

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); and
 - (d) one representative of the Security Sub-Committee and one representative of the Technical Architecture and Business Architecture Sub-Committee (in each case as further described in Section L1.10); 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 “**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) Member 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 Draft Proposals in respect of those documents;

- (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 Draft 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 in the latter case the use of the Contingency 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 Sub-Committee, the Change Board and Working Groups with support and advice in respect of Draft Proposals and 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 DCC KI 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 Draft Proposals and 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 Draft Proposals):

- (a) the SMKI PMA shall be entitled to submit Draft 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 Draft 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).

L3 THE SMKI SERVICES

The SMKI Services

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

- (a) the Device Certification Authority;
- (b) the Organisation Certification Authority; or
- (c) the IKI Certification Authority,

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

Authorised Subscribers

General Provisions

L3.2 For the purposes of this Section L3:

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

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

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

L3.4 The DCC shall provide any SMKI Services that may be requested by an Authorised

Subscriber where the request is made by that Authorised Subscriber in accordance with the applicable requirements of the SMKI SEC Documents.

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

Registration Data Providers

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

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

- (a) that RDP shall not, by virtue of acting in the capacity of an RDP for different Network Parties, be required to become a Subscriber for different Organisation Certificates;
- (b) to the extent to which that RDP can be clearly identified as acting on behalf of one Network Party, that Network Party shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP;
- (c) to the extent to which that RDP cannot be clearly identified as acting on behalf of one Network Party, each of the Network Parties which nominated that RDP shall be subject to the requirements of Section L3.6 in respect of the actions of the RDP.

Determinations by the Panel

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

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

- (a) shall determine whether the relevant applicant satisfies the criteria set out in the relevant Certificate Policy and the SMKI RAPP; and
- (b) where the Panel determines that the relevant applicant meets those criteria, it shall notify the DCC, and the applicant shall (subject to any other requirements of the relevant Certificate Policy or the SMKI RAPP) become an Authorised Subscriber.

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

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

Changes in Circumstance

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

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

- (a) assess whether that Authorised Subscriber continues to satisfy the relevant criteria to be an Authorised Subscriber as set out in the relevant Certificate Policy and the SMKI RAPP; and
- (b) where it determines that the Authorised Subscriber does not continue to satisfy the relevant criteria, notify the Authorised Subscriber which, subject to Section L3.14, shall cease to be an Authorised Subscriber in accordance with the

Certificate Policy.

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

- (a) the provisions of Section L3.8 to L3.11 shall apply as if the person notified had made an unsuccessful application to become an Authorised Subscriber in respect of the relevant Certificate Policy; and
- (b) where the relevant Certificate Policy is the Organisation Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, revoke any Organisation Certificates for which that person is the Subscriber;
- (c) where the relevant Certificate Policy is the IKI Certificate Policy, the DCC shall, subject to any determination made by the Panel in accordance with Section L3.9, take such steps in relation to any IKI Certificates for which that person is the Subscriber as may be set out in that Certificate Policy or in the SMKI RAPP.

Eligible Subscribers

L3.15 An Authorised Subscriber:

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

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.

<u>Party</u>	<u>Subject</u>
The DCC	Either: (a) a Communications Hub Function; or (b) a Gas Proxy Function.
An Import Supplier	Either: (a) an Electricity Smart Meter; or (b) a Type 1 Device.
A Gas Supplier	Either: (a) a Gas Smart Meter; (b) a Gas Proxy Function; or (c) a Type 1 Device.
Any other Party	Either: (a) an Electricity Smart Meter (b) a Gas Smart Meter; or (c) a Type 1 Device, but only in so far as the SMI Status of that Device is not set to ‘commissioned’ or ‘installed not commissioned’.
The DCC acting as the Production Proving Function	Any Production Proving Device.

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 X520OrganizationalUnitName 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 it is identified with that Remote Party Role in the second column of that table and the Certificate Signing Request originates from the individual System referred in the paragraph of the definition of DCC Live Systems identified in the fourth column of that table; 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.

<u>Remote Party Role</u>	<u>Party</u>	<u>User Role or RDP</u>	<u>DCC Live Systems definition paragraph</u>

root	The DCC	[Not applicable]	(d)
recovery	The DCC	[Not applicable]	(f)
transitionalCoS	The DCC	[Not applicable]	(c)
wanProvider	The DCC	[Not applicable]	(a)
accessControlBroker	The DCC	[Not applicable]	(ba)
issuingAuthority	The DCC	[Not applicable]	(a)
networkOperator	A Network Party	Either: (a) Electricity Distributor; or (b) Gas Transporter.	[Not applicable]
supplier	A Supplier Party	Either: (a) Import Supplier; or (b) Gas Supplier.	[Not applicable]
other	An RDP or any Party other than the DCC	Either: Other User; Registered Supplier Agent; Registration Data Provider; or Export Supplier.	[Not applicable]
pPPXmlSign	The DCC	[Not Applicable]	(g)

pPRDPFileSign	The DCC	[Not Applicable]	(g)
s1SPxmlSigning	The DCC	[Not Applicable]	(g)
<u>xmlSign</u>	<u>An RDP or any Party other than the DCC</u>	<u>Either:</u> <u>Import Supplier;</u> <u>Gas Supplier;</u> <u>Electricity Distributor;</u> <u>Gas Transporter.</u> <u>Other User;</u> <u>Registered Supplier Agent;</u> <u>Registration Data Provider; or</u> <u>Export Supplier.</u>	<u>[Not applicable]</u>
commissioningPartyFileSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
requestingPartyFileSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
s1SPMigrationSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]
commissioningPartyXmlSigning	The DCC	[Not Applicable]	[Only relevant during SMETS1 Migration]

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 (accessControlBroker) - digitalSignature Certificate;
- (g) the DCC (accessControlBroker) – 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 X520OrganizationalUnitName 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.

<u>Certificate</u>	<u>keyUsage</u> <u>Value</u>	<u>Remote Party Role</u>	<u>DCC Role</u>
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	transitionalCoS	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) “**X520OrganizationalUnitName**” 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.

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 (~~and including~~ the use of the Contingency 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 (~~and including~~ the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the use of the Contingency 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 in the latter case the Contingency 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 submit any Draft 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 Symmetric 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; and
- (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).~~

Annex A to Section L

Table 1: Remote Party Roles and associated Remote Party Role Codes in addition to those specified in the GB Companion Specification

Remote Party Role	Remote Party Role Code
pPPXmlSign	128
pPRDPFileSign	129
s1SPxmlSigning	126
commissioningPartyFileSigning	132
requestingPartyFileSigning	131
s1SPMigrationSigning	130
commissioningPartyXmlSigning	133
<u>xmlSign</u>	<u>134</u>