMKI Repository Code of Connection and (where applicable) for the purpose of SMKI Entry Process Testing.

L6.2 The DCC shall ensure that the SMKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the SMKI Services in accordance with Section L3 (The SMKI Services); and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating SMKI Entry Process Testing.

**The SMKI Repository Interface**

L6.3 For the purposes of this Section L6, the "**SMKI Repository Interface**" means a communications interface designed to allow communications to be sent from and received by the SMKI Repository for the purposes of the SMKI Repository Service.

**SMKI Repository Interface Design Specification**

L6.4 For the purposes of this Section L6, the "**SMKI Repository Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the SMKI Repository Interface; and

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

Repository Interface.

**SMKI Repository Code of Connection**

L6.5    For the purposes of this Section L6, the "**SMKI Repository Code of Connection**" shall be a SEC Subsidiary Document of that name which:

(a)     sets out the way in which the Parties and RDPs, the Panel and the SMKI PMA may access the SMKI Repository Interface;

(b)     may specify limits on the use of the SMKI Repository Interface, including in particular limits on the time or extent of its use, or conditions which must be satisfied for the purposes of its use at a specified time or to a specified extent;

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

(d)     includes a description of the way in which the authentication and protection of communications taking place over the SMKI Repository Interface will operate.

**SMKI Repository Interface Document Development**

L6.6    The DCC shall develop drafts of the SMKI Repository Interface Design Specification and SMKI Repository Code of Connection:

(a)     in accordance with the process set out at Section L6.7; and

(b)     so that the drafts are available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L6.7    The process set out in this Section L6.7 for the development of drafts of the SMKI Repository Interface Design Specification and SMKI Repository Code of Connection is that:

(a)     the DCC shall, in consultation with the Parties and such other persons as it considers appropriate, produce a draft of each document;

(b)     where a disagreement arises with any person who is consulted with regard to

SEC – Section L

any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c)     the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

   (i)     a statement of the reasons why the DCC considers that draft document to be fit for purpose;

   (ii)    copies of the consultation responses received; and

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

(d)     the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either document, including in particular:

   (i)     any requirement to produce and submit to the Secretary of State a further draft of either document; and

   (ii)    any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

**L7**   **SMKI AND REPOSITORY ENTRY PROCESS TESTS**

**Eligibility Generally**

L7.1   A Party or RDP shall not be entitled to:

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

(b)   access the SMKI Repository,

until that Party or RDP has successfully completed the SMKI and Repository Entry Process Tests for the purposes of paragraph (a) or (b) above (as applicable).

L7.2   Only persons that are Parties or RDPs are eligible to complete the SMKI and Repository Entry Process Tests.

**SMKI and Repository Entry Guide**

L7.3   The DCC shall establish and arrange for the publication on the Website of a guide to the SMKI and Repository Entry Process Tests, which shall identify any information that a Party or RDP is required to provide in support of its application to complete the SMKI and Repository Entry Process Tests (whether for the purposes of Section L7.1(a) or (b) or both).

**SMKI and Repository Entry Process Tests**

L7.4   A Party or RDP that wishes to complete the SMKI and Repository Entry Process Tests (whether for the purposes of Section L7.1(a) or (b) or both) must apply to the DCC in compliance with any requirements identified in the guide referred to in Section L7.3.

L7.5   On receipt of an application from a Party or RDP pursuant to Section L7.4, the DCC shall process that Party's or RDP's application to complete the SMKI and Repository Entry Process Tests in accordance with this Section L7.

**SMKI and Repository Entry Process Test Requirements**

L7.6   A Party or RDP wishing to:

(a)     become an Authorised Subscriber for the purposes of any Certificate Policy must have successfully completed the SMKI and Repository Entry Process Tests for that purpose; or

(b)     access the SMKI Repository must have successfully completed the SMKI and Repository Entry Process Tests for that purpose.

L7.7    A Party or RDP will have successfully completed the SMKI and Repository Entry Process Tests for a particular purpose once that Party or RDP has received confirmation from the DCC that it has met the relevant requirements of Section L7.6.

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

**Network Parties and RDPs**

L7.9    Each Network Party shall ensure that its Registration Data Provider (being the Network Party itself where that is deemed to be the case in accordance with the definition of Registration Data Provider) shall, when acting in its capacity as the Network Party's RDP to undertake the SMKI and Repository Entry Process Tests, comply with the obligations expressed to be placed on RDPs under Section H14 (Testing Services) and the SMKI and Repository Test Scenarios Document.

L7.10   Where more than one Network Party nominates the same Registration Data Provider, each of those Network Parties shall be jointly and severally liable for any failure by that RDP, when acting in its capacity as the Network Parties' RDP to undertake the SMKI and Repository Entry Process Tests, to comply with any of the obligations expressed to be placed on RDPs under Section H14 (Testing Services) and the SMKI and Repository Test Scenarios Document.

## L8    SMKI PERFORMANCE STANDARDS AND DEMAND MANAGEMENT

**SMKI Services: Target Response Times**

L8.1    The DCC shall undertake the following activities within the following time periods (each such time period being, in respect of each such activity, the "**Target Response Time**" for that activity):

(a)    in response to a single Certificate Signing Request, sending to an Eligible Subscriber either an Organisation Certificate or Device Certificate within 30 seconds of receipt of the Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface; and

(b)    in response to a Batched Certificate Signing Request, sending to an Eligible Subscriber the number of Device Certificates that were requested:

(i)    where the receipt of the Batched Certificate Signing Request from that Eligible Subscriber over the SMKI Service Interface occurred between the hours of 08:00 and 20:00 on any day, by no later than 08:00 on the following day; or

(ii)    where the receipt of the Batched Certificate Signing Request from that Eligible Supplier over the SMKI Service Interface did not occur between the hours of 08:00 and 20:00, within 24 hours of the time of that receipt.

L8.2    For the purposes of Section L8.1, a "**Batched Certificate Signing Request**" is a single communication containing Certificate Signing Requests for the Issue of more than one but no more than 50,000 Device Certificates.

L8.3    For the purposes of Section L8.1, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Interface Design Specification.

**SMKI Repository Service: Target Response Time**

L8.4    The DCC shall send to a Party, an RDP, the Panel or the SMKI PMA (as the case may be) a copy of any document or information stored on the SMKI Repository within 3 seconds of receipt of a request for that document from that person or body over the

SMKI Repository Interface (and that time period shall be the "**Target Response Time**" for that activity).

L8.5 For the purposes of Section L8.4, the concepts of 'sending' and 'receipt' are to be interpreted in accordance with the explanation of those concepts in the SMKI Repository Interface Design Specification.

**Code Performance Measures**

L8.6 Each of the following performance measures constitute a Code Performance Measure (to which the following Target Service Level and Minimum Service Level will apply, measured over the following Performance Measurement Period):

| No. | Code Performance Measure | Performance Measurement Period | Target Service Level | Minimum Service Level |
|-----|--------------------------|-------------------------------|---------------------|----------------------|
| 7 | Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services. | monthly | 99% | 96% |
| 8 | Percentage of documents stored on the SMKI Repository delivered within the applicable Target Response Time for the SMKI Repository Service. | monthly | 99% | 96% |

**SMKI Services: Managing Demand**

L8.7 Each Party which is an Authorised Subscriber in accordance with the Device Certificate Policy shall:

(a) as soon as reasonably practicable after becoming an Authorised Subscriber; and

(b) subsequently by the 15th Working Day of the months of March, June, September and December in each year,

provide the DCC with a forecast of the number of Certificate Signing Requests that the Authorised Subscriber will send in each of the 8 months following the end of the month in which such forecast is provided. Such forecast shall contain a breakdown of the total

number of Certificate Signing Requests in respect of Device Certificates between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests.

L8.8 The DCC shall monitor and record the aggregate number of Certificate Signing Requests sent by each Authorised Subscriber in total.

L8.9 By no later than the 10th Working Day following the end of each month, the DCC shall provide:

(a) each Authorised Subscriber with a report that sets out the number of Certificate Signing Requests sent by that Authorised Subscriber in respect of Device Certificates during that month (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers sent against the numbers most recently forecast for the applicable month; and

(b) (in so far as there were one or more Parties or RDPs which were Authorised Subscribers during the applicable month) a report to the Panel that sets out:

(i) the aggregate number of Certificate Signing Requests in respect of Device Certificates sent by all Authorised Subscribers collectively during that month (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched Certificate Signing Requests), and comparing the actual numbers for that month sent against the numbers most recently forecast for the applicable month; and

(ii) where the number of Certificate Signing Requests in respect of Device Certificates sent by any Authorised Subscriber during that month is greater than or equal to 110% of the Authorised Subscriber's most recent monthly forecast for the applicable month, the identity of each such Authorised Subscriber and the number of Certificate Signing Requests in respect of Device Certificates sent by each such Authorised Subscriber (in total and broken down between those which request the Issue of a single Device Certificate and those which are Batched

Certificate Signing Requests)

L8.10　The Panel shall publish each report provided to it pursuant to Section L8.9(b) on the Website, save that the Panel may decide not to publish one or more parts of a report concerning under-forecasting as referred to in Section L8.9(b)(ii) where the Panel considers that the under-forecasting was reasonable in the circumstances (including where it arose as a result of matters beyond the Authorised Subscriber's reasonable control).

L8.11　The DCC shall, as soon as is reasonably practicable, submit a Modification Proposal containing rules that it considers appropriate to enable the prioritisation by the DCC of Certificate Signing Requests in respect of Device Certificates sent over the SMKI Service Interface in circumstances in which the aggregate demand for the Issue of Device Certificates cannot be satisfied within the applicable Target Response Times.

L8.12　The DCC shall not be considered to be in breach of this Code with regard to the obligation to achieve the Target Response Times set out at Section L8.1 if, during the month in question, the aggregate Certificate Signing Requests in respect of Device Certificates sent by all Authorised Subscribers exceeds 110% of the aggregate demand most recently forecast for that month by all Authorised Subscribers pursuant to Section L8.7 (provided that the DCC shall nevertheless in such circumstances take reasonable steps  to achieve the Target Response Times).

**L9** **THE SMKI DOCUMENT SET**

**Obligations on the SMKI PMA**

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

**Obligations on SMKI Participants**

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

**The SMKI Document Set**

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

(a)     the SMKI SEC Documents;

(b)     the Device CPS;

(c)     the Organisation CPS; and

(d)     the IKI CPS.

**The SMKI SEC Documents**

L9.4 For the purposes of this Section L, the "**SMKI SEC Documents**" means the provisions of the Code comprising:

(a)     the following SEC Subsidiary Documents:

(i)      the Device Certificate Policy;

(ii)     the Organisation Certificate Policy;

(iii)    the IKI Certificate Policy;

(iv)     the SMKI Compliance Policy;

(v)      the SMKI RAPP;

(vi)     the SMKI Recovery Procedure;

(vii)    the SMKI Interface Design Specification;

(viii)   the SMKI Code of Connection;

(ix)     the SMKI Repository Interface Design Specification;

(x)      the SMKI Repository Code of Connection;

(xi)     the SMKI and Repository Test Scenarios Document

(b)     the provisions of Sections L1 to L12; and

(c)     every other provision of the Code which relates to the provision or the use of the SMKI Services or the SMKI Repository Service or to any matters directly arising from or affecting the provision or the use of those Services.

**The Registration Authority Policies and Procedures: Document Development**

L9.5    The DCC shall develop a draft of the SMKI RAPP:

(a)     to make provision for such matters as are specified in the Certificate Policies as being matters provided for in the SMKI RAPP;

(b)     to make provision for such other matters as are necessary or appropriate in relation to the exercise of its functions as the Registration Authority;

(c)     to make provision for such matters as are necessary or appropriate in relation to Test Certificates that are being made available to Testing Participants;

(d)     to make such provision as the DCC may consider appropriate in relation to the means by which the identity and authorisation of individuals and Parties may be verified for the purposes of the DCCKI Services (in addition to any such provision made in respect of the SMKI Services);

(e)     in accordance with the process set out at Section L9.6; and

(f)     so that the draft is available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L9.6    The process set out in this Section L9.6 for the development of a draft of the SMKI RAPP is that:

(a)     the DCC shall, in consultation with the Parties and such other persons as it

considers appropriate, produce a draft of the SMKI RAPP;

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

(c)     the DCC shall send a draft of the SMKI RAPP to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i)      a statement of the reasons why the DCC considers that draft to be fit for purpose; and

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

(d)     the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the SMKI RAPP, including in particular:

(i)      any requirement to produce and submit to the Secretary of State a further draft of the document; and

(ii)     any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

**The Device Certification Practice Statement**

L9.7    The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**Device CPS**".

L9.8    The Device CPS shall be a document which:

(a)     sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the Device Certificate Policy;

(b)     incorporates the detailed operating procedures to be used by the DCC for the

purposes of its compliance with the requirements of that Policy;

(c)     incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d)     is approved by the SMKI PMA as appropriate for these purposes.

L9.9    For the purposes of the approval of the Device CPS by the SMKI PMA in accordance with Section L9.8(d):

(a)     the DCC shall submit an initial draft of the Device CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b)     the SKMI PMA shall review the initial draft of the Device CPS and shall:

(i)      approve the draft, which shall become the Device CPS; or

(ii)     state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c)     the DCC shall make any amendments to the draft Device CPS that may be directed by the SMKI PMA, and the amended draft shall become the Device CPS.

L9.10   The DCC shall keep the Device CPS under review, and shall in particular carry out a review of the Device CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.11   Following any review of the Device CPS:

(a)     the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b)     those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.12   Both the DCC and the SMKI PMA shall treat the Device CPS as confidential.

**The Organisation Certification Practice Statement**

L9.13 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**Organisation CPS**".

L9.14 The Organisation CPS shall be a document which:

(a) sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the Organisation Certificate Policy;

(b) incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c) incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d) is approved by the SMKI PMA as appropriate for these purposes.

L9.15 For the purposes of the approval of the Organisation CPS by the SMKI PMA in accordance with Section L9.14(d):

(a) the DCC shall submit an initial draft of the Organisation CPS to the SMKI PMA by no later than the date which falls three months prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b) the SKMI PMA shall review the initial draft of the Organisation CPS and shall:

(i) approve the draft, which shall become the Organisation CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft Organisation CPS that may be directed by the SMKI PMA, and the amended draft shall become the Organisation CPS.

L9.16 The DCC shall keep the Organisation CPS under review, and shall in particular carry out a review of the Organisation CPS whenever (and to the extent to which) it may be

required to so by the SMKI PMA.

L9.17 Following any review of the Organisation CPS:

(a)     the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b)     those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.18 Both the DCC and the SMKI PMA shall treat the Organisation CPS as confidential.

**The IKI Certification Practice Statement**

L9.19 The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**IKI CPS**".

L9.20 The IKI CPS shall be a document which:

(a)     sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the IKI Certificate Policy;

(b)     incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c)     incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code; and

(d)     is approved by the SMKI PMA as appropriate for these purposes.

L9.21 For the purposes of the approval of the IKI CPS by the SMKI PMA in accordance with Section L9.20(d):

(a)     the DCC shall submit an initial draft of the IKI CPS to the SMKI PMA by no later than the date which falls one month prior to the commencement of Systems Integration Testing or such later date as may be agreed by the SMKI PMA;

(b)     the SMKI PMA shall review the initial draft of the IKI CPS and shall:

(i)     approve the draft, which shall become the IKI CPS; or

(ii) state that it will approve the draft subject to the DCC first making such amendments to the document as it may direct; and

(c) the DCC shall make any amendments to the draft IKI CPS that may be directed by the SMKI PMA, and the amended draft shall become the IKI CPS.

L9.22 The DCC shall keep the IKI CPS under review, and shall in particular carry out a review of the IKI CPS whenever (and to the extent to which) it may be required to so by the SMKI PMA.

L9.23 Following any review of the IKI CPS:

(a) the DCC may propose amendments to it, which it shall submit to the SMKI PMA for its approval; and

(b) those amendments may be made only to the extent to which the SMKI PMA has approved them.

L9.24 Both the DCC and the SMKI PMA shall treat the IKI CPS as confidential.

**Enquiries in relation to the SMKI Document Set**

L9.25 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party or RDP in relation to the SMKI Services, the SMKI Repository Services or the SMKI Document Set, but excluding any request for a copy of any document or information which can be accessed through the SMKI Repository.

**L10**   **THE SMKI RECOVERY PROCEDURE**

**The SMKI Recovery Procedure**

L10.1   For the purposes of this Section L10, the "**SMKI Recovery Procedure**" shall be a SEC Subsidiary Document of that name which sets out, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised:

(a)   the mechanism by which Parties and RDPs may notify the DCC and the DCC may notify Parties, RDPs and the SMKI PMA that the Relevant Private Key has been (or is suspected of having been) Compromised;

(b)   procedures relating to the use of the Recovery Private Key and Contingency Private Key (including the use of the Symmetric Key) where such use has been required in accordance with a decision of the SMKI PMA;

(c)   procedures relating to:

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

(ii)   the coordination of the submission of Certificate Signing Requests by Eligible Subscribers following the replacement of any OCA Certificate;

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

(i)   notification of the Compromise (or suspected Compromise); and

(ii)   the process for taking steps to avoid or mitigate the adverse effects of, or to recover from, the (actual or suspected) Compromise, which steps may differ depending on the Relevant Private Key that has been (or is suspected of having been) Compromised and the nature and extent of the (actual or suspected) Compromise and the adverse effects arising from it; and

(e)   arrangements to be made preparatory to and for the purpose of ensuring the

effective operation of the matters described in paragraphs (a) to (d), and the associated technical solutions employed by the DCC, including for their periodic testing.

L10.2  The SMKI Recovery Procedure:

(a)     shall make provision for the use of the Recovery Private Key and Contingency Private Key (including the use of the Symmetric Key) only where such use has been required in accordance with a decision of the SMKI PMA;

(b)     shall make provision for the DCC, if it has reason to believe that the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key) is likely to be required by the SMKI PMA, to take or instruct any Party, any SMKI PMA Member or any Panel Member to take such preparatory steps in respect of that use as it considers appropriate; and

(c)     may make provision:

(i)      that, in specified circumstances, certain requirements of the SMKI Recovery Procedure, or of decisions made under and in accordance with the provisions of the SMKI Recovery Procedure, may take precedence over the other provisions of the Code;

(ii)     for the operation of procedures which, in specified circumstances, require that decisions over whether or not to take certain steps are referred to the SMKI PMA for its determination;

(iii)    for the SMKI PMA to require any Party to nominate individuals for the purpose of performing specified tasks.

L10.3  Where the DCC follows any of the procedures specified in the SMKI Recovery Procedure, it shall, as soon as is reasonably practicable, notify the SMKI PMA of the steps that it has taken and provide such additional supporting information as the SMKI PMA reasonably requests.

**SMKI Recovery Procedure: Obligations**

L10.4  The DCC, each Party, the SMKI PMA (and SMKI PMA Members) and the Panel (and

Panel Members) shall comply, in so far as applicable to it (or them), with any requirements set out in the SMKI Recovery Procedure.

L10.5    Any SMKI PMA Member or Panel Member who is appointed by (respectively) the SMKI PMA or Panel to carry out a specific role in respect of the SMKI Recovery Procedure must take reasonable steps to act in accordance with any instructions given to him by the SMKI PMA or Panel (as the case may be) in relation to the way in which that role is to be carried out.

L10.6    The DCC shall reimburse the reasonable costs of any Party which that Party can demonstrate were incurred by it solely and directly in consequence of actions taken by it to support the maintenance of the procedures and arrangements set out in the SMKI Recovery Procedure, and which it would not otherwise have incurred.

**SMKI Recovery Procedure: Document Development**

L10.7    The DCC shall develop a draft of the SMKI Recovery Procedure:

(a)       in accordance with the process set out at Section L10.8; and

(b)       so that the draft is available by no later than the date which falls six months prior to the commencement of Systems Integration Testing or such later date as may be specified by the Secretary of State.

L10.8    The process set out in this Section L10.8 for the development of a draft of the SMKI Recovery Procedure is that:

(a)       the DCC shall, in consultation with the Parties, the SMKI PMA and such other persons as it considers appropriate, produce a draft of the SMKI Recovery Procedure;

(b)       where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the SMKI Recovery Procedure, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the SMKI Recovery Procedure specified in Section L10.1;

(c)       the DCC shall send a draft of the SMKI Recovery Procedure to the Secretary of State as soon as is practicable after it is produced, and shall when doing so

provide to the Secretary of State:

    (i)      a statement of the reasons why the DCC considers that draft to be fit for purpose; and

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

(d)    the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the SMKI Recovery Procedure, including in particular:

    (i)      any requirement to produce and submit to the Secretary of State a further draft of the document; and

    (ii)     any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

**The SMKI Recovery Key Guidance**

L10.9  For the purposes of this Section L10, the "**SMKI Recovery Key Guidance**" shall be a document of that name which makes such provision as is appropriate, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, for any one or more of the following:

(a)    any factors which shall be taken into account by the SMKI PMA in deciding whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key);

(b)    any other factors which may in particular be taken into account by the SMKI PMA for the purposes of that decision;

(c)    any weighting or order of priority which shall, or may, be given by the SMKI PMA to any of the factors referred to in paragraphs (a) and (b); and

(d)    any criteria that are to be applied by the SMKI PMA, any approach that is to be followed by it, or any steps that are to be taken by it, prior to making a decision

whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key).

**Recovery Key Guidance: Obligations**

L10.10 The SMKI PMA:

(a)    shall act in accordance with the SMKI Recovery Key Guidance in making any decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key); and

(b)    may request such information and assistance from the DCC, the Security Sub-Committee or any Party as it reasonably considers appropriate for the purposes of making any such decision or ensuring that it will be prepared to make any such decision that may fall to be made by it at a future date.

L10.11 The DCC, each other Party, and the Security Sub-Committee shall promptly provide the SMKI PMA with such information and assistance as may be requested in accordance with Section L10.10.

L10.12 The DCC shall, where requested to do so, reimburse the reasonable costs of any Party associated with the provision of assistance in accordance with Section L10.11.

**Recovery Key Guidance: Document Development**

L10.13 The SMKI PMA shall:

(a)    develop the SMKI Recovery Key Guidance, and for that purpose:

(i)    consult with the DCC, the Security Sub-Committee, the Parties, the Secretary of State and the Authority; and

(ii)    have regard to the views of each person consulted by it prior to determining the content of the document;

(b)    periodically review the SMKI Recovery Key Guidance, and in particular carry out a review whenever (and to the extent to which) it may be required to do so by the Panel or the Authority;

(c)     where, following any review, it proposes to amend the SMKI Recovery Key Guidance:

      (i)     consult the DCC, the Security Sub-Committee, the Parties and the Authority in relation to the proposed amendments; and

      (ii)    have regard to the views of each person consulted by it prior to making any amendments to the document; and

(d)     publish the SMKI Recovery Key Guidance, as initially determined by it and on each amendment made to that document from time to time.

**Recovery Events and Recovery Costs**

Recovery Events

L10.14 For the purposes of this Section L10, a "**Recovery Event**" is an event that shall be taken to have occurred when the circumstances described in either Section L10.15 or L10.16 exist.

L10.15 The circumstances described in this Section L10.15 are that:

(a)     the DCC has notified the SMKI PMA that a Relevant Private Key has been (or is suspected of having been) Compromised; and

(b)     in consequence of that (actual or suspected) Compromise, the SMKI PMA has decided to require the use of the Recovery Private Key or Contingency Private Key (including the use of the Symmetric Key) in accordance with the SMKI Recovery Procedure.

L10.16 The circumstances described in this Section L10.16 are that:

(a)     the DCC has notified the SMKI PMA that a Relevant Private Key has been (or is suspected of having been) Compromised;

(b)     the SMKI PMA has been provided with (or otherwise obtained) evidence that:

      (i)     attempts have been made, by means of sending appropriate Commands, to replace the Data comprising part of the Device Security Credentials

of Relevant Devices which derive from any Organisation Certificate or OCA Certificate which is (or is suspected of being) Compromised; or

(ii) it was not feasible or appropriate for any such attempt to be made; and

(c) the SMKI PMA has decided not to require the use of the Recovery Private Key or Contingency Private Key (including the Symmetric Key).

Recovery Costs

L10.17 For the purposes of this Section L10, the "**Recovery Costs**" shall be such costs as are reasonably incurred in consequence of a Recovery Event (and which would not otherwise have incurred) by any Party:

(a) in respect of the use of the Recovery Private Key or Contingency Private Key (including the use of the Symmetric Key) in accordance with the requirement of the SMKI PMA; and

(b) in taking such action as is necessary, where the Recovery Private Key or Contingency Private Key (including the Symmetric Key) has not been used or has been used unsuccessfully, to replace:

(i) Relevant Devices for which that Party is the Responsible Supplier; or

(ii) the Data comprising part of the Device Security Credentials of such Relevant Devices which derive from any Organisation Certificate or OCA Certificate which is (or is suspected of being) Compromised.

Payment of Recovery Costs by the DCC

L10.18 Where any Party incurs Recovery Costs, it may submit to the DCC a request to be recompensed in respect of those costs.

L10.19 Where any Party wishes to submit a request in accordance with Section L10.18, it shall:

(a) within three months of the Recovery Event, notify the DCC of its intention to do so;

(b) unless, at the same time as notifying the DCC of that intention it also notifies

the DCC of the total amount of the costs in respect of which it requests to be recompensed:

(i)     provide to the DCC at that time its best estimate of the likely amount of those costs; and

(ii)    at least once in every subsequent period of three months, until such time as it notifies the DCC of the total amount of the costs in respect of which it requests to be recompensed, provide to the DCC an updated best estimate of the likely amount of those costs; and

(c)     as soon as possible, and in any event within three months of the date on which it ceases to incur Recovery Costs, notify the DCC of the total amount of the costs in respect of which it requests to be recompensed.

L10.20 A Party giving notice to the DCC in accordance with Section L10.19 shall:

(a)     subject to paragraph (b), provide to the DCC such evidence in respect of the amount of the Recovery Costs incurred by that Party:

(i)     as the DCC may reasonably require;

(ii)    by such dates as the DCC may reasonably specify; or

(b)     where the Panel considers the matter either of its own motion or on a referral by the Party or the DCC, provide to the DCC such evidence relating to the amount of the costs incurred by that Party:

(i)     as the Panel may determine is reasonably required;

(ii)    by such dates as the Panel may reasonably specify.

L10.21 The evidence referred to in Section L10.20 may include in particular, if the DCC or the Panel (as the case may be) determines that it is reasonably required, the report of an independent auditor verifying that the amount requested by a Party represents a fair and accurate statement of the Recovery Costs incurred by that Party.

L10.22 On receipt by it of a request from a Party to be recompensed in respect of Recovery Costs, the DCC shall, where it is satisfied that the amount of the costs requested by that

Party is adequately supported by the evidence provided to it in accordance with Section L10.20, pay to the Party that amount.

L10.23 Where the DCC has any question whether the evidence provided to it by a Party is adequate to support the amount of the costs requested:

(a)     it shall refer that question to the Panel for its determination; and

(b)     the Panel shall determine that question by directing that the DCC shall pay to the Party the full amount requested or only part of that amount (in a sum that is specified by the Panel), or shall make no payment to that Party.

L10.24 Where the amount of the Recovery Costs requested by any Party is (whether alone or taken together with amounts requested by any other Parties in relation to the same Recovery Event) for a sum exceeding that which is determined from time to time by the Panel, following consultation with the Parties and the Authority, for the purposes of this Section L10.24:

(a)     the DCC may refer to the Panel, for its determination, the question of the dates on which the payments of the amounts requested shall be made;

(b)     the Panel shall determine the dates on which those payments shall be made, and may in particular determine that:

(i)      different Parties shall be paid at different times; and

(ii)     any amount which is to be paid to a Party shall be paid in instalments at different times; and

(c)     the Panel shall consider whether to make any Modification Proposal in relation to the Charging Methodology (taking into account whether it is proposed by the Authority to make any adjustment to the allowable revenues of the DCC, or by the DCC to amend the Charging Statement).

Breach of the Code by the Relevant Subscriber

L10.25 Where a Recovery Event occurs, and where the Relevant Subscriber is the DCC, the DCC shall be deemed to be in breach of:

(a)     where the (actual or suspected) Compromise is to an Organisation Certificate, Section L11.9 (Organisation and IKI Certificates: Protection of Private Keys); or

(b)     where the (actual or suspected) Compromise is to an OCA Certificate, Part 6.2.1 of the Organisation Certificate Policy (Cryptographic Module Standards and Controls).

L10.26  Where a Recovery Event occurs, and where the Relevant Subscriber is any Party other than the DCC, that Party shall be deemed to be in breach of Section L11.9 (Organisation and IKI Certificates: Protection of Private Keys), unless the (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event was due to the (actual or suspected) Compromise of an OCA Certificate.

L10.27  Where a Relevant Subscriber is, by virtue of Section L10.25 or L10.26, deemed to be in breach of a provision of this Code, it shall cease to be so deemed (and no such breach shall be treated as having occurred) where:

(a)     within three months of the date of the Recovery Event it refers the matter to the Panel;

(b)     following that referral it demonstrates to the reasonable satisfaction of the Panel, that the (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event was not due to its breach of Section L11.9 or of Part 6.2.1 of the Organisation Certificate Policy (as the case may be); and

(c)     the Panel determines accordingly that no such breach occurred.

L10.28  In all circumstances other than those described in Section L10.27, and subject to the provisions of Section L10.29, where a breach is deemed to have occurred in accordance with Section L10.25 or L10.26, that shall be treated as a final and binding determination of its occurrence for the purposes of this Code.

Appeal to the Authority

L10.29  Any decision made by the Panel in accordance with Section L10.20, L10.23, L10.24 or L10.27 may be appealed to the Authority, whose decision shall be final and binding for

the purposes of this Code.

**Definitions**

L10.30 For the purposes of this Section L10:

(a)     a "**Relevant Device**" means a Device:

(i)     which has, or had immediately prior to a Recovery Event, an SMI Status of 'commissioned'; and

(ii)    the Device Security Credentials of which are populated with, or are reasonably believed immediately prior to a Recovery Event to have been populated with, Data from an Organisation Certificate or OCA Certificate which has been (or is suspected of having been) Compromised as a result of an (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event;

(b)     the "**Relevant Subscriber**" means, where a Recovery Event has occurred, the Subscriber for an Organisation Certificate or OCA Certificate which has been (or is suspected of having been) Compromised as the result of an (actual or suspected) Compromise to the Relevant Private Key which gave rise to the Recovery Event;

(c)     a "**Relevant Private Key**" means a Private Key which is used to encrypt the Contingency Key Pair, or a Private Key which is associated with a Public Key contained in:

(i)     any Organisation Certificate or OCA Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System; or

(ii)    any OCA Certificate that was used as part of the process of Issuing any such Organisation Certificate or OCA Certificate;

(d)     a "**Recovery Key Pair**" means a Key Pair established by the DCC for the purposes of the replacement of Organisation Certificates on Devices after a Relevant Private Key has been Compromised, and:

(i)      a "**Recovery Private Key**" means the Private Key which is part of that Key Pair; and

(ii)      a "**Recovery Certificate**" means an Organisation Certificate Issued by the OCA and containing the Public Key which is part of that Key Pair; and

(e)      a "**Contingency Key Pair**" means a Key Pair established by the DCC for the purposes of the replacement of Root OCA Certificates on Devices after a Relevant Private Key has been Compromised, and comprising:

(i)      a "**Contingency Private Key**", being the Private Key which is part of that Key Pair; and

(ii)      a "**Contingency Public Key**", being the Public Key which is part of that Key Pair and which is stored in the WrappedApexContingencyKey field of the Root OCA Certificate (being the field identified as such in the Root OCA Certificate Profile at Annex B of the Organisation Certificate Policy)."

**L11**     **THE SUBSCRIBER OBLIGATIONS**

**Certificate Signing Requests**

L11.1   Each Eligible Subscriber shall ensure that all of the information contained in each Certificate Signing Request made by it is true and accurate.

L11.2   No Eligible Subscriber may make a Certificate Signing Request which contains:

(a)      any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(b)      any confidential information which would be contained in a Certificate Issued in response to that Certificate Signing Request.

L11.3   Each Eligible Subscriber shall ensure that either:

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

(b)      in every other case, the Public Key that is included within a Certificate Signing Request is part of a Key Pair that has been generated using random numbers which are such as to make it computationally infeasible to regenerate that Key Pair even with knowledge of when and by means of what equipment it was generated.

L11.4   No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

(a)      a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate;

(b)      an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of the Root OCA Certificate to the extent to which it is expressly permitted in

accordance with the Organisation Certificate Policy); or

(c)     an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate.

**Subscribing for or Rejecting Organisation Certificates**

L11.5   Where any Organisation Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a)     establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b)     if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i)     reject that Certificate; and

(ii)    immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c)     where it does not reject the Certificate, become a Subscriber for that Certificate.

**Subscribing for or Rejecting Device Certificates**

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

(a)     take reasonable steps to establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b)     if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i)     reject that Certificate; and

(ii)    immediately inform the DCC that it rejects the Certificate and give to the

DCC its reasons for doing so; and

(c)      where it does not reject the Certificate, become a Subscriber for that Certificate.

**Subscribing for or Rejecting IKI Certificates**

L11.7   Where any IKI Certificate is Issued to an Eligible Subscriber in response to a Certificate Signing Request, that Eligible Subscriber shall:

(a)      establish whether the information contained in that Certificate is consistent with information that was contained in the Certificate Signing Request;

(b)      if it identifies that the Certificate contains any information which is untrue or inaccurate:

(i)      reject that Certificate;

(ii)     immediately inform the DCC that it rejects the Certificate and give to the DCC its reasons for doing so; and

(c)      where it does not reject the Certificate, become a Subscriber for that Certificate.

**Use of Certificates and Key Pairs**

L11.8   Each Subscriber shall ensure that it does not use any Certificate, Public Key contained within a Certificate, or Private Key associated with a Public Key contained in a Certificate, that is held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from Devices and the DCC pursuant to the Code.

**Organisation and IKI Certificates: Protection of Private Keys**

L11.9   Each Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) take reasonable steps to ensure that no Compromise occurs to any:

(a)      Private Key which is associated with a Public Key contained in an Organisation Certificate or IKI Certificate for which it is the Subscriber; or

(b)     Secret Key Material associated with that Private Key.

**Organisation Certificates: Expiry of Validity Period**

L11.10 Each Subscriber shall, prior to the expiry of the Validity Period of an Organisation Certificate or OCA Certificate for which it is the Subscriber:

(a)     request a replacement for that Certificate by applying for the Issue of a new Organisation Certificate or OCA Certificate in accordance with the provisions of the Organisation Certificate Policy; and

(b)     ensure that any Data from that Certificate which are used to populate the Device Security Credentials of any Device are replaced by Data from the new Certificate Issued to it by the OCA.

**L12    RELYING PARTY OBLIGATIONS**

**Relying Parties**

L12.1   For the purposes of this Section L12, a 'Relying Party' in relation to an Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate means any Party or RDP which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from a Device or another Party or RDP pursuant to this Code.

L12.2   For the purposes of Section L12.1, a Relying Party shall be deemed to include:

(a)     in the case of a Device which relies on a Certificate, the Responsible Supplier for that Device; and

(b)     in the case of a Communications Hub Function or Gas Proxy Function which relies on a Certificate, the DCC.

**Duties in relation to Organisation Certificates, OCA Certificates, IKI Certificates and ICA Certificates**

L12.3   Each Relying Party shall:

(a)     before relying on any Organisation Certificate:

(i)     Check Cryptographic Protection in respect of the Organisation CRL on the SMKI Repository; and check the version of the Organisation CRL on the SMKI Repository, in accordance with the GB Companion Specification; and

(ii)    where that Certificate is shown on the Organisation CRL as having been revoked, not rely on the Certificate;

(b)     before relying on any OCA Certificate:

(i)     Check Cryptographic Protection in respect of the Organisation ARL on the SMKI Repository; and

(ii)    where that Certificate is shown on the Organisation ARL as having been

revoked, not rely on the Certificate;

(c)     before relying on any IKI Certificate:

    (i)     Check Cryptographic Protection in respect of the IKI CRL; and

    (ii)     where that Certificate is shown on the IKI CRL as having been revoked, not rely on the Certificate; and

(d)     before relying on any ICA Certificate:

    (i)     Check Cryptographic Protection in respect of the IKI ARL; and

    (ii)     where that Certificate is shown on the IKI ARL as having been revoked, not rely on the Certificate.

L12.4  No Relying Party may rely on an Organisation Certificate or IKI Certificate where the Validity Period of that Certificate has expired.

L12.5  No Relying Party may rely on an Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate where it suspects that the Certificate has been Compromised.

L12.6  Each Relying Party shall take reasonable steps, by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate.

**L13** **DCC KEY INFRASTRUCTURE**

**The DCCKI Services**

The DCCKI Services

L13.1 For the purposes of this Section L13, the "**DCCKI Services**" means all of the activities undertaken by the DCC in its capacity as the DCCKI Certification Authority in accordance with the applicable requirements of the Code.

DCCKI Authorised Subscribers

L13.2 Any Party or RDP may apply to become a DCCKI Authorised Subscriber in accordance with, and by following the relevant procedures set out in, the DCCKI Certificate Policy and the DCCKI RAPP.

L13.3 The DCC shall authorise any Party or RDP to submit a DCCKI Certificate Signing Request, or any User to submit a Personnel Authentication Certification Application, and so to become a DCCKI Subscriber, where that person has successfully completed the relevant procedures and satisfied the criteria set out in the DCCKI Certificate Policy and the DCCKI RAPP.

L13.4 The DCC shall provide any DCCKI Services that may be requested by a DCCKI Authorised Subscriber where the request is made by that DCCKI Authorised Subscriber in accordance with the applicable requirements of the DCCKI SEC Documents.

L13.5 The DCC shall ensure that in the provision of DCCKI Services it acts in accordance with Good Industry Practice.

Registration Data Providers

L13.6 Where a Registration Data Provider (other than an Electricity Network Party or Gas Network Party which is deemed to be an RDP, acting in its capacity as such) has become a DCCKI Authorised Subscriber, the Network Party that nominated that Registration Data Provider shall ensure that the RDP complies with all of its obligations in that capacity under this Section L13.

L13.7 Where a Registration Data Provider has been nominated as such by more than one

Network Party:

(a)     to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L13.6 in respect of the actions of the RDP;

(b)     to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L13.6 in respect of the actions of the RDP.

DCCKI Eligible Subscribers

L13.8   A DCCKI Authorised Subscriber:

(a)     shall be known as a "**DCCKI Eligible Subscriber**" in respect of a DCCKI Certificate if it is entitled to become a DCCKI Subscriber for that DCCKI Certificate; and

(b)     will be entitled to become a DCCKI Subscriber for a DCCKI Certificate only if it is identified as a DCCKI Eligible Subscriber in respect of that DCCKI Certificate in accordance with the provisions of the DCCKI Certificate Policy and the DCCKI RAPP.

DCCKI Subscribers

L13.9   A Party or RDP shall be entitled to become a DCCKI Subscriber in accordance with, and by following the relevant procedures set out in, the DCCKI Certificate Policy and the DCCKI RAPP.

**The DCCKI Service Interface**

DCC: Obligation to Maintain the DCCKI Service Interface

L13.10 The DCC shall maintain the DCCKI Service Interface in accordance with the DCCKI Interface Design Specification and make it available, to DCCKI Authorised Subscribers, for sending and receiving communications in accordance with the DCCKI Code of Connection.

L13.11 The DCC shall ensure that the DCCKI Service Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a)    from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and

(b)    prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing.

<u>The DCCKI Service Interface</u>

L13.12 For the purposes of this Section L13, the "**DCCKI Service Interface**" means a communications interface designed to allow communications to be sent between a DCCKI Authorised Subscriber and the DCC for the purposes of the DCCKI Services.

<u>DCCKI Interface Design Specification</u>

L13.13  For the purposes of this Section L13, the "**DCCKI Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a)    shall specify the technical details of the DCCKI Service Interface;

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

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

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

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

(iii)    PKCS is the Public Key Cryptography Standard; and

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

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

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

DCCKI Code of Connection

L13.14 For the purposes of this Section L13, the "**DCCKI Code of Connection**" shall be a SEC Subsidiary Document of that name which:

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

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

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

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

DCCKI Interface Document Development

L13.15 The DCC shall develop drafts of the DCCKI Interface Design Specification and DCCKI Code of Connection:

(a)    in accordance with the process set out at Section L13.16; and

(b)    so that the drafts are available by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.16 The process set out in this Section L13.16 for the development of drafts of the DCCKI Interface Design Specification and DCCKI Code of Connection is that:

(a)     the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of each document;

(b)     where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c)     the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

   (i)     a statement of the reasons why the DCC considers that draft document to be fit for purpose; and

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

(d)     the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

   (i)     any requirement to produce and submit to the Secretary of State a further draft of either document; and

   (ii)    any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

**The DCCKI Repository Service**

The DCCKI Repository

L13.17 For the purposes of this Section L13, the "**DCCKI Repository**" means a System for storing and (subject to the provisions of this Section) making available copies of the following:

(a)     all DCCKI Infrastructure Certificates;

(b)     the Root DCCKICA Certificate and the EII DCCKICA Certificate;

(c)     all versions of the DCCKI Certificate Policy;

(d)     the latest version of the DCCKI RAPP;

(e)     the latest version of the EII DCCKICA CRL;

(f)     the latest version of the DCCKI ARL; and

(g)     such other documents or information as the DCC, in its capacity as the provider of the DCCKI Services, may from time to time consider appropriate.

The DCCKI Repository Service

L13.18   The DCC shall establish, operate, maintain and make available the DCCKI Repository in accordance with the provisions of this Section L13 (the "**DCCKI Repository Service**").

L13.19   The DCC shall ensure that the documents and information described in Section L13.17 may be lodged in the DCCKI Repository by itself for the purpose of providing the DCCKI Services or complying with any other requirements placed on it under the Code.

L13.20   The DCC shall ensure that no person may lodge documents or information in the DCCKI Repository other than in accordance with Section L13.19.

L13.21   The DCC shall ensure that the DCCKI Repository may be accessed for the purpose of viewing and/or obtaining a copy of any document or information stored on it by any Party or RDP which reasonably requires such access in accordance, or for any purpose associated, with the Code.

L13.22   The DCC shall make available a copy of any document stored on the DCCKI Repository to the Panel or the SMKI PMA (or the Code Administrator acting on their behalf) following receipt of a reasonable request to do so.

Parties: Duties in relation to the DCCKI Repository

L13.23 No Party or RDP may access the DCCKI Repository for the purpose of viewing and/or obtaining a copy of any document or information stored on it except to the extent that it reasonably requires such access in accordance, or for any purpose associated, with the Code.

**The DCCKI Repository Interface**

DCC: Obligation to Maintain the DCCKI Repository Interface

L13.24 The DCC shall maintain the DCCKI Repository Interface in accordance with the DCCKI Repository Interface Design Specification and make it available to the Parties and to RDPs to send and receive communications in accordance with the DCCKI Repository Code of Connection and (where applicable) for the purpose of Entry Process Testing.

L13.25 The DCC shall ensure that the DCCKI Repository Interface is available at all times (subject to Planned Maintenance undertaken in accordance with Section H8.3):

(a) from the date on which the DCC is first obliged to provide the DCCKI Services in accordance with this Section L13; and

(b) prior to that date, on such dates and to such extent as is necessary for the purpose of facilitating Entry Process Testing.

The DCCKI Repository Interface

L13.26 For the purposes of this Section L13, the "**DCCKI Repository Interface**" means a communications interface designed to allow communications to be sent from and received by the DCCKI Repository for the purposes of the DCCKI Repository Service.

DCCKI Repository Interface Design Specification

L13.27 For the purposes of this Section L13, the "**DCCKI Repository Interface Design Specification**" shall be a SEC Subsidiary Document of that name which:

(a) specifies the technical details of the DCCKI Repository Interface; and

(b) includes the protocols and technical standards that apply to the DCCKI Repository Interface.

DCCKI Repository Code of Connection

L13.28 For the purposes of this Section L13, the "**DCCKI Repository Code of Connection**" shall be a SEC Subsidiary Document of that name which sets out the way in which the Parties and RDPs may access the DCCKI Repository Interface.

DCCKI Repository Interface Document Development

L13.29 The DCC shall develop drafts of the DCCKI Repository Interface Design Specification and DCCKI Repository Code of Connection:

(a) in accordance with the process set out at Section L13.30; and

(b) so that the drafts are available by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.30 The process set out in this Section L13.30 for the development of drafts of the DCCKI Repository Interface Design Specification and DCCKI Repository Code of Connection is that:

(a) the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of each document;

(b) where a disagreement arises with any person who is consulted with regard to any proposal as to the content of either document, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the document;

(c) the DCC shall send a draft of each document to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

(i) a statement of the reasons why the DCC considers that draft document to be fit for purpose; and

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

(d) the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to either draft document, including in particular:

(i) any requirement to produce and submit to the Secretary of State a further draft of either document; and

(ii) any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

**The DCCKI Document Set**

Obligations on the SMKI PMA

L13.31 The SMKI PMA shall exercise the functions that are allocated to it under and (in so far as they apply to it) comply with the requirements of the DCCKI Document Set.

Obligations on DCCKI Participants

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

The DCCKI Document Set

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

(a) the DCCKI SEC Documents; and

(b) the DCCKI CPS.

The DCCKI SEC Documents

L13.34 For the purposes of this Section L13, the "**DCCKI SEC Documents**" means the provisions of the Code comprising:

(a) the following SEC Subsidiary Documents:

(i) the DCCKI Certificate Policy;

(ii) the DCCKI RAPP;

(iii)    the DCCKI Interface Design Specification;

(iv)    the DCCKI Code of Connection;

(v)    the DCCKI Repository Interface Design Specification;

(vi)    the DCCKI Repository Code of Connection;

(b)    the provisions of this Section L13; and

(c)    every other provision of the Code which relates to the provision or the use of the DCCKI Services or the DCCKI Repository Service or to any matters directly arising from or affecting the provision or the use of those Services.

The DCCKI Registration Authority Policies and Procedures: Document Development

L13.35 The DCC shall develop a draft of the DCCKI RAPP:

(a)    to make provision for such matters as are specified in the DCCKI Certificate Policy as being matters provided for in the DCCKI RAPP;

(b)    to make provision for such other matters as are necessary or appropriate in relation to the exercise of its functions as the DCCKI Registration Authority;

(c)    in accordance with the process set out at Section L13.36; and

(d)    so that the draft is available by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be specified by the Secretary of State.

L13.36 The process set out in this Section L13.36 for the development of a draft of the DCCKI RAPP is that:

(a)    the DCC shall, in consultation with the Parties, RDPs and such other persons as it considers appropriate, produce a draft of the DCCKI RAPP;

(b)    where a disagreement arises with any person who is consulted with regard to any proposal as to the content of the DCCKI RAPP, the DCC shall endeavour to reach an agreed proposal with that person consistent with the purposes of the

DCCKI RAPP specified in Section L13.35;

(c)     the DCC shall send a draft of the DCCKI RAPP to the Secretary of State as soon as is practicable after it is produced, and shall when doing so provide to the Secretary of State:

   (i)     a statement of the reasons why the DCC considers that draft to be fit for purpose; and

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

(d)     the DCC shall comply with any requirements in a direction given to it by the Secretary of State in relation to the draft of the DCCKI RAPP, including in particular:

   (i)     any requirement to produce and submit to the Secretary of State a further draft of the document; and

   (ii)    any requirement as to the process to be followed by the DCC (and the time within which that process shall be completed) prior to submitting a further such draft.

The DCCKI Certification Practice Statement

L13.37  The DCC shall establish, give effect to, maintain and comply with a document which shall be known as the "**DCCKI CPS**".

L13.38  The DCCKI CPS shall be a document which:

(a)     sets out the policies and procedures of the DCC designed to ensure that it will comply with the requirements of the DCCKI Certificate Policy;

(b)     incorporates the detailed operating procedures to be used by the DCC for the purposes of its compliance with the requirements of that Policy;

(c)     incorporates such other provisions as may be required by or in accordance with that Policy or any other part of the Code;

(d)     is reviewed by the SMKI PMA to assess whether it is appropriate for these purposes; and

(e)     is approved by the individual(s) carrying out the DCCKI PMA Functions as being appropriate for these purposes.

L13.39 For the purposes of the review of the DCCKI CPS by the SMKI PMA in accordance with Section L13.38(d), the DCC shall submit an initial draft of the DCCKI CPS to the SMKI PMA by no later than the commencement of Systems Integration Testing or 2 March 2015 (whichever is earlier), or such later date as may be agreed by the SMKI PMA.

L13.40 The DCC shall keep the DCCKI CPS under review, and shall in particular carry out a review of the DCCKI CPS:

(a)     whenever (and to the extent to which) it may be required to so by the SMKI PMA or the individual(s) carrying out the DCCKI PMA Functions; and

(b)     following receipt of a notification from the SMKI PMA in accordance with Section L1.17(e) (Duties of the SMKI PMA).

L13.41 Following:

(a)     any review of the DCCKI CPS, the DCC may propose amendments to it, which it shall submit to:

(i)      the SMKI PMA for its review; and

(ii)     the individual(s) carrying out the DCCKI PMA Functions for his (or their) approval;

(b)     a review carried out in accordance with Section L13.40(b), the DCC shall report to the SMKI PMA any remedial steps taken or proposed to be taken in order for it to continue to meet its obligations under Section G (Security).

Enquiries in relation to the DCCKI Document Set

L13.42 The DCC shall respond within a reasonable time to any reasonable request for information made by a Party or RDP in relation to the DCCKI Services, the DCCKI

Repository Service or the DCCKI Document Set, but excluding any request for a copy of any document or information which can be accessed through the DCCKI Repository.

**The DCCKI Subscriber Obligations**

<u>DCCKI Certificate Signing Requests and Personnel Authentication Certificate Applications</u>

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

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

(a)     any information that constitutes a trade mark, unless it is the holder of the Intellectual Property Rights in relation to that trade mark; or

(b)     any confidential information which would be contained in a DCCKI Certificate Issued in response to that DCCKI Certificate Signing Request or Personnel Authentication Certificate Application.

<u>Subscribing for or Rejecting DCCKI Certificates</u>

L13.45  Where any DCCKI Certificate is Issued to a DCCKI Eligible Subscriber in response to a DCCKI Certificate Signing Request, or any Personnel Authentication Certificate is Issued to a DCCKI Eligible Subscriber in response to a Personnel Authentication Certificate Application, that DCCKI Eligible Subscriber shall:

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

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

(c)     in the absence of any such rejection, become a DCCKI Subscriber for that DCCKI Certificate or Personnel Authentication Certificate.

Use of DCCKI Certificates

L13.46 Each DCCKI Subscriber shall ensure that it does not use any DCCKI Certificate held by it other than for the purposes of creating, sending, receiving and processing communications sent to and from the DCC pursuant to the Code.

DCCKI Certificates: Protection of Private Keys

L13.47 Each DCCKI Subscriber shall (in addition, if it is the DCC, a User or an RDP, to its obligations under Section G (Security)) take reasonable steps to ensure that no Compromise occurs to any:

(a)     Private Key which is associated with a Public Key contained in a DCCKI Certificate for which it is the DCCKI Subscriber; or

(b)     Secret Key Material associated with that Private Key.

**The DCCKI Relying Party Obligations**

DCCKI Relying Parties

L13.48 For the purposes of this Section L13, a **"DCCKI Relying Party"** in relation to a DCCKI Certificate or DCCKICA Certificate, means any Party or RDP which relies on the Certificate for the purposes of creating, sending, receiving or processing communications sent to and from the DCC or another Party or RDP pursuant to this Code.

Duties in relation to DCCKI Certificates and DCCKICA Certificates

L13.49 Each DCCKI Relying Party shall:

(a)     before relying on any DCCKI Certificate:

(i)     Check Cryptographic Protection in respect of the EII DCCKICA CRL (or, in the case of DCC only, any DCCKI Certificate Revocation List relevant to that DCCKI Certificate) on the DCCKI Repository, in

accordance with IETF RFC 5280; and

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

(b)     before relying on any DCCKICA Certificate:

(i)     Check Cryptographic Protection in respect of the DCCKI ARL on the DCCKI Repository, in accordance with IETF RFC 5280; and

(ii)     where that DCCKICA Certificate is shown on the DCCKI ARL as having been revoked, not rely on the DCCKICA Certificate.

L13.50 No DCCKI Relying Party may rely on a DCCKI Certificate where the Validity Period of that DCCKI Certificate has expired.

L13.51 No DCCKI Relying Party may rely on a DCCKI Certificate or DCCKICA Certificate where it suspects that the DCCKI Certificate has been Compromised.

L13.52 Each DCCKI Relying Party shall take reasonable steps , by means of appropriate Systems, to verify Digital Signatures, Check Cryptographic Protection, Confirm Validity and perform other appropriate cryptographic operations before relying on any DCCKI Certificate or DCCKICA Certificate.

**The DCCKI PMA Functions**

Performance of the DCCKI Functions

L13.53 The DCC shall make arrangements which shall ensure that:

(a)     a senior member of DCC Personnel;

(b)     a senior member of the personnel of a DCC Service Provider; or

(c)     a number of individuals, each of whom falls within either paragraph (a) or (b), acting together,

shall carry out the DCCKI PMA Functions.

### The DCCKI PMA Functions

L13.54 For the purpose of this Section L13, the "**DCCKI PMA Functions**" shall mean the activities of:

(a)     approving the DCCKI CPS, and any amendments to it;

(b)     periodically:

     (i)     reviewing the effectiveness of the DCCKI Document Set (including so as to evaluate whether the DCCKI Document Set remains consistent with the SEC Objectives); and

     (ii)    identifying any changes that should be made to the DCCKI Document Set in order to ensure that the DCC meets its obligations under Section G (Security);

(c)     as soon as is reasonably practicable following the incorporation of each of the following documents into this Code, its re-incorporation, or its modification in accordance with section 88 of the Energy Act 2008, carrying out in relation to it the activities specified in paragraph (a) above:

     (i)     the DCCKI Certificate Policy;

     (ii)    the DCCKI RAPP;

(d)     on receipt by the DCC of a notification from the SMKI PMA in accordance with Section L1.17(e) (Duties of the SMKI PMA), carrying out in relation to the DCCKI Document Set the activities specified in paragraph (a) above, having regard in particular to any recommendation for action made by the SMKI PMA; and

(e)     performing any other duties expressly described as DCCKI PMA Functions elsewhere in this Code.

### The Duties of the DCC

L13.55 Where the individual(s) carrying out the DCCKI PMA Functions notifies the DCC of any matter, or makes any recommendation with regard to the compliance by the DCC with its obligations under Section G (Security) (including in particular any recommendation for the modification of the DCCKI Document Set for the purpose of ensuring such compliance), the DCC shall:

(a)     consider and take into account the matter notified, or recommendation made, to it; and

(b)     where, having done so, it considers that it would be appropriate to make a change to the:

    (i)     DCCKI SEC Documents, submit a Modification Proposal for that purpose; and

    (ii)    DCCKI CPS, propose amendments to it in accordance with Section L13.42.

L13.56 The DCC shall ensure that the SMKI PMA and Security Sub-Committee shall each be provided with such of the following information as it may request:

(a)     any notification or recommendation made to the DCC by the individual(s) carrying out the DCCKI PMA Functions; and

(b)     copies of all agenda and supporting papers available at any meeting between individuals acting together to carry out the DCCKI PMA Functions, insofar as those agenda and papers are reasonably relevant to the functions of the SMKI PMA or Security Sub-Committee (as the case may be).

L13.57 The DCC shall ensure that, where it receives any report with regard to its ISO 27001 certification and part of that report relates to any matters concerned with the DCCKI Services, it will as soon as reasonably practicable provide those parts of that report to the SMKI PMA.