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 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:

(i) a Private Key which is used to encrypt the Contingency Key Pair;

~~(i) , or~~ a Private Key which is associated with a Public Key contained in ~~:~~

(ii) 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;

~~(A) 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~~

(iii) ~~any OCA Certificate that was used as part of the process of Issuing any such Organisation Certificate or OCA Certificate;~~a Private Key which is associated with a Public Key contained in any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP;

(iv) a Private Key which was used as part of the process of Issuing any OCA Certificate or Organisation Certificate referred to in paragraph (ii) or (iii) above;

(v) a Private Key which is used to Digitally Sign any XML Document, and which is associated with a Public Key that is contained within any Organisation Certificate; or

~~(ii)~~(vi) a Private Key which is associated with a Public Key contained in any certificate issued in accordance with an S1SPKI Certificate Policy, and which is determined by the SMKI PMA as being a Private Key for the purposes of this paragraph;

~~(c)~~(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

~~(d)~~(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).