

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP198 ‘Further Changes from the Review of the SMKI and DCCKI Document Set’

Legal text – version 0.1

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix L ‘SMKI Recovery Procedure’

These changes have been redlined against Appendix L version 5.0.

Amend Appendix as follows:

Appendix L

SMKI Recovery Procedure

1. Introduction

1.1 Purpose & Interpretation

Section L10.4 of the Code sets out the principal rights and obligations for compliance with any requirements set out in the SMKI Recovery Procedure.

This document, the SMKI Recovery Procedure, sets out the procedural requirements and the rights and obligations in respect of the DCC, Parties and the SMKI PMA relating to recovery from the Compromise of a Relevant Private Key. The scope of the SMKI Recovery Procedure is as set out in Section L10 of the Code and is further set out in more detail in Section 1.2 of this document.

The procedures as set out in this document shall be executed in the event of a Compromise of a Relevant Private Key, other than as directed by the SMKI PMA, in accordance with the procedures set out in this document.

For the purposes of the SMKI Recovery Procedure defined terms shall have the meaning in SEC Section A (Definitions and Interpretations), SEC Appendix B (Organisation Certificate Policy), and Appendix F (Definitions) of this SEC Appendix L (SMKI Recovery Procedure). Additionally, the following shall apply:

- a) notwithstanding the definition as set out in Section A of the Code, "Subscriber" means, in relation to any Organisation Certificate associated with a Relevant Private Key, a Party which has been Issued with and accepted that Organisation Certificate, acting in its capacity as the holder of the Organisation Certificate;
- b) "M#N Share" means, in relation to a Private Key, that the key is split into N Key Components such that the Private Key may be recreated using any M or more Key Components, and the Private Key may not be recreated using fewer than M Key Components;
- c) except where explicitly stated otherwise, or where it would be inappropriate within the context of its use, the term "Compromise" shall be interpreted to be a reference to a Compromise or a suspected Compromise.
- d) "Contingency Symmetric Key" means, as defined in the SEC Section A, the Symmetric Key used to encrypt the Contingency Public Key;
- e) Relevant Private Key has, as defined in the SEC Section A, the meaning set out in Section L10;
- f) "Recovery Action Risks" has the meaning defined in section 3.5 of this document;
- g) "Party" has the meaning set out in SEC Section A except for the DCC, which shall not be a Party for the purposes of this document;
- h) "TADP" means the Threshold Anomaly Detection Procedures;
- i) "XML Signing Private Key" means a Private Key for which an associated Organisation Certificate has been issued that would allow the Subscriber to sign XML documents pursuant to the SEC. For clarity, this includes private keys which are (1) used by the DSP, or by a provider of WAN services to the DCC, only to sign XML and (2) have a GBCS defined Remote Party Role.
- j) where an obligation is expressed as being an obligation on a Key Custodian it shall be interpreted as being an obligation on:
 - i. in the case of a Key Custodian appointed by a Party or the DCC, that Party or the DCC as the context requires, and

- ii. in the case of a Key Custodian appointed by the SMKI PMA or the Panel, the SMKI PMA or the Panel Member as the context requires;
- k) except for a Root OCA Certificate, a Private Key is “associated” with an Organisation Certificate or OCA Certificate where that Private Key is associated with the Public Key contained within that Organisation Certificate or OCA Certificate. For a Root OCA Certificate, a Private Key is “associated” with that Root OCA Certificate if it is associated with the Public Key contained in unencrypted form within that Root OCA Certificate. Note that a Contingency Public Key will also be present in a Root OCA Certificate but that it will be presented in an encrypted form;
- l) “CoS Certificate” means an Organisation Certificate issued to the DCC, acting in the role of the CoS Party, which has a Remote Party Role of ‘transitionalCoS’ with the meaning of SEC Section L, clause 3.18;
- m) an Organisation Certificate or OCA Certificate is considered to be “stored” on a Device if information from that Organisation Certificate or OCA Certificate forms part of the Device Security Credentials of that Device; and
- n) “Contingency Symmetric Key Splitting” means the splitting of the Contingency Symmetric Key into parts, each of which are securely retained by each of the “Symmetric Key Custodians”. “Symmetric Key Custodians” shall be interpreted accordingly with the roles being fulfilled by the DCC.

1.2 Scope

The SMKI Recovery Procedure sets out the detail of the arrangements between the DCC, Parties, the SMKI PMA and the Panel in respect of:

- a) **Pre-Recovery:**
 - i. confirmation of a Compromise of a Relevant Private Key that the DCC becomes aware of, including where this is reported to the DCC by a Party, resulting in an Incident being raised in accordance with sections 2.1 and 2.2 of the Incident Management Policy;
 - ii. notification to the DCC of the Anomaly Detection Thresholds (or amendment of Anomaly Detection Thresholds by the DCC where necessary, including where the DCC will be originating Commands as part of the recovery procedure) that are required to support replacement of affected Organisation Certificates or OCA Certificates stored on Devices;
 - iii. where use of the Recovery Private Key or the Contingency Private Key would be required in order to recover, consultation by the DCC with the SMKI PMA to determine the extent to which the recovery procedure should be executed and the manner in which it should be executed;
 - iv. revocation of affected Organisation Certificates or OCA Certificates (where required); and
 - v. other steps as set out in this SMKI Recovery Procedure;
- b) **Execution of Recovery:**
 - i. execution of activities to recover from a Compromise of a Relevant Private Key; and
- c) **Post-Recovery:**
 - i. replacement of Organisation Certificates and OCA Certificates and Private Keys (where necessary);
 - ii. post-Incident review and reporting;
 - iii. provision to relevant parties of information intended to prevent reoccurrence of similar Incidents; and

SEC - Appendix L

- iv. revocation of replaced Organisation Certificates and OCA Certificates (where necessary).

The SMKI Recovery Procedure addresses recovery from a Compromise in respect of any Relevant Private Key listed immediately below:

- a) Pursuant to L10.30 (c) (ii) and (iii):
 - i. a Private Key which is associated with any Organisation 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. a Private Key which is associated with any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP;
- b) Pursuant to L10.30 (c) (i), the Contingency Symmetric Key;
- c) Pursuant to L10.30 (c) (ii), the Contingency Private Key;
- d) Pursuant to L10.30 (c) (iv), the Private Key associated with an Issuing OCA Certificate;
- e) Pursuant to L10.30 (c) (ii) and (iv), the Private Key associated with a Root OCA Certificate;
- f) Pursuant to L10.30 (c) (ii) the Private Key associated with a Recovery Certificate; and
- g) Pursuant to L10.30 (c) (v), an XML Signing Private Key.

Pursuant to L10.30 (c) (vi), the relevant Certification **Practise** Statement (CPS) addresses recovery from a Compromise in respect of any 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 requiring a recovery procedure.

Commented [GH1]: Legal Advice please: Spelled as 'Practice' here but 'Practice' everywhere else - search 'CPS'

Figure 1, immediately below, shows the relevant Organisation Certificates and OCA Certificates that are stored on applicable SMETS2+ Devices. The details listed in the column labelled 'ESME' apply both to Devices which are ESME and to Devices which are SAPC.

Devices		ESME electricity meter	GSME gas meter	CHF comms hub	GPF gas proxy	PPMID pre-payment meter	HCALC HAN auxiliary load control	Other DCC Keys/Certificates that could be affected by a Compromise	
DCC	Root OCA	●	●	●	●	●	●	DCC	Root OCA Private Key / Certificate
DCC	Recovery	●	●	●	●	●	●	DCC	Issuing OCA Private Key / Certificate
Supplier	Supplier Digital Signature	●	●	●	●	●	●		
Supplier	Supplier Key Agreement	●	●	●	●	●	●	DCC	Contingency Symmetric Key
Supplier	Supplier Key Agreement (Pre-Payment)	●	●	●	●	●	●	DCC	Contingency Private Key
Network Operator	Network Operator Digital Signature	●	●	●	●	●	●		
Network Operator	Network Operator Key Agreement	●	●	●	●	●	●		
DCC	AccessControlBroker Digital Signature	●	●	●	●	●	●	DCC	Recovery Private Key / Certificate
DCC	AccessControlBroker Key Agreement	●	●	●	●	●	●		
DCC	transitionalCoS Digital Signature	●	●	●	●	●	●		
DCC	wanProvider Digital Signature	●	●	●	●	●	●		

Figure 1: Public Key Organisation Certificates / Keys covered by the SMKI Recovery Procedure

Figure 2, immediately below, shows the relevant Organisation Certificates that form the Device Security Credentials held by an S1SP for SMETS1Devices that are Commissioned within the DCC Systems:

		ESME electricity meter	GSME gas meter	CHF comms hub	GPF gas proxy	PPMID pre-payment meter	Other DCC Keys/Certificates that could be affected by a Compromise	
Supplier	Notified Critical Supplier Certificate	●	●	●	●	●	DCC	Root OCA Private Key
Supplier	Notified Non-Critical Supplier Certificate	●	●	●	●	●	DCC	Issuing CA Private Key
Network Operator	Notified Critical Network Operator Certificate	●	●	●	●	●		
Network Operator	Notified Non-Critical Network Operator Certificate	●	●	●	●	●		

Figure 2: Organisation Certificates used by SMETS1 Service Providers for security credentials for SMETS1 Devices

The Check Cryptographic Protection applied by a SMETS1 Service Provider and the DCC to a Critical Service Request targeting a SMETS1 CHF or SMETS1 PPMID is carried out using the Notified Critical Supplier ID for the corresponding SMETS1 ESME.

2. Overview of the SMKI Recovery Procedure

In the event of an incident which:

SEC - Appendix L

- a) results in the Compromise of a Relevant Private Key; or
- b) causes the Subscriber for the Certificate associated with any of the Keys in a) above to reasonably suspect that there has been a Compromise of any such Key,

the provisions of this SMKI Recovery Procedure shall apply.

The SMKI Recovery Procedure includes procedures which detail the obligations of the DCC, Subscribers and the SMKI PMA, in respect of recovery from Compromise of a Relevant Private Key as set out in Section 1.2 of this document.

The table as set out immediately below summarises the actions required and the section(s) of this document which contain the applicable recovery procedure(s). It should be noted that it is possible to handle only one scenario type at a time and there is a logical order of Section 4 first, then Section 6 second and then Section 5 last to address increasing severity scenarios, their impact on the DCC Total System and the nature of the recovery procedure required. However, the execution of the steps is subject to SMKI PMA direction.

Compromise or Suspected Compromise of:	Section(s) of this document containing the procedure(s)
A Private Key which is associated with any Organisation Certificate, Data from which is used to populate the Device Security Credentials of a Device comprising part of an Enrolled Smart Metering System; or a Private Key which is associated with any Organisation Certificate, Data from which is used to populate part of any Device Security Credentials held by an S1SP	4.1 Method 1 – recovery by the affected Subscriber using the Compromised Private Key (or any other relevant key held by the Subscriber) to replace the associated Organisation Certificates on SMETS2+ Devices 4.1.1 Pre-Recovery 4.1.2 Execution of Recovery Procedure 4.1.3 Post-Recovery 4.1A Method 1A – replacement of an Organisation Certificate forming part of S1SP Held Device Security Credentials 4.1A.1 Pre-Recovery 4.1A.2 Execution of Recovery Procedure 4.1A.3 Post-Recovery 4.2 Method2 – recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected SMETS2+ Devices (only available to a Supplier Party) 4.2.1 Pre-Recovery 4.2.2 Execution of Recovery Procedure 4.2.3 Post-Recovery Method 3 – recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on SMETS2+ Devices 4.3.1 Pre-Recovery 4.3.2 Execution of Recovery Procedure 4.3.3 Post-Recovery

Root OCA Private Key	5.1 Pre-Recovery 5.2 Execution of Recovery Procedure 5.3 Post Recovery
Contingency Private Key or Contingency Symmetric Key	6.1.1 Pre-Recovery 6.1.2 Execution of Recovery Procedure 6.1.3 Post-Recovery
Recovery Private Key	6.2.1 Pre-Recovery 6.2.2 Execution of Recovery Procedure 6.2.3 Post-Recovery
Issuing OCA Private Key	6.3.1 Pre-Recovery 6.3.2 Execution of Recovery Procedure 6.3.3 Post-Recovery
Replacement of an XML Signing Private Key	7.1.1 XML Signing Private Key destruction considerations

3. General obligations

3.1 DCC Obligations

The DCC shall:

- a) conduct the procedures set out in this document;
- b) comply with any decisions made by the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise;
- c) where the DCC attempts but fails to replace one or more Organisation Certificates or OCA Certificates as part of operating these procedures, execute as many retries to replace such Organisation Certificates or OCA Certificates as the DCC can reasonably accommodate given the circumstances of the Compromise and capability of the DCC Systems, prior to any deadline for recovery as approved by the SMKI PMA;
- d) where the DCC consults with the SMKI PMA regarding whether or not to take certain steps in order to recover from a Compromise and the DCC is directed such that recovery using the Recovery Private Key or Contingency Private Key should not be performed, the DCC shall inform all affected Parties of the outcome and any reasons provided by the SMKI PMA, as soon as reasonably practicable following such instruction, via a secured electronic means;
- e) maintain confidential, auditable and secured records relating to the recovery from a Compromise, and the Devices and Subscribers affected by such Compromise; and
- f) within three Working Days of the recovery from a Compromise, prepare a report regarding execution of the recovery and provide such report to the SMKI PMA, where such report shall include:
 - i. the process steps executed and the timing of the procedure to recover from the Compromise;
 - ii. where possible, carry out an analysis of which communications have been submitted to, or in relation to, any relevant affected Devices and any anomalous activity that should be investigated further by the DCC and/or affected Subscribers, and/or addressed via remedial actions; and

- iii. keep this document under review and following consultation with the SMKI PMA, propose modifications to the SMKI Recovery Procedure that the DCC believes are necessary for the SMKI Recovery Procedure to meet the objectives more effectively as set out in the SEC.

Where such adjustments are needed to allow the effective executions of the procedures in this document, the DCC shall, as provided for in SEC Section L 10.2 (c), adjust the Anomaly Detection Thresholds, which it sets in other situations only after they are agreed by the Security Sub-Committee, subject only to the agreement of the SMKI PMA.

3.2 Notification and confirmation of a suspected Compromise

Any person may notify the DCC that there is a Compromise Relevant Private Key.

Where the DCC is notified or becomes aware of a Compromise Relevant Private Key, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall notify the SMKI PMA, via secured electronic means, that a Compromise has been notified. The DCC shall contact the Subscriber for the Organisation Certificate associated with that Private Key or Contingency Symmetric Key (which may include the DCC itself as the Subscriber), as soon as reasonably practicable, via telephone and email using the contact details held by the SMKI Registration Authority. The DCC shall provide the Subscriber, via secured electronic means, with the appropriate Incident reference number and information relating to the notified Compromise. The DCC shall request confirmation from the Subscriber as to whether the Subscriber reasonably believes that a Compromise has occurred, and wishes to proceed with one or more of the recovery processes, which shall be confirmed by:

- a) A SMKI Senior Responsible Officer (SMKI SRO) on behalf of a Party; or
- b) A SMKI SRO, SMKI Registration Authority Manager or a member of SMKI Registration Authority Personnel authorised to act on behalf of the DCC in this capacity.

The Subscriber shall take reasonable steps to ensure that confirmation of whether it reasonably believes that a Compromise has occurred is provided to the DCC by the representatives above, within 24 hours of the request for confirmation from the DCC, via secured electronic means. Where the Subscriber confirms that it does not reasonably believe that a Compromise has occurred, the DCC shall close the Incident in accordance with section 2.12 of the Incident Management Policy.

Where the DCC receives confirmation that the Subscriber reasonably believes that a Compromise has occurred, the DCC shall also identify any Responsible Supplier(s) that are affected by the confirmed Compromise, in accordance with the procedures as set out in this document.

Where the DCC receives multiple Compromise notifications, the DCC may execute a common set of procedural steps to address such multiple Compromises, where it reasonably believes that such an approach would achieve the required recovery in an efficient manner.

3.3 Permitted mechanisms for confirmation of suspected Compromise

The DCC shall only accept the confirmation of a Compromise from a representative of the Subscriber as is defined in section 3.2 of this document, for an Organisation Certificate associated with a Compromised Private Key or from the DCC in respect of a Compromised Contingency Symmetric Key or the Compromise of an Organisation Certificate or OCA Certificate for which the DCC is the Subscriber, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means.

3.4 Appointment and responsibilities of Key Custodians

The Organisation Certification Practice Statement (Organisation CPS) requires the Contingency Private Key and Recovery Private Key to be split into M#N Shares and that such Private Keys may be activated only via collaboration between appointed Key Custodians. The procedure as set out in this section 3.4 shall be followed in order to appoint such Key Custodians as are required.

3.4.1. Responsibilities in respect of Key Custodians

Each Party, the DCC, the SMKI PMA or the Panel, on behalf of which an individual acting on behalf of that organisation becomes a Key Custodian, shall ensure that the Key Custodian:

- a) does not seek to find out the identity of other Key Custodians or otherwise collude with other Key Custodians in relation to matters associated with this Recovery Procedure other than for the purposes as set out in this SMKI Recovery Procedure;
- b) does not disclose the fact that they are a Key Custodian, other than:
 - i. in the case of each Party, to a Director, Company Secretary, SMKI SRO or Chief Information Security Officer for the organisation they represent; or
 - ii. in the case of the SMKI PMA or Panel, to other members of the SMKI PMA or Panel; and
 - iii. to those other persons to whom the information reasonably needs to be disclosed for reasons of personnel management within the relevant organisation, and furthermore shall ensure that persons within their organisation who are aware of the identity of a Key Custodian shall not disclose the identity of a Key Custodian more widely;
- c) takes all reasonable steps to protect and not to lose any safety deposit box key issued to them to secure any Cryptographic Module as part of the relevant Key Generation Ceremony, and which is used by the Key Custodian to secure the Cryptographic Module containing the Key Component issued to them, in accordance with any guidance documentation provided by the DCC to the Key Custodian via secured electronic means;
- d) where the safety deposit box securing the Cryptographic Module containing a Key Component cannot be accessed, or the safety deposit key is lost or cannot be accessed, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall take such steps as are necessary to resolve the Incident;
- e) takes all reasonable steps to attend a Key Generation Ceremony or Key Activation Ceremony when requested by the DCC and, where they are to attend, to take all steps that are reasonably practical to attend at the time requested by the DCC; and
- f) is, upon request to attend a Key Generation Ceremony or Key Activation Ceremony by the DCC, immediately released to perform the Key Custodian role unless it would be materially disruptive to the business of the relevant organisation for them not to be released at that time.

Where a Party is the Subscriber for an Organisation Certificate that is Compromised (or is suspected to be Compromised), the Subscriber is not the DCC and an individual acting on behalf of that Subscriber is a Key Custodian; the DCC may exclude that Key Custodian from attending any Key Generation Ceremony or Key Activation Ceremony required as part of the applicable recovery procedure, where the DCC considers such action to be appropriate to mitigate security risks. If such exclusion occurs, the DCC shall record the decision made, and shall notify that Key Custodian and a SMKI SRO for the Subscriber, via secured electronic means.

3.4.2. Ceasing to be a Key Custodian

In the event that a Party, the DCC, the SMKI PMA or the Panel wishes a particular individual to cease their role as a Key Custodian:

- a) such Party, the SMKI PMA or the Panel shall notify the DCC in writing, at least one month in advance of the date on which that it wishes the individual acting as a Key Custodian to cease to be a Key Custodian;

SEC - Appendix L

- b) the relevant Party, the DCC, the SMKI PMA or the Panel shall arrange for the Key Custodian to return the physical key for the corresponding safety deposit box in which the Cryptographic Module containing the relevant Key Component is held, to a Registration Authority Manager at the DCC's address as published on the DCC Website, by secure courier;
- c) the DCC shall update its records of Key Custodians; and
- d) the DCC shall conduct, insofar as necessary, the procedure as set out in section 3.4.3 immediately below.

3.4.3. Detailed procedure for appointment of Key Custodians

The procedure as set out immediately below shall be executed by the DCC, Parties, the SMKI PMA and the Panel in order to appoint Key Custodians.

Step	When	Obligation	Responsibility	Next Step
3.4.3.1	As identified by the DCC that Key Custodians are required	The DCC shall identify the need for Key Custodians in respect of a Recovery Private Key or Contingency Private Key.	DCC	3.4.3.2
3.4.3.2	As soon as reasonably practicable, following 3.4.3.1	The DCC shall issue a request for nominations, via a secured electronic means, to Parties, the DCC, the SMKI PMA and the Panel, for individuals to become Key Custodians for the Recovery Private Key or Contingency Private Key as identified in step 3.4.3.1. Such request for nominations shall: a. include the Key Custodian nomination form as published on the DCC Website; b. be marked as confidential; and c. detail the locations where each relevant Key Generation Ceremony and any corresponding Key Activation Ceremony will take place.	DCC	3.4.3.3
3.4.3.3	Within 10 Working Days of the issuance of the request for nominations	Each Party, the DCC, the SMKI PMA or the Panel wishing to nominate an individual to become a Key Custodian in respect of a particular Private Key shall provide, via secured electronic means, to the DCC for each nominated individual, a completed Key Custodian nomination form using the pro-forma as published on the DCC Website. The nomination form should contain the following information: a. the full name of a Director, Company Secretary or SMKI Senior Responsible Officer who is nominating the individual to become a Key Custodian for a Party, the DCC, the SMKI PMA Chair for the SMKI PMA or the Panel Chair for the Panel; b. the full name of the nominated individual; c. contact telephone details for the nominated individual;	Party, DCC, the SMKI PMA or the Panel	3.4.3.4

SEC - Appendix L

		d. the nominated individual's normal work location; e. the estimated time to travel to the location of the relevant Key Generation Ceremony and to the location of the corresponding Key Activation Ceremony, as notified in step 3.4.2; f. evidence that the individual is: - for a Party, an employee or Director of the Party; - for the DCC, an employee of the DCC or a DCC Service Provider; - for the SMKI PMA, an appointed member of the SMKI PMA; or - for the Panel, an appointed member of the Panel; and g. evidence that the nominated individual has successfully completed security screening in a manner that is compliant with: - British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or - any equivalent to that British Standard which updates or replaces it from time to time. Where necessary in order to have a sufficient number of Key Custodians appointed, the SMKI PMA may direct any Party to nominate individuals to become Key Custodians. Where this occurs, the directed Party shall identify and nominate individuals in accordance with this step 3.4.3.3.		
3.4.3.4	As soon as reasonably practicable following 3.4.3.3	The DCC shall determine: - using publicly available information, whether the Director, Company Secretary, SMKI Senior Responsible Officer, SMKI PMA Chair or Panel Chair who is nominating the individual to become a Key Custodian holds such a role on behalf of the organisation; and - whether the information supplied in the Key Custodian nomination form is complete and accurate. Where there are omissions/discrepancies, agree actions with the nominating Director, Company Secretary, SMKI Senior Responsible Officer, SMKI PMA Chair or Panel Chair, via secured electronic means or in writing.	DCC	If complete, 3.4.3.5; if not complete, 3.4.3.3
3.4.3.5	As soon as reasonably practicable,	The DCC shall collate nominations received and shall provide to SMKI PMA:	DCC	3.4.3.6

SEC - Appendix L

	following 10 Working Days after issuance of request for nominations	a. details of those nominated individuals and the organisation they are representing; and b. upon request from the SMKI PMA, details held by the DCC of all existing holders of Key Components.		
3.4.3.6	As soon as reasonably practicable, following 3.4.3.5	The SMKI PMA shall determine the individuals that shall become Key Custodians, which shall take into account geographical location and how many Key Components are held by any particular organisation or individual (where relevant). The SMKI PMA shall inform the DCC of the individuals which shall become Key Custodians.	SMKI PMA	3.4.3.7 if sufficient Key Custodians can be appointed; if not, 3.4.3.3
3.4.3.7	As soon as reasonably practicable, following 3.4.3.6	The DCC shall confirm that the individual has been selected by the SMKI PMA to become a Key Custodian and shall confirm the date and time for a verification meeting for the nominated individual at the DCC's offices, to the Director, Company Secretary, SMKI Senior Responsible Officer, SMKI PMA Chair or Panel Chair of the applicant organisation who nominated the individual to become a Key Custodian, via secured electronic means.	DCC	3.4.3.8
3.4.3.8	At verification meeting	The DCC shall, in person, verify the individual identity of the nominated individual to the level pursuant to the SMKI PMA Guidance on 'Verifying Individual Identity' published on the Website.	DCC	If successful for all, 3.4.3.10; for unsuccessful, 3.4.3.9
3.4.3.9	As soon as reasonably practicable following rejection	The DCC shall notify the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, in writing, that the nominated individual could	DCC	3.4.3.6

SEC - Appendix L

		not at that point be appointed as a Key Custodian.		
3.4.3.10	As soon as reasonably practicable, following 3.4.3.8	The DCC shall notify, in writing via secured electronic means: - the individual, in person, that they are eligible to become a Key Custodian; and - the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, that the nominated individual is eligible to become a Key Custodian.	DCC	3.4.3.11
3.4.3.11	As soon as reasonably practicable, following 3.4.3.10	The DCC shall: - update its records of eligible Key Custodians for Private Keys for which Key Components are issued and shall store such records in a secured manner; and - inform the SMKI PMA Chair, in writing, that the nominated individual has become a Key Custodian	DCC	Relevant procedure to recover from a notified Compromise

3.5 Recovery Actions Risk

3.5.1 Actions to be taken only after considering Recovery Action Risks

The actions detailed in this section 3.5.1 shall only be taken when those identified, in this document, as responsible for decision making have considered the risks detailed in sections 3.5.2 and 3.5.3 ('Recovery Action Risks'), and either concluded that they are not relevant or that, on balance, the risks of taking the actions are less than the risks of not taking them, having factored in any mitigations that have been, or are being, put in place. The timing of any such actions may therefore be delayed to a later time, including to ensure that mitigations are in place.

Such consideration shall factor in the risk that a Compromised Private Key may, depending on the Compromise, be used to send unauthorised instructions to the corresponding fleet of Devices, until the associated Certificates on SMETS2+ Devices have been replaced and also revoked (so that DCC systems will no longer accept their use).

The actions to be considered prior to a decision to undertake SMKI Recovery are:

- Any action that would lead to one or more Devices having their SMI status set to 'Recovery';
- The revocation of a Certificate;
- The destruction of a Private Key (or any other action that would render it unusable); or
- The placing of Access Control Broker Certificates in Supplier Trust Anchor Cells on a SMETS2+ Device, and therefore any request to use 'Method 2', with its section 4.2 meaning.

3.5.2 Prepayment functionality and continuity of Supply to the Consumer

Where a capitalised term in this section is not defined either in this document or in SEC Section A, that term shall have its SMETS meaning.

All SMETS ESME and GSME have the ability to operate in Prepayment Mode, a feature of which is that, when there is insufficient credit, Supply to the Premises will be Disabled. To ensure continuity of supply in recovering from a Compromise, it is important either that supplier prepayment functions can continue to operate during the

recovery, or that the potentially affected ESME and/or GSME are placed in a state where they will not Disable Supply during the recovery. For example, this could be achieved by switching such Devices to Credit mode and then locking out supplier functionality until recovery is complete.

Whilst the technical security mechanisms (and so potential effects of recovery actions) vary somewhat between SMETS1 and SMETS2+, the recovery actions that may affect operation in Prepayment Mode include:

- Destruction of XML Signing Private Keys, where they are used to sign Service Requests for prepayment functions, or revocation of associated Certificates. In the absence of replacements, this would mean all prepayment functionality, other the locally entered SMETS2+ top ups, would be lost;
- Destruction of supplier Private Keys, where they are used to sign Commands to SMETS2+ Devices. In the absence of a replacement, this would mean all SMETS2+ prepayment functionality, other the locally entered SMETS2+ top ups, would be lost. It is important to note that revocation of the associated supplier Certificates does NOT stop the supplier Private Keys being used to instruct SMETS2+ Devices;
- Destruction of supplier Private Keys, where they are used to create SMETS2+ top ups. In the absence of a replacement, and the corresponding update of supplier related Device Security Credentials (i.e. certificate information) on SMETS2+ Devices, this would prevent SMETS 2+ top ups. It is important to note that revocation of the associated supplier Certificates does NOT stop the supplier Private Keys being used to instruct SMETS2+ Devices;
- Replacement of supplier credentials on SMETS2+ Devices with Access Control Broker credentials. This locks out all supplier prepayment functionality on the Device, until the Access Control Broker credentials have subsequently successfully been replaced with valid supplier credentials;
- Revocation of Certificates associated with XML Signing Private Keys, which means that those Private Keys can no longer be used to sign XML needed to deliver prepayment functionality; and
- Setting the SMI Status of a Smart Meter to 'Recovery' which blocks prepayment functionality delivered via the DCC.

An important factor to consider is therefore the number of ESME and/or GSME that could be affected by the Compromise and are understood to currently be in Prepayment mode. However, it is important to note that certain Compromises could, in theory, allow Devices to be switched to Prepayment Mode without supplier authorisation. In such cases, the speed at which that potential risk is removed should also be factored in.

3.5.3 Devices in the supply chain

Where a capitalised term in this section is not defined either in this document or in SEC Section A, that term shall have its GBCS meaning.

To enforce end-to-end security, the SEC requires that SMETS2+ Devices have the range of security credentials, detailed in Figure 1, recorded in the Device's Trust Anchor Cells before installation. To that end, the DCC makes available a set of the following Certificates for loading on to Devices before installation. The relevant Certificates must be recorded on Devices before they are installed, otherwise enduring communications will not be possible:

- Root Certificate;
- Recovery Certificate;
- CoS Certificate; and
- Access Control Broker Certificates (one with a key usage of key agreement, and the other with a key usage of digital signature).

Additionally:

SEC - Appendix L

- Communications Hub Functions must hold information from a WAN Provider Certificate.
- ESME and GSME may hold information from Supplier Certificates, although information from Access Control Broker Certificates can be used in the Supplier and Network Operator Trust Anchor Cells.

Should any of the associated Private Keys (including the Contingency Private Key) be destroyed or made unusable as part of a recovery process, then it may no longer be possible to Commission Devices still in the supply chain, or such Commissioning may require keeping the Recovery or Contingency Private Key in extended operation, with the risks that brings.

In light of the potential economic costs and logistical disruption to the maintenance of metering, careful consideration should therefore be given to the destruction of, or making inoperable, any such Private Keys.

After a Contingency event as described in Section 6, all supply chain Devices will still be able to be commissioned and used by being updated to the new Root in a future Recovery Event to restore the Contingency capability.

4. Procedure to recover from the Compromise of a Private Key corresponding with a Public Key contained within an Organisation Certificate held on a SMETS2+ Device (other than the Recovery Private Key); or which forms part of any S1SP Held Device Security Credentials

This section sets out the procedures that may be used in order to recover from the Compromise of a Private Key associated with an Organisation Certificate held on a SMETS2+ Device (other than the Recovery Private Key), or to replace Organisation Certificates forming part of any S1SP Held Device Security Credentials where a Subscriber wishes to recover from the Compromise using this procedure.

Where a Subscriber wishes to recover from the Compromise of such a Private Key and its associated Public Key contained within the Organisation Certificate using any of the methods listed immediately below, it shall notify the DCC of which of the methods listed immediately below that it wishes to use, using the mechanisms as defined in the DCC's SMKI operational recovery procedures, which shall be made available by the DCC to Parties via secured electronic means. The DCC shall update the Incident Management Log to record such notification in accordance with H9.1(g).

- a) **Method 1:** the Subscriber shall seek to recover using the Compromised (or one suspected of being Compromised) Private Key (or any other relevant key held by the Subscriber) to replace the associated Organisation Certificate to which the Relevant Private Key relates on all affected SMETS2+ Devices;
- b) **Method 1A:** the Subscriber shall seek to recover using the Compromised (or one suspected of being Compromised) Private Key (or any other relevant key held by the Subscriber) to replace all affected S1SP Held Device Security Credentials to which the Relevant Private Key relates;
- c) **Method 2:** (only applicable where the Subscriber is a Supplier Party), the DCC shall use the Recovery Private Key to replace affected Certificates on SMETS2+ Devices with a DCC Access Control Broker Certificate. The Responsible Supplier shall then complete the recovery process by replacing the DCC Access Control Broker Certificate with new Organisation Certificates for which it is the Subscriber; or
- d) **Method 3:** the DCC shall recover using the Recovery Private Key to replace affected Organisation Certificates on SMETS2+ Devices with new Organisation Certificates provided by the Subscriber.

Following the notification of the selected recovery method by the Subscriber, the DCC shall:

- e) Where method 1 has been selected, perform the procedure as set out in Section 4.1 of this document;
- f) Where method 1A is being used, perform the procedure as set out in Section 4.1A of this document;
- g) Where method 2 has been selected, perform the procedure as set out in Section 4.2 of this document; or
- h) Where method 3 has been selected, perform the procedure as set out in Section 4.3 of this document.

4.1 Method 1 - recovery by the affected Subscriber using the Compromised Private Key (or any other relevant key held by the Subscriber) to replace the associated Organisation Certificates on SMETS2+ Devices

4.1.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate held on a SMETS2+ Devices, in accordance with section 3.2 of this document and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

Informative:

Where the Compromised Private Key is a supplier Private Key, there are two ways in which the Subscriber (the supplier) can, using Private Keys it controls, effect replacement of the associated Certificates. Specifically, it can use either of the two mechanisms provided for in DUIS:

- Update Security Credentials (KRP) (SRV 6.15.1) or
- Update Security Credentials (CoS) (SRV 6.23)

The 'CoS' mechanism will work regardless of the state of the supplier Digital Signature Private Key (so the key used to sign Commands to Devices), and so may have advantages in some scenarios, including in its allowing earlier destruction of any Compromised supplier Digital Signature Private Key.

Thus, in the scenario where the Compromised Private Key is a supplier Private Key, the Subscriber should always consider both DUIS options and factor that consideration in to assessing how best to recover from the Compromise.

- This section does not apply to XML Signing Private Keys. Please see Section 7 of this document for further guidance on the XML Signing Private Keys.
- This section is only applicable to Responsible Suppliers, Electricity Distributors, Gas Transporters and the DCC.

Step	When	Obligation	Responsibility	Next Step
4.1.1.1	As soon as possible, following notification that the Subscriber wishes to recover using its own Compromised (or one suspected of being Compromised) Private Key	The affected Subscriber shall consider the Recovery Action Risks before undertaking any of the associated actions. If the Private Key is not operable at this stage, the affected Subscriber should first consider using other Private Keys that it controls to affect the recovery. Specifically, if the Subscriber is a Supplier Party it should consider using other Private Keys to invoke	Subscriber	4.1.1.2 or 4.2

SEC - Appendix L

	associated with the Public Key contained within an Organisation Certificate held on a SMETS2+ Device	Update Security Credentials (CoS) (SRV 6.23) Service Requests as the certificate replacement method (including factoring in that this would not block prepayment functionality and would allow certificate replacement to Devices in the supply chain). If such methods are considered not viable or sufficient, the Subscriber should follow the Recovery Procedure as laid out in Section 4.2, Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected SMETS2+ Devices.		
4.1.1.2	As soon as reasonably practicable, following 4.1.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a. the Incident to which the submission relates; b. the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise of the Private Key relates; and c. for each Organisation Certificate that is affected by the Compromise of the associated Private Key, the serial number of the Organisation Certificate, the SMETS2+ Device IDs and the SMETS2+ Device Trust Anchor Cell which is populated with the affected Organisation Certificate related to the Compromised (or one suspected of being Compromised) Private Key. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to replace all affected Organisation Certificates on SMETS2+ Devices. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is submitted in accordance with the provisions of the TADP.	Subscriber	4.1.1.3
4.1.1.3	As soon as reasonably practicable, following 4.1.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a. that a Compromise of an Organisation's Private Key has been notified; b. that the Subscriber intends to use method 1 (as set out in section 4.1 of this document) to recover;	DCC	4.1.1.4

SEC - Appendix L

		c. which of the two sub-options that the Subscriber intends to use (i.e. Update Security Credentials (KRP) (SRV 6.15.1) or Update Security Credentials (CoS) (SRV 6.23) or a combination of the two); and <u>d.</u> of details relating to the Compromise, comprising the Subscriber and the number of SMETS2+ Devices affected, which will include the Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC; and d.e. of recommendations for any Global Anomaly Detection Threshold amendments		
4.1.1.4	As soon as reasonably practicable, following 4.1.1.3	Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.1.1.1, the DCC shall notify the Responsible Supplier, via secured electronic means, that a Subscriber wishes to recover from Compromise using its own Private Key. The DCC shall also provide to the Responsible Supplier, via a secured electronic means, one or more Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC, which together contain details of the SMETS2+ Device IDs to which the Compromise relates.	DCC	Procedure as set out in section 4.1.2 of this document

4.1.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.1.1 of this document except for 4.1.2.6 which may be undertaken at any time that is decided in accordance with these.

Step	When	Obligation	Responsibility	Next Step
4.1.2.1	As soon as reasonably practicable, following procedure as set out in section 4.1.1	The DCC shall apply the amended Anomaly Detection Thresholds for the affected Subscriber in accordance with the TADP. The DCC shall inform, via a secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.1.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1.2.2

SEC - Appendix L

		<u>The DCC shall apply any amended Global Anomaly Detection Thresholds that are agreed with SMKI PMA in accordance with the TADP.</u>		
4.1.2.2	As soon as reasonably practicable, following 4.1.2.1	The affected Subscriber shall either: a. identify replacement Organisation Certificates; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	4.1.2.3
4.1.2.3	As soon as reasonably practicable, following 4.1.2.2	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification, to replace affected Organisation Certificates on all relevant SMETS2+ Devices and shall, in doing so, monitor replacement of such affected Organisation Certificates.	Subscriber	4.1.2.4
4.1.2.4	As soon as reasonably practicable, following 4.1.2.3	Upon completion of its activities to replace affected Organisation Certificates on affected SMETS2+ Devices, the affected Subscriber shall inform the DCC, via a secured electronic means: a. that its activities in respect of the replacement of Organisation Certificates have been completed; and b. of the SMETS2+ Devices for which replacement of affected Organisation Certificates has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E.	Subscriber	4.1.2.6 or 4.1.2.5 if appropriate
4.1.2.5	As soon as reasonably practicable, following 4.1.2.4	Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.1.1.1, the DCC shall notify the Responsible Supplier for affected SMETS2+ Devices, via secured electronic means, which SMETS2+ Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in section 4.1.2.6 of this document

SEC - Appendix L

4.1.2.6	As decided after considering the Recovery Action Risks	The affected Subscriber shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the Subscriber concludes that, at this time, Certificates should not be revoked and / or Private Keys not destroyed, the Subscriber shall inform the SMKI PMA as to the rationale. The affected Subscriber may, having considered the Recovery Action Risks, submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Organisation Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP section 8.2. The affected Subscriber may, having considered the Recovery Action Risks, destroy the Private Key associated with the revoked Organisation Certificates.	Subscriber, DCC	Procedure as set out in section 4.1.3 of this document
---------	--	---	-----------------	--

4.1.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Private Key associated with an Organisation Certificate using the procedures as set out in sections 4.1.1 and 4.1.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.1.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.1.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, in accordance with the TADP. The DCC shall amend the relevant Anomaly Detection Thresholds in accordance with the TADP.	DCC (DSP TAD)	4.1.3.2
4.1.3.2	As soon as reasonably practicable, following 4.1.3.1	The DCC shall notify the SMKI PMA via a secured means of: the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1; and	DCC	End of procedure

		b. the SMETS2+ Devices for which recovery was not completed, which may be provided in one or more which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.		
--	--	---	--	--

4.1A Method 1A – replacement by the affected Subscriber using its Compromised Private Key of associated S1SP Held Device Security Credentials

4.1A.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate that forms a part of any S1SP Held Device Security Credentials, in accordance with section 3.2 of this document and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

Informative:

- Please see Section 7 of this document for further guidance on the XML Signing Private Keys.
- This section is only applicable to Responsible Suppliers, Electricity Distributors and Gas Transporters.
- All S1SP Held Device Security Credentials are Organisation Certificates.
- S1SP Held Device Security Credentials are held by the SMETS1 Service Provider and not on the SMETS1 Device.

Step	When	Obligation	Responsibility	Next Step
4.1A.1.1	As soon as possible, following notification that the Subscriber wishes to recover using its own Compromised (or one suspected of being Compromised) Private Key associated with the Public Key contained within an Organisation Certificate that forms part of any S1SP Held Device Security Credentials	The affected Subscriber shall consider the security risks arising from the Compromise of its Private Key and be aware that, until the Private Key is destroyed, there is a risk of the Private Key being used to achieve adverse consequences for the consumer. Revoking the Organisation Certificate (that forms part of any S1SP Held Device Security Credentials) containing the Public Key associated with the Compromised (or one suspected of being Compromised) Private Key will prevent the Private Key from being used to send authorised Commands to a SMETS1 Device. Due consideration should be given before destroying a Compromised (or one suspected of being Compromised) Private Key if the recovery steps detailed in 4.1A.2.1 to 4.1A.2.5 of this section have not yet been carried out. Destroying the Private Key prior to carrying out these steps may put pre-payment customers at risk. It would be advisable to conduct the replacement of Organisation Certificates that forms part of any S1SP Held Device Security Credentials as quickly as possible.	Subscriber	4.1A.1.2

SEC - Appendix L

4.1A.1.2	As soon as reasonably practicable, following 4.1A.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B. The affected Subscriber should ensure that such files together contain details of: a. the Incident to which the submission relates; b. the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise of the Private Key relates; and c. for each Organisation Certificate that forms part of any S1SP Held Device Security Credentials and is affected by the Compromise, the serial number of the Organisation Certificate, the SMETS1 Device IDs and the nature of the affected S1SP Held Device Security Credentials. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to replace the affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File submitted in accordance with the TADP.	Subscriber	4.1A.1.3
4.1A.1.3	As soon as reasonably practicable, following 4.1A.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a. that a Compromise of an Organisation's Private Key has been notified; b. that the Subscriber intends to use method 1 (as set out in section 4.1A of this document) to recover; and c. of details relating to the Compromise, comprising the Subscriber and the number of Organisation Certificates that form a part of any S1SP Held Device Security Credentials affected, which will include the Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	DCC	4.1A.1.4

4.1A.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.1A.1 of this document, except for 4.1A.2.6 which may be undertaken at any time that is decided in accordance with these.

Step	When	Obligation	Responsibility	Next Step
4.1A.2.1	As soon as reasonably practicable, following procedure as set out in section 4.1A.1	The DCC shall amend the Anomaly Detection Thresholds for the affected Subscriber in accordance with the TADP. The DCC shall inform, via a secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.1A.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1A.2.2
4.1A.2.2	As soon as reasonably practicable, following 4.1A.2.1	The affected Subscriber shall either: a) identify replacement Organisation Certificates that form a part of any S1SP Held Device Security Credentials; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that form a part of any S1SP Held Device Security Credentials.	Subscriber	4.1A.2.3
4.1A.2.3	As soon as reasonably practicable, following 4.1A.2.2	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification, to replace affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials and shall, in doing so, monitor replacement of such affected Organisation Certificates.	Subscriber	4.1A.2.4
4.1A.2.4	As soon as reasonably practicable, following 4.1A.2.3	Upon completion of its activities to replace affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials, the affected Subscriber shall inform the DCC, via a secured electronic means: a) that its activities in respect of the replacement of Organisation Certificates that form a part of any S1SP Held Device Security Credentials have been completed; and b) of the Organisation Certificates that form a part of any S1SP Held Device Security Credentials for which replacement has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set	Subscriber	4.1A.2.6 or 4.1A.2.5 if appropriate

SEC - Appendix L

		out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E.		
4.1A.2.5	As soon as reasonably practicable, following 4.1A.2.4	Where the affected Subscriber is not the Responsible Supplier for a SMETS1 Device that is notified in step 4.1A.1.1, the DCC shall notify the Responsible Supplier for affected SMETS1 Devices, via secured electronic means, which SMETS1 Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in section 4.1A.2.6 of this document
4.1A.2.6	As decided following consideration of the Recovery Action Risks, following 4.1A.2.4	The affected Subscriber shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the Subscriber concludes that, at this time, Certificates should not be revoked and / or Private Keys not destroyed, the Subscriber shall inform the SMKI PMA as to the rationale. The affected Subscriber may, having considered the Recovery Action Risks, submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials. The DCC shall revoke Organisation Certificates that form a part of any S1SP Held Device Security Credentials in accordance with the provisions of Appendix B of the Code and the SMKI RAPP. The affected Subscriber may, having considered the Recovery Action Risks, destroy the Private Key associated with the revoked Organisation Certificate that forms a part of any S1SP Held Device Security Credentials.	Subscriber, DCC	Procedure as set out in section 4.1A.3 of this document

4.1A.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Private Key associated with an Organisation Certificate using the procedures as set out in sections 4.1A.1 and 4.1A.2 of this document.

Step	When	Obligation	Responsibility	Next step
4.1A.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.1A.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, in accordance with the TADP. The DCC shall amend the relevant Anomaly Detection Thresholds in accordance with in the TADP.	DCC (DSP TAD)	4.1A.3.2
4.1A.3.2	As soon as reasonably practicable, following 4.1A.3.1	The DCC shall notify the SMKI PMA via a secured means of: a. the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1A; and b. the Organisation Certificates that form a part of any S1SP Held Device Security Credentials for which recovery was not completed, which may be provided in one or more which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	End of procedure

4.2. Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected SMETS2+ Devices

4.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document, and notification from the affected Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

The affected Subscriber shall only request use of the procedure in this section having considered the Recovery Action Risks, including that section 4.2.1.3 requires the DCC to disable access, via the DCC, to affected Devices **before the SMKI PMA has reached a decision as to whether to proceed**. For clarity, this includes disablement of all prepayment functionality operated via the DCC.

Step	When	Obligation	Responsibility	Next Step
------	------	------------	----------------	-----------

SEC - Appendix L

4.2.1.1	As soon as possible, following notification that the Subscriber wishes to recover using the procedure set out in section 4.2 of this document	The affected Subscriber should not take any action, prior to the SMKI PMA making a decision as to whether to use this procedure, that would prejudice that outcome unless they consider risks are sufficient to justify such advance actions. For clarity, this includes the actions to which Recovery Action Risks relate.	Subscriber, DCC	4.2.1.2
4.2.1.2	As soon as possible, following 4.2.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more Organisation Compromise Notification Files that each comply with Appendix B of this document and which together contain details of: a) the Incident to which the submission relates; b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c) for each Organisation Certificate that is affected by the Compromise, the serial number of the Organisation Certificate, the SMETS2+ Device IDs and the SMETS2+ Device Trust Anchor Cell which is populated with information from the affected Organisation Certificate. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the TADP; b) in the format as set out in section 5.3 of the TADP; and c) Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files as set out in section 6 of the TADP.	Subscriber	4.2.1.3
4.2.1.3	As soon as reasonably practicable, following 4.2.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise of an Organisation Certificate or Organisation Certificates, using the	DCC	4.2.1.4

SEC - Appendix L

		procedure as set out in section 4.2.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Certificates on SMETS2+ Devices). The DCC shall disable processing of communications destined for SMETS2+ Devices that it has been notified (in Step 4.2.1.2) are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those SMETS2+ Devices to 'recovery'. The DCC shall then request a decision from the SMKI PMA as to whether recovery should be carried out.		
4.2.1.4	As soon as reasonably practicable, following 4.2.1.3	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a) the number of affected SMETS2+ Devices, which may be provided in in one or more Organisation Compromise Notification Files that comply with Appendix B of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the steps that DCC reasonably believes should be taken to recover from the Compromise; and d) anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA.	DCC, Subscriber	4.2.1.5
4.2.1.5	As soon as reasonably practicable, following 4.2.1.4	The DCC shall notify the relevant Network Parties via secured electronic means: a) that a Responsible Supplier wishes to recover using the procedure as set out in section 4.2.2 of this document; and b) the SMETS2+ Device IDs to which the Compromise relates, which shall be submitted in one or more Organisation Compromise Notification Files that comply with Appendix B of this document.	DCC	4.2.1.6

SEC - Appendix L

4.2.1.6	As soon as reasonably practicable, following 4.2.1.5	Where the DCC believes that use of the Recovery Private Key is likely to be agreed by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): a) determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b) inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c) notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and d) activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	4.2.1.7
4.2.1.7	As soon as reasonably practicable, following 4.2.1.6	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; and b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.2.1.4 for recovery, are approved or whether alternate timescales should apply; and c. if the SMKI PMA has determined that steps in	SMKI PMA, DCC	4.2.1.8

		this procedure should be undertaken, detail the timing of actions that the Subscriber is to undertake, in terms of Private Key destruction and Certificate revocations, pursuant to section 4.2.2.10. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
4.2.1.8	As soon as reasonably practicable, following 4.2.1.7	The DCC shall inform the affected Subscriber, of the SMKI PMA's decision whether or not to execute the procedure as set out in section 4.2.2, and the timing of the section 4.2.2.10 actions that the Subscriber must undertake.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise procedure as set out in section 4.2.2 of this document

4.2.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.2.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.2.2.1	As soon as possible, following notification from the SMKI PMA to the DCC that this procedure should be executed	Should the decision of the SMKI PMA be not to disable device communications, the DCC shall re-enable communications to any SMETS2+ Devices where communications have previously been disabled by setting the SMI Status of any SMETS2+ Device that had been set to "recovery" pursuant to Step 4.2.1.3 back to the SMI Status each such SMETS2+ Device held immediately prior to the execution of step 4.2.1.3 of this procedure.	DCC	4.2.2.2

4.2.2.2	As soon as reasonably practicable, following 4.2.2.1	Where: a. The DCC is to issue Commands using the Recovery Private Key, the DCC shall, where necessary, amend the relevant Anomaly Detection Thresholds; and b. the affected Subscriber is to submit Service Requests to replace DCC Access Control Broker Certificates with Organisation Certificates, the Subscriber shall submit the necessary revised Anomaly Detection Thresholds in accordance with the TADP. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.2.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1A.2.3
4.2.2.3	As soon as reasonably practicable, following 4.2.2.2	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key.	DCC	4.2.2.4
4.2.2.4	As soon as reasonably practicable, following 4.2.2.3	The DCC shall send Commands to each affected SMETS2+ Device, Digitally Signed using the Recovery Private Key, in order to replace Organisation Certificates in all of the Supplier Trust Anchor Cells on SMETS2+ Devices as notified in step 4.2.1.2, with a DCC Access Control Broker Certificate. In doing so, the DCC shall monitor its	DCC	4.2.2.5

SEC - Appendix L

		Command acknowledgement records, to determine the progress of recovery in respect of SMETS2+ Devices affected by the Compromise.		
4.2.2.5	As soon as reasonably practicable, following 4.2.2.4	Upon completion of step 4.2.2.4 for each SMETS2+ Device, the DCC shall restore processing of communications destined for the affected SMETS2+ Device by setting the SMI Status to 'recovered'.	DCC	4.2.2.6
4.2.2.6	As soon as reasonably practicable, following 4.2.2.5	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected SMETS2+ Devices: a. upon replacement of affected Organisation Certificates on each SMETS2+ Device, using a DCC Alert issued via the DCC User Interface; and b. upon completion of attempts to replace all affected Organisation Certificates on relevant SMETS2+ Devices, in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document, provided via secured electronic means.	DCC	4.2.2.7
4.2.2.7	As soon as reasonably practicable, following 4.2.2.6	The affected Subscriber shall either: a. identify replacement Organisation Certificates; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates.	Subscriber	4.2.2.8
4.2.2.8	As soon as reasonably practicable, following 4.2.2.7	Where the DCC has recovered by replacing Organisation Certificates of the Responsible Supplier, with a DCC Access Control Broker Certificate, the Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace the DCC Access Control Broker Certificate in each Supplier SMETS2+ Device slot with a replacement Organisation Certificate, for each SMETS2+ Device as established in step 4.2.1.1 within section 4.2 of this document. Upon successful completion of such replacement for a SMETS2+ Device, the DCC shall set the SMI Status for that SMETS2+ Device to the SMI Status that was in place immediately prior to the execution of step 4.2.2.1 of this procedure.	Responsible Supplier	4.2.2.9

SEC - Appendix L

4.2.2.9	As soon as reasonably practicable, following 4.2.2.8	The Responsible Supplier shall notify the DCC in respect of replacement of such DCC Access Control Broker Certificates with new Organisation Certificates, via secured electronic means and in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document.	DCC	Procedure as set out in Section 4.2.2.10 of this document.
4.2.2.10	As required by the SMKI PMA	Where required by the SMKI PMA, the affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Organisation Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP. Where required by the SMKI PMA, the affected Subscriber shall destroy the Private Key associated with the revoked Organisation Certificate.	Subscriber, DCC	Procedure as set out in section 4.2.3 of this document

4.2.3 Post-Recovery

The procedure as set out immediately below shall be used following execution of the procedures as set out in sections 4.2.1 and 4.2.2 of this document.

Step	When	Obligation	Responsibility	Next Step
4.2.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.2.2 of this document	A SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC in accordance with the TADP. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the TADP. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.2 of this document.	DCC (DSP TAD)	4.2.3.2
4.2.3.2	As soon as reasonably practicable, following 4.2.3.1	The DCC shall notify the SMKI PMA, via a secured means, of:	DCC	End of procedure

		a. whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Organisation Compromise Recovery Progress Files that comply with Appendix C of this document; and b. the number of SMETS2+ Devices for which recovery was not successful.		
--	--	--	--	--

4.3. Method 3 - recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on SMETS2+ Devices

4.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate, in accordance with section 3.2 of this document, and notification from the relevant Subscriber that it wishes to recover from the Compromise using the procedure set out in this section.

The affected Subscriber shall only request use of the procedure in this section having considered the Recovery Action Risks, including that section 4.3.1.3 requires the DCC to disable access, via the DCC, to affected Devices **before the SMKI PMA has reached a decision as to whether to proceed**. For clarity, this includes all prepayment functionality operated via the DCC.

Step	When	Obligation	Responsibility	Next Step
4.3.1.1	As soon as possible, following notification that the Subscriber wishes to recover using the procedure set out in section 4.3.2 of this document	The affected Subscriber should not take any action, prior to the SMKI PMA making a decision as to whether to use this procedure, that would prejudice that outcome unless they consider risks are sufficient to justify such advance actions. For clarity, this includes the actions to which Recovery Action Risks relate.	Subscriber, DCC	4.3.1.2
4.3.1.2	As soon as reasonably practicable, following 4.3.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC. The affected Subscriber should ensure that such files together contain details of: a. the Incident to which the submission relates;	Subscriber	4.3.1.3

SEC - Appendix L

		b. the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise relates; and c. for each Organisation Certificate that is affected by the Compromise, the serial number of the Organisation Certificate, the SMETS2+ Device IDs and the SMETS2+ Device Trust Anchor Cell which is populated with information from the affected Organisation Certificate.		
4.3.1.3	As soon as reasonably practicable, following 4.3.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Subscriber wishes the DCC to recover from the Compromise of its Organisation Certificate using the procedure as set out in section 4.3.2 of this document (which requires use by the DCC of the Recovery Private Key to replace Organisation Certificates on SMETS2+ Devices). Where the Compromise affects Certificates where the Remote Party Role is supplier or wanProvider (with their GBCS meaning) the DCC shall disable processing of communications destined for those SMETS2+ Devices that it has been notified (in Step 4.3.1.2) that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status of those SMETS2+ Devices to 'recovery'. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	4.3.1.4
4.3.1.4	As soon as reasonably practicable, following 4.3.1.3	Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means: a. that a Subscriber wishes to recover using the procedure as set out in section 4.3.2 of this document; and b. the SMETS2+ Device IDs to which the Compromise relates, which shall be submitted in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	DCC	4.3.1.5
4.3.1.5	As soon as reasonably practicable, following 4.3.1.4	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should	DCC, Subscriber	4.3.1.6

SEC - Appendix L

		be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): - the number of affected SMETS2+ Devices, which may be provided in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC; - the extent to which the vulnerabilities that caused the Compromise have been addressed; - the steps that DCC reasonably believes should be taken to recover from the Compromise; and - anticipated timescales for recovery. The affected Subscriber shall take reasonable steps to provide information to the DCC in order for the DCC to provide such information to the SMKI PMA.		
4.3.1.6	As soon as reasonably practicable, following 4.3.1.5	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, the DCC shall identify such preparatory steps that it considers appropriate and either take such steps or instruct Parties to take steps as required, which may include (but shall not be limited to): - determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); - inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; - notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and - activities required to prepare such systems environments that are required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	4.3.1.7
4.3.1.7	As soon as reasonably practicable, following 4.3.1.6	The SMKI PMA shall:	SMKI PMA, DCC	4.3.1.8

		a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 4.3.1.5 for recovery, are approved or whether alternate timescales should apply; and c. if the SMKI PMA has determined that steps in this procedure should be undertaken, detail the actions that the Subscriber is to undertake, in terms of Private Key Destruction and Certificate revocations, including their timing. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
4.3.1.8	As soon as reasonably practicable, following 4.3.1.7	The DCC shall notify the affected Subscriber, via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2 and of the action the SMKI PMA requires the Subscriber to take in terms of Private Key destruction and Certificate revocation, and their timing. Where the affected Subscriber is not the Responsible Supplier for a SMETS2+ Device that is notified in step 4.3.1.2, the DCC shall notify the Responsible Supplier via secured electronic means, of the SMKI PMA's decision whether or not to execute the procedure (amended as directed by the SMKI PMA) as set out in section 4.3.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise procedure as set out in section 4.3.2 of this document

4.3.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA in accordance with section 4.3.1 of this document, shall be used, following execution of the process as set out in section 4.3.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.3.2.1	As soon as possible, following notification from the SMKI PMA to the DCC that this procedure should be executed	Should the decision of the SMKI PMA be not to disable device communications, the DCC shall re-enable communications to any devices where communications have previously been disabled by setting the SMI Status of any SMETS2+ Device that had been set to "recovery" pursuant to Step 4.3.1.3 back to the SMI Status each such SMETS2+ Device held immediately prior to the execution of step 4.3.1.3 of this procedure.	DCC	4.3.2.2

SEC - Appendix L

4.3.2.2	As soon as possible, following 4.3.2.1	Where necessary, the DCC shall temporarily amend the relevant Anomaly Detection Thresholds, for: a) the DCC that relate to the issuance of Commands to replace Organisation Certificates on SMETS2+ Devices, to enable replacement of affected Organisation Certificates as notified in section 4.3.1 of this document. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 4.3.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.3.2.3
4.3.2.3	As soon as reasonably practicable, following 4.3.2.2	The affected Subscriber shall either: a. identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Private Key; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are not Digitally Signed by the Compromised Private Key. The affected Subscriber shall notify the DCC of the serial numbers of the replacement Organisation Certificates that should be used to populate a SMETS2+ Device and specify the SMETS2+ Device Trust Anchor Cell to which the replacement Organisation Certificate relates, which shall be provided via secured electronic means in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Appendix B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Appendix D where the Subscriber is the DCC.	Subscriber	4.3.2.4
4.3.2.4	As soon as reasonably practicable, following 4.3.2.3	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the Recovery Private Key.	DCC	4.3.2.5
4.3.2.5	As soon as reasonably practicable, following 4.3.2.4	The DCC shall send Commands to all SMETS2+ Devices, Digitally Signed using the Recovery Private Key, in order to replace affected Organisation Certificates on relevant SMETS2+ Devices as notified in step 4.3.1.1 with replacement Organisation Certificates as notified by the affected Subscriber. In doing so, the DCC shall monitor	DCC	4.3.2.6

SEC - Appendix L

		its Command acknowledgement records, to determine the progress of recovery in respect of SMETS2+ Devices affected by the Compromise.		
4.3.2.6	As soon as reasonably practicable, following 4.3.2.5	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected SMETS2+ Devices: a. upon replacement of affected Organisation Certificates on each SMETS2+ Device, using a DCC Alert issued via the DCC User Interface; and b. upon completion of attempts to replace all affected Organisation Certificates on relevant SMETS2+ Devices, in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC, provided by secured electronic means.	DCC	4.3.2.7
4.3.2.7	As soon as reasonably practicable, following 4.3.2.6	Upon completion of step 4.3.2.6 for each SMETS2+ Device, the DCC shall restore processing of communications destined for the affected SMETS2+ Device by setting the SMI Status for that SMETS2+ Device to the SMI Status that was in place immediately prior to the execution of step 4.3.2.1 of this procedure.	DCC	4.3.2.8
4.3.2.8	As soon as reasonably practicable, following 4.3.2.7	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, by secured electronic means, which SMETS2+ Devices were not recovered successfully in one or more one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC.	DCC	Procedure as set out in Section 4.3.3 of this document.

4.3.3 Post-Recovery

The procedure as set out immediately below shall be used following execution of the procedures as set out in sections 4.3.1 and 4.3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
------	------	------------	----------------	-----------

4.3.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 4.3.2 of this document	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 4.3 of this document.	DCC (DSP TAD)	4.3.3.2
4.3.3.2	As soon as reasonably practicable, following 4.3.3.1	The DCC shall notify the SMKI PMA, via a secured electronic means, of: - whether the recovery from the Compromise has been successfully completed, which may be provided in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Appendix C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Appendix E where the Subscriber is the DCC; and - the number of SMETS2+ Devices for which recovery was not successful.	DCC	End of procedure

5. Recovery using the Contingency Private Key

5.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following:

- the notification of the Compromise of the Root OCA Private Key, in accordance with section 3.2 of this document; or
- where the use of the Recovery Private Key has been unsuccessful (as set out in sections 4.2, 4.3, 6.2 and 6.3 of this document) and the DCC reasonably believes that the nature of the Compromise could require use of the Contingency Private Key.

The DCC shall only request use of the procedure in this section having considered the Recovery Action Risks, including that, for the time between the action in section 5.2.1 and those in section 5.3.2, access, via the DCC, to affected Devices will not be possible. For clarity, this includes all prepayment functionality operated via the DCC.

Step	When	Obligation	Responsibility	Next Step
5.1.1	As soon as reasonably practicable, following notification of the Compromise of the Root OCA	The DCC shall notify the SMKI PMA and all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Root OCA Key has been notified, or that use of the Recovery Private Key has been unsuccessful that the DCC reasonably believes that the nature of the Compromise	DCC	5.1.2

SEC - Appendix L

	Private Key or escalation due to failure of recovery using the Recovery Private Key, in accordance with section 3.2 of this document	could require use of the Contingency Private Key. The DCC shall also provide details to affected Subscribers of the affected SMETS2+ Devices and Organisation Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.		
5.1.2	As soon as reasonably practicable, following 5.1.1	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the affected SMETS2+ Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b. the extent to which DCC's monitoring indicates that there has been unauthorised use of the Root OCA Private Key; c. the extent to which the vulnerabilities that caused the Compromise have been addressed; d. information relevant to the SMKI PMA's consideration of the Recovery Action Risks; e. the steps that DCC reasonably believes should be taken to recover from the Compromise; and f. anticipated timescales for recovery.	DCC	5.1.3
5.1.3	As soon as reasonably practicable, following 5.1.2	Where the DCC believes that use of the Contingency Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a. inform the requisite number of Key Custodians, via a secured electronic means, that a Key Activation Ceremony for the Contingency Private Key is required (which may be greater than the minimum number required to activate the Contingency Private Key), and the date, time and location of each Key Activation Ceremony;	DCC, Key Custodians	5.1.4

		b. notifying Key Custodians to attend the location at which a relevant Key Activation Ceremony may be required; and c. activities required to prepare the systems environment required to support activation and use of the Contingency Private Key.		
5.1.4	As soon as reasonably practicable, following 5.1.3	Having considered the Recovery Action Risks, the SMKI PMA shall: a. determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 5.1.2 for recovery, are approved or whether alternate timescales should apply; and c. for Certificates and Private Keys in the scope of section 5.1.6, determine which of the DCC controlled Private Keys are to be destroyed, and which of the DCC controlled Certificates are to be revoked and when. For clarity, the old Contingency Symmetric Key and old Contingency Private must not be	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 5.1.5

		destroyed until all Commands that are needed pursuant to section 5.2.8 (including for any Device in the supply chain) have been created, since when they are destroyed, no further such Commands can be created. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.		
5.1.5	As soon as reasonably practicable, following 5.1.4	The DCC shall notify affected Subscribers, via a secured electronic means, of the SMKI PMA's decision whether or not to execute the recovery procedure (amended as directed by the SMKI PMA) as set out in section 5.2.	DCC	Where required by SMKI PMA, 5.1.6; otherwise End of procedure
5.1.6	As directed by the SMKI PMA	The DCC shall execute steps in order, where applicable in accordance with the SMKI PMA's decision, to revoke: a. the Root OCA Certificate; b. the associated Issuing OCA Certificate(s) As described in section 5.1.4 c, the DCC shall may be directed to update and lodge the relevant ARL in the SMKI Repository, and shall <u>The DCC may be directed to</u> destroy affected Private Keys and Symmetric Keys, which may include: a. the old Root OCA Private Key; b. the old Issuing OCA Private Key(s); c. the old Contingency Private Key; and d. the old Contingency Symmetric Key.	DCC	Procedure as set out in section 5.2 of this document

5.2 Execution of Recovery Procedure

The DCC shall execute the steps as notified by the SMKI PMA, in accordance with the procedure in section 5.1 of this document, which may include (but will not be limited to) some or all of the steps as set out in this section 5.2.

Step	When	Obligation	Responsibility	Next Step
5.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that recovery using the Contingency Private Key should be carried out	The DCC shall disable processing of communications destined for SMETS2+ Devices that are affected by the Compromise, for all Parties other than the DCC, by setting the SMI Status to 'recovery'.	DCC	5.2.2
5.2.3	As soon as possible, following 5.2.2	Where: a. The DCC is to issue Commands using the Contingency Private Key, the DCC shall, where necessary, amend the relevant Anomaly Detection Thresholds; and b. the affected Subscriber is to submit Service Requests to replace DCC Access Control Broker Certificates with Organisation Certificates, the Subscriber shall submit the necessary revised Anomaly Detection Thresholds in accordance with the TADP. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 5.2.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	5.2.4
5.2.4	As soon as reasonably practicable, following 5.2.3	The DCC, shall conduct relevant Key Generation Ceremonies in accordance with the Organisation <u>CP and Organisation CPS and DCC local procedures</u>, in order to generate: The DCC shall securely transport the new Contingency Public Key from DSP to TSP a. a new Contingency Symmetric Key;		5.2.4b5

		a. a new Contingency Key Pair; b. <u>a new Contingency Symmetric Key;</u> c. a new wrappedApexContingencyKey; d. a new Root OCA Key Pair; and e. a new Issuing OCA Key Pair.		
<u>5.2.4a</u>	<u>As soon as reasonably practicable, following 5.2.4</u>	<u>Where directed by the SMKI PMA, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the Organisation CP and Organisation CPS, in order to generate the following: a new Contingency Key Pair</u> <u>The DCC shall make the public key available to the TSP.</u>	<u>DCC (as DSP)</u>	<u>5.2.4b</u>
<u>5.2.4bb</u>	<u>As soon as reasonably practicable, following 5.2.4a</u>	<u>Where directed by the SMKI PMA, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the Organisation CP and Organisation CPS, in order to generate the following: new Contingency Symmetric Key</u> <u>The DCC shall use the new Contingency Symmetric Key to encrypt the new Contingency Public Key to produce the value to be placed in the WrappedApexContingencyKey extension (with the meaning of IETF RFC 5934 section 9) in the new Root OCA Certificate.</u>	<u>DCC (as TSP)</u>	<u>5.2.5</u>
5.2.5	As soon as reasonably practicable, following 5.2.4	The DCC shall generate a new Root OCA Certificate, embedding the new wrappedApexContingencyKey that has been generated as part of the process as set out in step 5.2.4 of this document. The new Root OCA Certificate shall be Digitally Signed by the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate signed by the new Root OCA Private Key.	DCC (as TSP)	5.2.6
5.2.6	As soon as reasonably practicable, following 5.2.5	The DCC shall lodge the new Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.	DCC	5.2.7

SEC - Appendix L

5.2.7	As soon as reasonably practicable, following 5.2.6	The DCC, in collaboration with Key Custodians, shall participate in a Key Activation Ceremony to activate the old Contingency Private Key and the plain text version of the old Contingency Symmetric Key that were used to generate the wrappedApexContingencyKey that is stored within the old Root OCA Certificate that has been deployed to SMETS2+ Devices. To facilitate this, the DCC shall bring together all parts of the old Contingency Symmetric Key.	DCC <u>(as DSP)</u>	5.2.8
5.2.8	As soon as reasonably practicable, following 5.2.7	The DCC shall send Commands to all SMETS2+ Devices, Digitally Signed using the old Contingency Private Key and including the old Contingency Symmetric Key to enable activation, attaching the following Certificates (where applicable according to the SMETS2+ Device type) to the corresponding SMETS2+ Devices: a. a new Root OCA Certificate; b. a replacement new DCC Transitional -CoS Certificate; c. a replacement new Recovery Certificate; d. a replacement new DCC Access Control Broker Certificate; e. a replacement new DCC WAN Provider Certificate; and f. a new DCC Access Control Broker Certificate which shall be placed in each Supplier SMETS2+ Device Trust Anchor Cell or Network Operator SMETS2+ Device Trust Anchor Cell in the corresponding SMETS2+ Device.	DCC	5.2.9
5.2.9	As soon as reasonably practicable, following 5.2.8	Upon completion of step 5.2.8 for each SMETS2+ Device, the DCC shall restore processing of communications destined for the affected SMETS2+ Device by setting the SMI Status to 'recovered'.	DCC	5.2.10
5.2.10	As soon as reasonably practicable, following 5.2.9	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of SMETS2+ Devices affected by the Compromise.	DCC	5.2.11

SEC - Appendix L

5.2.11	As soon as reasonably practicable, following 5.2.10	The DCC shall notify the affected Subscriber of the replacement of Organisation Certificates on affected SMETS2+ Devices: a. upon replacement of affected Organisation Certificates on each SMETS2+ Device with a DCC Access Broker Certificate, via DCC Alert issued via the DCC User Interface to the affected Subscriber; and b. upon completion of attempts to replace all affected Organisation Certificates (for each affected Subscriber) on relevant SMETS2+ Devices, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, which shall be provided via secured electronic means.	DCC	5.2.12
5.2.12	As soon as reasonably practicable, following 5.2.11	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, via secured electronic means, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, which SMETS2+ Devices were not recovered successfully.	DCC	Procedure as set out in Section 5.3 of this document

5.3 Post Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Root OCA Private Key.

Step	When	Obligation	Responsibility	Next Step
5.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 5.2 of this document	The affected Subscriber shall generate new Private Keys and Certificate Signing Requests (CSRs), and submit such CSRs that are required in order to acquire new associated Organisation Certificates.	Subscriber	5.3.2
5.3.2	As soon as reasonably practicable, following 5.3.1	The Responsible Supplier shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, to replace:	Subscriber	5.3.3

		a. the DCC Access Control Broker Certificate in each Supplier SMETS2+ Device Trust Anchor Cell with a replacement Organisation Certificate that is Issued under the new Issuing OCA, for each SMETS2+ Device as established in step 5.2.2 within section 5.2 of this document; and b. the DCC Access Control Broker Certificate in each Network Operator SMETS2+ Device Trust Anchor Cell with an Organisation Certificate to which the Network Operator is the Subscriber that is Issued under the new Issuing OCA, for each SMETS2+ Device as established in step 5.2.2 within section 5.2 of this document. Upon successful completion of such replacement for a SMETS2+ Device, the DCC shall set the SMI Status for that SMETS2+ Device to the SMI Status that was in place immediately prior to the execution of step 5.2.1 of this procedure. The Responsible Supplier shall notify the DCC in respect of replacement of affected Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.		
5.3.3	As soon as reasonably practicable, following 5.3.2	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC, which shall be submitted as a file as set out in section 5.1 of the TADP that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the Subscriber for the purpose of Digital Signing of files. The DCC shall amend the relevant Anomaly Detection Thresholds to the values as submitted by the affected Subscriber, including performing the checks and validations set out in the TADP. The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 5 of this document.	Subscriber, DCC (DSP TAD)	5.3.4

5.3.4	As soon as reasonably practicable, following 5.3.3	The DCC shall notify the SMKI PMA and affected Subscribers, via a secured means, of: a. whether the recovery from the Compromise has been successfully completed, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document; and b. the number of SMETS2+ Devices for which recovery was not successful.	DCC	End of procedure 5.3.5
-------	--	--	-----	-----------------------------------

<u>5.3.5</u>	<u>As soon as reasonably practicable, following 5.3.4</u>	<u>If the compromised key material remains available to the DCC, then the DCC may be directed by the SMKI PMA to issue CRLs/ARLs for the impacted Organisation Certificates.</u> <u>The DCC may be directed to revoke and destroy affected Private Keys and Symmetric Keys, which may include:</u> <u>a. the old Root OCA Private Key;</u> <u>b. the old Issuing OCA Private Key(s);</u> <u>c. the old Contingency Private Key; and</u> <u>d. the old Contingency Symmetric Key.</u>	DCC	<u>End of procedure</u>
--------------	---	--	-----	-------------------------

6. Recovery from Compromise of a Contingency Private Key, Contingency Symmetric Key, Recovery Private Key or Issuing OCA Private Key

6.1 Recovery from Compromise of a Contingency Private Key or the Contingency Symmetric Key

This will replace only the Root OCA Certificate. All subordinate certificates remain valid as the Root OCA Key Pair does not change.

6.1.1 Pre-Recovery

Where the DCC becomes aware that a Compromise to the Contingency Private Key or the Contingency Symmetric Key has occurred, the DCC shall raise an Incident in accordance with sections 2.1 and 2.2 of the Incident Management Policy and shall execute the procedure as set out immediately below.

SEC - Appendix L

Step	When	Obligation	Responsibility	Next Step
6.1.1.1	As soon as reasonably practicable, following notification of the Compromise of the Contingency Private Key or Contingency Symmetric Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Contingency Private Key or Contingency Symmetric Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.1.1.2
6.1.1.2	As soon as reasonably practicable, following 6.1.1.1	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the extent to which the vulnerabilities that caused the Compromise have been addressed; b. <u>b.</u> the extent to which DCC's monitoring indicates that there has been unauthorised use of the Contingency Private Key and/or Contingency Symmetric Key; c. <u>c.</u> the likely impact on Services if Recovery is carried out; b.d. <u>d.</u> the likely impact on Services if the Compromise were to be exploited; e.e. <u>e.</u> the steps that DCC reasonably believes should be taken to recover from the Compromise; and d.f. <u>f.</u> anticipated timescales for recovery.	DCC, SMKI PMA	6.1.1.3
6.1.1.3	As soon as reasonably practicable, following 6.1.1.2	Where the DCC believes that replacement of the Contingency Key Pair and generation of a replacement Root OCA Certificate (and therefore a new Contingency Private Key and Contingency Symmetric Key) is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to take steps as required, including (but not limited to): a. informing the requisite number of Key Custodians, via a secured electronic means, that a Key Generation Ceremony for the Contingency	DCC, Key Custodians	6.1.1.4

SEC - Appendix L

		Key Pair, and for the Contingency Symmetric Key is required and the date, time and location of each such Key Generation Ceremony; b. notifying Key Custodians to attend the relevant Key Generation Ceremony; and c. activities required to prepare such systems environment required to support: a. generation of a new Contingency Key Pair; b. creating a new M#N Share of the Contingency Private Key; c. generation of a new Contingency Symmetric Key; d. encryption of the new Contingency Public Key using the new Contingency Symmetric Key; e. for the new symmetric key, conducting Contingency Symmetric Key Splitting; f. generation of a replacement Root OCA Certificate, containing the Public Key from the current Root OCA Certificate and the new encrypted Contingency Public Key; - g.		
6.1.1.4	As soon as reasonably practicable, following 6.1.1.3	The SMKI PMA shall: a. determine which of the steps (if any) as set out in section 5 4.2.2 of this document should be executed, in order to recover from the Compromise; b. confirm whether the timescales proposed by the DCC in step 6.1.1.3 for recovery, are approved or whether alternate timescales should apply; and c. consider preparing a communication for notifying Subscribers and instruct the DCC that the SMKI PMA will determine whether and, if so, what the timing of issue should be of any such a notification. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of procedure; otherwise 6.1.2

6.1.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 6.1.1 of this document.

Step	When	Obligation	Responsibility	Next Step
6.1.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	The DCC shall temporarily amend the Anomaly Detection Thresholds for the CS02b Update Security Credentials (anyExceptAbnormalRootByRecovery) Command (where those terms have their GBCS meaning) from 0 to the level required to instruct all affected SMETS2+ Devices. The DCC should perform the checks and validations set out in the TADP, for the DCC that relate to the issuance of recovery Commands to replace Root OCA Certificates on SMETS2+ Devices.	DCC	6.1.2.2
6.1.2.2	As soon as reasonably practicable, following 6.1.2.1	Where directed by the SMKI PMA, the DCC shall conduct relevant Key Generation Ceremonies <u>in accordance with the Organisation CP and Organisation CPS</u> , in order to generate the following a new Contingency Key Pair: a. a new Contingency Symmetric Key; and b. a new Contingency Key Pair The DCC <u>shall securely transport the new Contingency Public Key from DSP to TSP</u> shall use the new Contingency Symmetric Key to encrypt the new Contingency Public Key to produce the value to be placed in the WrappedApexContingencyKey extension (with the meaning of IETF RFC 5934 section 9) in the new Root OCA Certificate.	DCC <u>(as DSP)</u>	6.1.2.2a
<u>6.1.2.2a</u>	<u>As soon as reasonably practicable, following 6.1.2.2a</u>	<u>Where directed by the SMKI PMA, in accordance with 6.1.2.2, the DCC shall conduct relevant Key Generation Ceremonies in accordance with the Organisation CP and Organisation CPS, in order to generate a new Contingency Symmetric Key</u> <u>The DCC shall use the new Contingency Symmetric Key to encrypt the new Contingency Public Key to produce the value to be placed in the WrappedApexContingencyKey extension (with the meaning of IETF RFC 5934 section 9) in the new Root OCA Certificate.</u>	<u>DCC (as TSP)</u>	<u>6.1.2.3</u>

6.1.2.3	As soon as reasonably practicable, following 6.1.2.2	The DCC shall generate a new Root OCA Certificate, embedding the new <code>WrappedApexContingencyKey</code> that has been generated as part of the process as set out in step 6.1.2.2 of this document. The replacement Root OCA Certificate shall be Digitally Signed by the <u>existing</u> Root OCA Private Key.	DCC <u>(as TSP)</u>	6.1.2.4
6.1.2.4	As soon as reasonably practicable, following 6.1.2.4	The DCC shall lodge the new Root OCA Certificate in the SMKI Repository.	DCC	6.1.2.5
6.1.2.5	As soon as reasonably practicable, following 6.1.2.4	The DCC shall: - retrieve <u>only</u> the new Root OCA Certificate from the SMKI Repository; - create the CS02b Update Security Credentials (<code>anyExceptAbnormalRootByRecovery</code>) Commands (where those terms have their GBCS meaning) as are required to replace the existing Root OCA Certificate <u>alone</u> on all SMETS2+ Devices (excluding IHDs) with the new Root OCA Certificate. - In such Commands the DCC shall use the new Root OCA Certificate as both the <code>NewWithOld</code> and <code>NewWithNew certificates</code> (where those terms have their GBCS meaning); and - Shall produce a list of the affected Devices by type in a proposed priority order of ESME, SAPC, HCALCS, GSME and PPMID and provide this to the SMKI PMA seeking guidance on any other prioritisation that might be needed.	DCC	6.1.2.6
6.1.2.6		On receipt of guidance from the SMKI PMA on any other priority order for recovery, the DCC shall send the resulting Commands to the target SMETS2+ Devices, undertaking retries where Responses indicate failure or Responses are not received.	DCC	6.1.2.7
6.1.2.7	As soon as reasonably practicable, following 6.1.2.6	The DCC shall monitor Responses to the Commands sent pursuant to 6.1.2.5, to determine the progress of recovery in respect of replacement of the Root OCA Certificate on SMETS2+ Devices. The DCC shall also continue to monitor for any unauthorised use of the Contingency Private Key/Contingency Symmetric Key and	DCC	6.1.2.8

SEC - Appendix L

		shall take all reasonable steps to keep the SMKI PMA informed of progress throughout and of any such unauthorised use. Where directed by the SMKI PMA to amend the recovery steps as a result of unauthorised use, the DCC execute steps as notified by the SMKI PMA.		
6.1.2.8	As soon as reasonably practicable, following 6.1.2.6	The DCC shall update the SMKI PMA with regular progress reports throughout the Recovery process on the steps taken; on the volumes of SMETS2+ Devices that are satisfactorily updated; on the volumes remaining to be updated; and on the number, type and Responsible Supplier of failed retries and shall seek a direction on: a. when to stop further re-tries; b. if and when to notify Subscribers; and c. for details of any communication to be sent to Subscribers.	DCC	6.1.3
6.1.2.9	As soon as reasonably practicable, following 6.1.2.8	On receipt of notification from the SMKI PMA, the DCC shall follow the instruction to either: a. continue to make efforts to recover all or some of the affected SMETS2+ Devices; or b. cease the recovery action; and c. to notify Subscribers as required by the SMKI PMA.	DCC	6.1.3

6.1.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Contingency Private Key or the Contingency Symmetric Key.

Step	When	Obligation	Responsibility	Next Step
6.1.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.1.2 of this document, as applicable	The DCC shall amend the Anomaly Detection Thresholds for the CS02b Update Security Credentials (anyExceptAbnormalRootByRecovery) Command (where those terms have their GBCS meaning) back to zero (0).	DCC	6.1.3.2

SEC - Appendix L

6.1.3.2	As soon as reasonably practicable, following 6.1.3.1	The DCC shall seek instruction from SMKI PMA as to whether to destroy the replaced Contingency Private Key and Contingency Symmetric Key.	DCC	6.1.3.3
6.1.3.3	As soon as reasonably practicable following 6.1.3.2	The SMKI PMA shall consider the implications and handling instructions for unrecovered Devices and for Devices still in the supply chain. When SMKI PMA is satisfied that it is appropriate to destroy the replaced Contingency Private Key and Contingency Symmetric Key Pair, the SMKI PMA shall instruct the DCC to initiate the destruction process.	SMKI PMA	6.1.3.4
6.1.3.4	As soon as reasonably practicable, following 6.1.3.3	The DCC shall notify the SMKI PMA, via a secured means of: a. whether all the instructions from the SMKI PMA have been successfully completed; b. the number, type and Responsible Supplier associated with the SMETS2+ Devices for which recovery was not successful; c. confirmation that the replaced Contingency Private Key and Contingency Symmetric Key Pair have been destroyed; d. details of any communications received from Users in response to any communication provided by the SMKI PMA; e. details of any Lessons Learned by the DCC from the Recovery Event; and f. the estimated costs of the Recovery Event.	DCC	End of procedure

6.2 Recovery from Compromise of the Recovery Private Key

6.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of the Recovery Private Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.2.1.1	As soon as reasonably practicable, following notification of the	The DCC shall notify the SMKI PMA, via a secured electronic	DCC	6.2.1.2

SEC - Appendix L

		Compromise of the Recovery Private Key, in accordance with section 3.2 of this document	means, as soon as reasonably practicable, that a Compromise, or suspected Compromise, of the Recovery Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.		
6.2.1.2	As soon as reasonably practicable, following 6.2.1.1	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means that the Compromise of the Recovery Private Key has been notified and shall provide details of the affected SMETS2+ Devices and Organisation Certificates, in one or more Other Compromise Notification Files which comply with Appendix D of this document.	DCC	6.2.1.3	
6.2.1.3	As soon as reasonably practicable, following 6.2.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the number of affected SMETS2+ Devices and Subscribers, which may be provided in one or more Other Compromise Notification Files which comply with Appendix D of this document; b. the extent to which DCC's monitoring indicates that there has been unauthorised use of the Recovery Private Key; c. the extent to which the vulnerabilities that caused the Compromise have been addressed; d. the steps that DCC reasonably believes should be taken to recover from the Compromise; and e. anticipated timescales for recovery.	DCC, SMKI PMA	6.2.1.4	
6.2.1.4	As soon as reasonably practicable, following 6.2.1.3	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers	DCC, Key Custodians	6.2.1.5	

SEC - Appendix L

		appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): - determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); - inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and - notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and - activities required to prepare such systems environment required to support activation and use of the Recovery Private Key.		
6.2.1.5	As soon as reasonably practicable, following 6.2.1.4	The SMKI PMA shall: - determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; and - confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.2.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 6.2.1.6
6.2.1.6	As soon as reasonably practicable, following 6.2.1.5	The DCC shall notify all Subscribers to Organisation Certificates, by secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.2.2.	DCC	Procedure as set out in section 6.2.2 of this document

6.2.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA in accordance with section 6.2.1 of this document, shall be used when a Recovery Private Key has been Compromised.

Step	When	Obligation	Responsibility	Next Step
------	------	------------	----------------	-----------

SEC - Appendix L

6.2.2.1	As soon as reasonably practicable, following confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds for the DCC that relate to the issuance of Commands to replace Organisation Certificates on SMETS2+ Devices, to enable replacement of affected Organisation Certificates as notified in section 4.2.1 of this document.	DCC (DSP TAD)	6.2.2.2
6.2.2.2	As soon as reasonably practicable, following 6.2.2.1	The DCC shall: a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c. participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key.	DCC, Key Custodians	6.2.2.3
6.2.2.3	As soon as reasonably practicable, following 6.2.2.2	The DCC shall: a. determine the number of Key Custodians required to attend a Key Generation Ceremony for the Recovery Private Key; b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and c. participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate.	DCC, Key Custodians	6.2.2.4
6.2.2.4	As soon as reasonably practicable, following 6.2.2.3	The DCC shall send Commands to all SMETS2+ Devices to replace the Recovery Certificate held on such SMETS2+ Devices with the Recovery Certificate generated in step 6.2.2.3. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key.	DCC (as DSP)	6.2.2.5

SEC - Appendix L

		Once submitted, the DCC shall confirm for each affected SMETS2+ Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure.		
6.2.2.5	As soon as reasonably practicable, following 6.2.2.4	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, by secured electronic means, which SMETS2+ Devices were not recovered successfully, in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	Procedure as set out in Section 6.2.3 of this document

6.2.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of a Recovery Private Key, as set out in section 6.2.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.2.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.2.2 of this document, as applicable	The DCC shall reinstate its relevant Anomaly Detection Threshold values that were in place immediately prior to the temporary values used during the execution of the procedure set out in this Section 6.2 of this document.	DCC (DSP TAD)	6.2.3.2
6.2.3.2	As soon as reasonably practicable, following 6.2.3.1	<u>The DCC shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the DCC concludes that, at this time, the Recovery Certificates should not be revoked and / or Private Keys not destroyed, the DCC shall inform the SMKI PMA as to the rationale.</u> <u>The DCC may, having considered the Recovery Action Risks, submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Recovery Certificates.</u> <u>The DCC shall revoke Recovery Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP section 8.2.</u> <u>The DCC may, having considered the Recovery Action Risks, destroy the Recovery Private Key associated with the revoked Recovery Certificates. The DCC shall destroy</u>	DCC (as DSP)	6.2.3.3

		the replaced Recovery Private Key and shall revoke the Recovery Certificate that has been replaced in the procedure as set out in Section 6.2.2 of this document.		
6.2.3.3	As soon as reasonably practicable, following 6.2.3.2	The DCC shall notify the SMKI PMA, via secured electronic means of: a. whether the recovery from the Compromise has been successfully completed; and b. the number of SMETS2+ Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	End of procedure

6.3 Recovery from Compromise of the Issuing OCA Private Key

6.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise of an Issuing OCA Private Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.3.1.1	As soon as reasonably practicable, following notification of the Compromise of an Issuing OCA Private Key, in accordance with section 3.2 of this document	The DCC shall notify the SMKI PMA and each Subscriber to affected Organisation Certificates, via a secured electronic means, as soon as reasonably practicable, that a Compromise of an Issuing OCA Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.3.1.2
6.3.1.2	As soon as reasonably practicable, following 6.3.1.1	The DCC shall notify each Subscriber to Organisation Certificates, via secured electronic means, the Compromise of the Issuing OCA Private Key has been notified and shall provide details of the affected SMETS2+ Devices and Organisation Certificates, in one or more Other Compromise Notification files which comply with Appendix D of this document	DCC	6.3.1.3

SEC - Appendix L

6.3.1.3	As soon as reasonably practicable, following 6.3.1.2	The DCC shall take all reasonable steps to provide information to the SMKI PMA to support the SMKI PMA's consideration of what procedural steps (if any) that should be taken in order to recover from the Compromise, where such information may include (but shall not be limited to): a. the number of affected SMETS2+ Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Appendix D of this document; b. the extent to which DCC's monitoring indicates that there has been unauthorised use of the Issuing OCA Private Key; c. the extent to which the vulnerabilities that caused the Compromise have been addressed; d. the steps that DCC reasonably believes should be taken to recover from the Compromise; e. anticipated timescales for recovery; and f. whether or not DCC is proposing to that multiple Compromises should be dealt with on a common basis and if so why the DCC proposes that they should be so treated.	DCC, SMKI PMA	6.3.1.4
6.3.1.4	As soon as reasonably practicable, following 6.3.1.3	Where the DCC believes that use of the Recovery Private Key is likely to be required by the SMKI PMA, it shall identify such preparatory steps that it considers appropriate and to either take such steps or instruct Parties to take steps as required, including (but not limited to): a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; c. notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony or Key Activation Ceremony may be required; and d. activities required to prepare such systems environment required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	6.3.1.5

SEC - Appendix L

6.3.1.5	As soon as reasonably practicable, following 6.3.1.4	The SMKI PMA shall: - determine which of the steps (if any) as set out in section 4.2.2 of this document should be executed, in order to recover from the Compromise; and - confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.3.1.3 for recovery, are approved or whether alternate timescales should apply. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	6.3.1.6
6.3.1.6	As soon as reasonably practicable, following 6.3.1.5	The DCC shall notify all Subscribers to affected Organisation Certificates, via secured electronic means, of the SMKI PMA's decision as to whether or not to execute the recovery procedure (amended as directed) as set out in section 6.3.2.	DCC	If SMKI PMA determines that no action is required, end of Procedure; otherwise 6.3.1.7
6.3.1.7	As soon as reasonably practicable, following 6.3.1.6	<u>The DCC shall consider the Recovery Action Risks before undertaking any of the associated actions. Where the DCC concludes that, at this time, the Recovery Certificates should not be revoked and / or Private Keys not destroyed, the DCC shall inform the SMKI PMA as to the rationale.</u> Otherwise, the DCC shall revoke the Issuing OCA Certificate to which the affected Issuing OCA Private Key relates, and shall update and lodge the relevant Organisation ARL in the SMKI Repository. The DCC shall destroy the Issuing OCA Private Key that is Compromised or suspected to be Compromised.	DCC (as DTSP)	Procedure as set out in Section 6.3.2 of this document

6.3.2 Execution of Recovery Procedure

The procedure as set out immediately below shall be executed in order to recover from the Compromise, or suspected Compromise of an Issuing OCA Private Key, following completion of the procedure as set out in section 6.3.1 of this document.

Step	When	Obligation	Responsibility	Next Step
6.3.2.1	As soon as reasonably practicable, following	A SMKI ARO acting on behalf of each affected Subscribers shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC,	Subscriber	6.3.2.2

SEC - Appendix L

	confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is submitted in accordance with the requirements of TADP.		
6.3.2.2	As soon as reasonably practicable, following 6.3.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds in accordance with the requirements of TADP, for affected Subscribers to allow submission of Service Requests to replace affected Organisation Certificates on SMETS2+ Devices. The DCC shall inform, via secured electronic means, a SMKI SRO acting and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended. The DCC shall amend its Anomaly Detection Thresholds that relate to the issuance of Commands to replace Organisation Certificates on SMETS2+ Devices, to enable replacement of the affected Recovery Certificate on SMETS2+ Devices.	DCC (DSP TAD)	6.3.2.3
6.3.2.3	As soon as reasonably practicable, following 6.3.2.2	The DCC shall generate a new Issuing OCA Key Pair and Issuing OCA Certificate, in accordance with the procedure as set out in the Organisation CPS.	DCC (as TSP)	6.3.2.4
6.3.2.4	As soon as reasonably practicable, following 6.3.2.3	The DCC shall: - determine the number of Key Custodians required to attend a Key Generation Ceremony for the relevant Recovery Private Key; - inform such Key Custodians in respect of the relevant Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Generation Ceremony for the Recovery Private Key; and - participate in the Key Generation Ceremony, as set out in the Organisation CPS, in order to generate a new Recovery Private Key and Recovery Certificate, Digitally Signed using the new Issuing OCA Private Key.	DCC, Key Custodians	6.3.2.5

SEC - Appendix L

6.3.2.5	As soon as reasonably practicable, following 6.3.2.4	The DCC shall: a. determine the number of Key Custodians required to attend a Key Activation Ceremony for the Recovery Private Key (which may be greater than the minimum number required to activate the Recovery Private Key); b. inform such Key Custodians in respect of the Recovery Private Key, via a secured electronic means, of the date, time and location of a Key Activation Ceremony for the Recovery Private Key; and c. participate in the Key Activation Ceremony, in accordance with the Organisation CPS, in order to activate the Recovery Private Key.	DCC, Key Custodians	6.3.2.6
6.3.2.6	As soon as reasonably practicable, following 6.3.2.5	The DCC shall send Commands to all SMETS2+ Devices to replace the Recovery Certificate held on such SMETS2+ Devices with the Recovery Certificate generated in step 6.3.2.4. Such Commands shall include the replacement Recovery Certificate and shall be Digitally Signed using the replaced Recovery Private Key. Once submitted, the DCC shall confirm for each affected SMETS2+ Device that the Command completed successfully and shall generate and maintain records of such confirmations, to support the DCC's confirmation of completion of the recovery procedure. The DCC shall notify each organisation as established in step 6.3.1.3, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, of the list of SMETS2+ Devices where the replacement of the Recovery Certificate has been successfully completed.	DCC (as DSP)	6.3.2.7
6.3.2.7	As soon as reasonably practicable, following 6.3.2.6	Each affected Subscriber shall either: a. identify replacement Organisation Certificates that are not Digitally Signed by the Compromised Issuing OCA Private Key; or b. submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that are Digitally Signed by the new Issuing OCA Private Key.	Subscriber	6.3.2.8
6.3.2.8	As soon as reasonably practicable, following 6.3.2.7	Each affected Subscriber shall submit Service Requests, in accordance with the provisions of the DCC User Interface Specification, in order to replace all Organisation Certificates for which it is the Subscriber that are held on SMETS2+	Subscriber	6.3.2.9

SEC - Appendix L

		Devices and are signed using the Compromised Issuing OCA Private Key, with new Organisation Certificate as identified in accordance with step 6.3.2.7 that are signed by the new Issuing OCA Private Key that is generated in accordance with step 6.3.2.3. Following attempts to replace affected Organisation Certificates on SMETS2+ Devices, each affected Subscriber shall notify the DCC in respect of replacement of affected Organisation Certificates with new Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.		
6.3.2.9	As soon as reasonably practicable, following 6.3.2.8	The DCC shall: a. monitor its records of replacement by affected Subscribers against the list as has been compiled in step 6.3.1.2, to identify successful replacement; b. identify any failures to replace affected Organisation Certificates that have been Digitally Signed using the Issuing OCA Private Key that has been Compromised; and c. monitor revocation of Organisation Certificates that are Digitally Signed using the Compromised Issuing OCA Private Key.	DCC	6.3.2.10
6.3.2.10	As soon as reasonably practicable, following 6.3.2.9	The DCC shall notify each Responsible Supplier for affected SMETS2+ Devices, via secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document, the SMETS2+ Devices for which replacement of the Recovery Certificate or affected Organisation Certificates was not successfully completed.	DCC	Procedure as set out in Section 1.1.1 of this document

6.3.3 Post-Recovery

The procedure as set out immediately below shall be used following recovery from the Compromise of an Issuing OCA Private Key.

Step	When	Obligation	Responsibility	Next Step
------	------	------------	----------------	-----------

SEC - Appendix L

6.3.3.1	As soon as reasonably practicable, following completion of the procedure as set out in Section 6.3.2 of this document	A SMKI ARO acting on behalf of each affected Subscriber shall, as soon as reasonably practicable, submit appropriate enduring Anomaly Detection Thresholds to the DCC in accordance with the requirements of TADP. The DCC shall amend the relevant Anomaly Detection Thresholds in accordance with the requirements of TADP.	DCC (DSP TAD)	6.3.3.2
6.3.3.2	As soon as reasonably practicable, following 6.3.3.1	The DCC shall notify the SMKI PMA, via a secured electronic means of: a. whether the recovery from the Compromise has been successfully completed; and b. the number of SMETS2+ Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Appendix E of this document.	DCC	End of procedure

7. Replacement of a XML Signing Private Key

The procedures for revoking an Organisation Certificate associated with an XML Signing Private Key that is Compromised is laid out in SEC Appendix D - SMKI RAPP section 8.2.

7.1 XML Signing Private Key destruction considerations

XML Signing Private Keys should not be capable of being used to sign any Commands pursuant to GBCS. In accordance with Section 3.3.1 of Appendix AD of the SEC, it is a requirement on Parties that each XML Signing Private Key must be a separate dedicated Key that is not be used for communication with Devices (i.e. different to that used to sign the GBCS Payload within Signed Pre-Commands). However, this separation is not currently a requirement in relation to DCC.

XML Signing Private Keys should also be different to any other Private Keys within the scope of this document. For Parties, such other Private Keys would have a key usage of key agreement only, as per the Organisation Certificate Policy, and so they cannot be used for any Digital Signature purpose.

Thus, recovery in relation to XML Signing Private Keys should be capable of being independent of other recovery methods. However, if the Compromise, or suspected Compromise, extends to Private Keys whose recovery is dealt with by other sections in this document, careful consideration should be given to the timing and sequencing of those other recovery steps, with steps to destroy XML Signing Private Keys and revoke associated Certificates.

To illustrate with the example of an XML Signing Private Key used by a Supplier Party to sign Service Requests:

Should the XML Signing Private Key be destroyed or the associated Organisation Certificate be revoked prior to either Method 1 or Method 2 recovery on a related Private Key being carried out, this would prevent the User from having Service Requests and Signed Pre-Commands successfully processed by the DCC until the XML Signing Private Key has been replaced and the corresponding replacement Organisation Certificate has been created by the DCC. This is the case even if the Private Key used to Digitally Sign the GBCS Payload held within Signed Pre-Commands has not been destroyed and the corresponding Organisation Certificate has not been revoked.

Therefore, it is important for Subscribers to consider the sequence of Private Key destruction and Organisation Certificate revocation when in such a recovery scenario. Specifically the Subscriber shall consider the Recovery Action Risks before undertaking such steps.

8. Periodic testing of the SMKI Recovery Procedure

8.1 Testing Arrangements

This section describes the DCC's obligations in respect of periodic testing of recovery procedures, in accordance with the provisions of Section L10.1(d) of the Code. At least once every year, the DCC shall:

- a) develop a testing plan and a series of testing scenarios which the DCC will conduct in a systems environment which will only be accessible by the DCC, which are representative of the Enrolled Smart Metering Systems and shall take account of any lessons learned from each previous execution of the SMKI Recovery Procedure to recover from a Compromise. The testing plan and testing scenarios will be conducted by the DCC and may include (but shall not be limited to) the following:
 - i. the means by which Key Custodians are notified and participate in Key Generation Ceremonies and/or Key Activation Ceremonies;
 - ii. generation of new DCC Key Material, including the Contingency Key Pair, the Recovery Key Pair and the Contingency Symmetric Key used to encrypt the Contingency Public Key;

SEC - Appendix L

- iii. processes relating to interactions between the DCC and the SMKI PMA in order to determine what steps (if any) should be taken when the use of the Recovery Private Key or Contingency Private Key would be required to recover from a Compromise;
 - iv. preparation of system environments required to support the SMKI Recovery Procedure;
 - v. issuance of Commands that are Digitally Signed using the Recovery Private Key and/or Contingency Private Key, and validation that such Commands are successful;
 - vi. testing of issuance of DCC Alerts following replacement of affected Organisation Certificates in accordance with the SMKI Recovery Procedure; and
 - vii. transfer of files between DCC and Subscribers to support the execution of the SMKI Recovery Procedure.
- b) develop a testing plan and a series of testing scenarios, and conduct such testing scenarios in a systems environment that is available to all Subscribers, which may include (but is not limited to) scenarios a)(vi) and a)(vii) as set out immediately above, along with replacement of Organisation Certificates on SMETS2+ Devices or S1SP Held Device Security Credentials and that are initiated via Service Requests issued by Subscribers.
- c) seek input from Subscribers to Organisation Certificates in relation to those testing scenarios that require participation by Subscribers, and take such input into account when proposing and agreeing the testing scenarios with the SMKI PMA;
- d) agree such testing scenarios with the SMKI PMA;
- e) create test data based upon data collected by the DCC and, where necessary, acquired from Parties;
- f) maintain a test environment in order to carry out such periodic testing of the SMKI Recovery Procedure;
- g) carry out testing of the SMKI Recovery Procedure for agreed scenarios; and
- h) provide a report to the SMKI PMA and Subscribers to Organisation Certificates following periodic testing, which shall detail the success or otherwise of such testing, proposed amendments to the SMKI Recovery Procedure, and any issues arising that require PMA consideration.

In respect of periodic testing of the SMKI Recovery Procedure:

- i) SMKI Users shall provide such reasonable assistance to the DCC as is required to support testing; and
- j) The SMKI PMA shall review reports from periodic testing and shall direct the DCC, as necessary, to update the SMKI Recovery Procedure.

Appendix A: Communication Formats

In Appendices B to E of this document, each of the CSV files specified shall be encoded using the ASCII character set and:

- must have a comma “,” as the field separator;
- must have a line feed character 0x0A as the record separator, which in this section is indicated by the “▲” character; and

SEC - Appendix L

- may include consecutive comma separators to the left of a record separator to specify that a field has a null value. Where this is the case, DCC shall interpret consecutive commas within a record to indicate a null value.

Some spreadsheets output a carriage return line feed 0x0D0A as the record separator for CSV files and/or do not terminate CSV files with a record separator. Each User submitting a CSV file that is to be Digitally Signed using the Private Key associated with a File Signing Certificate shall, prior to Digitally Signing that file, ensure that:

- the CSV file is formatted to ensure that each record has a separator which is a 0x0A character and that any 0x0D character is removed from the file; and
- the CSV file is terminated with a 0x0A character.

Details of the function of the software utility and the method of Digital Signing of files to support the recovery procedures are contained within section 6 of the TADP.

Appendix B: Organisation Compromise Notification File

Due to the differences in the validation mechanisms in the SMETS1 and SMETS2+ system, the terminology used for Organisation Certificates is different. For the purposes of this Appendix, a SMETS1 Notified Critical Supplier/Network Operator Certificate is considered equivalent to a SMETS2+ Supplier/Network Operator Digital Signature Certificate. A Notified Non-Critical Supplier/Network Operator Certificate is equivalent to a Supplier/Network Operator Key Agreement Certificate. On compromise, these Organisation Certificates shall be included in the corresponding parameters in the Notification File. Pre-payment Key Agreement Certificates have no corresponding SMETS1 equivalent. A SMETS1 Supplier does not need to populate this field.

Each Organisation Compromise Notification File shall be in the format set out in this Appendix and shall have a filename of the form:

a) *OC_Priority_UserID_IncidentID_N_FileNum.csv*

Where:

- a) *OC* denotes that the file relates an Organisation Compromise.
- b) *Priority* contains an integer value which shall be set to a value of 1 or 2, where a lesser value denotes that the file has a higher priority than a file submitted in respect of the same Incident with a Priority field containing a higher value. Where the Subscriber submitting the Organisation Compromise Notification File wishes to apply a priority to Organisation Certificate replacement recovery activities, it shall determine such priority values and include the integer priority value within the filename for each Organisation Compromise Notification File submitted.
- c) *UserID* contains the EUI-64 Compliant identifier for:
 - the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
 - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
 - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
- d) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
- e) *N* denotes that the file is a notification of affected Organisation Certificates and Devices.

SEC - Appendix L

- f) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Organisation Compromise Notification File shall be generated in accordance with the procedure set out immediately below:

- a) an “initial” CSV file shall be created, which shall contain the following records:
- UserID ▲
 - Device_ID, Affected_Certificate_Serial_Number_DS,
Affected_Certificate_Serial_Number_KAK,
Affected_Certificate_Serial_Number_KAKPP,
Replacement_Certificate_Serial_Number_DS,
Replacement_Certificate_Serial_Number_KAK,
Replacement_Certificate_Serial_Number_KAKPP (*repeated for each affected Device, with no more than 1 million 100,000 such records permitted within any file or any larger number of records as directed by the SMKI PMA*) ▲
- b) a File Signing Certificate_ID shall be appended to the end of the “initial” file, comprising:
- all of the attributes contained within the ‘Issuer’ field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
 - the Certificate serial number obtained from the ‘serialNumber’ field in the File Signing Certificate, followed by a 0x0A character; and
- c) a Digital_Signature shall be generated from the concatenation of the “initial” CSV file and the File Signing Certificate_ID and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the TADP.

Where:

- a) The *UserID* field contains the EUI-64 Compliant identifier for:
- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
 - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
 - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
- b) The *Device_ID* field contains the Device ID.
- c) The *Affected_Certificate_Serial_Number_DS* field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Digital Signing Trust Anchor Cell on affected Devices.

SEC - Appendix L

- d) The `Affected_Certificate_Serial_Number_KAK` field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Key Agreement Key Trust Anchor Cell on affected Devices.
- e) The `Affected_Certificate_Serial_Number_KAKPP` field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the pre- payment Key Agreement Key Trust Anchor Cell on affected Devices. Where the Subscriber that is submitting the file is a Network Party, the `Affected_Certificate_Serial_Number_KAKPP` field shall not be populated.
- f) The `Replacement_Certificate_Serial_Number_DS` field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Digital Signing Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.
- g) The `Replacement_Certificate_Serial_Number_KAK` field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.
- h) The `Replacement_Certificate_Serial_Number_KAKPP` field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the prepayment Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.
- i) The `File_Signing_Certificate_ID` field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.
- j) The `Digital_Signature` field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Where multiple Organisation Compromise Notification Files are submitted by an affected Subscriber to the DCC in respect of single IncidentID, the DCC shall process the files in order of Priority value, where files with a lower Priority value shall be processed first.

Appendix C: Organisation Compromise Recovery Progress File

Each Organisation Compromise Recovery Progress File shall be in the format set out in this Appendix and shall have a filename of the form:

- k) `OC_Priority_UserID_IncidentID_P_FileNum.csv`

Where:

- a) `OC` denotes that the file relates an Organisation Compromise.
- b) `Priority` contains an integer value which shall be set to 1 or 2, where a lesser value denoting that the file has a higher priority than a file submitted in respect of the same Incident with a `Priority` field containing a higher value. Such priority values shall have the same value as the corresponding Organisation Compromise Notification File.
- c) `UserID` contains the EUI-64 Compliant identifier for:

SEC - Appendix L

- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
 - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
 - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
- d) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
- e) *P* denotes that the file is a notification of progress in respect of replacement of affected Certificates and Devices.
- f) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Organisation Compromise Recovery Progress File shall be generated in accordance with the procedure set out immediately below:

- a) an "initial" CSV file shall be created, which shall contain the following records:
- UserID ▲
 - Device_ID, Overall_status, Overall_status_description,
Affected_Certificate_Serial_Number_DS,
Affected_Certificate_Serial_Number_KAK,
Affected_Certificate_Serial_Number_KAKPP,
Replacement_Certificate_Serial_Number_DS,
Replacement_Certificate_Serial_Number_KAK,
Replacement_Certificate_Serial_Number_KAKPP,
Replacement_Status_DS, Replacement_Status_KAK, Replacement_Status_KAKPP (*repeated for each affected Device, with no more than ~~1 million-100,000~~ such records permitted within any file or any larger number of records as directed by the SMKI PMA*) ▲
- b) a File Signing Certificate_ID shall be appended to the end of the "initial" CSV file, comprising:
- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
 - the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and
- c) a Digital_Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the TADP.

Where:

- a) The UserID field contains the EUI-64 Compliant identifier for:

SEC - Appendix L

- the affected Subscriber submitting the file, where an affected Subscriber is submitting the file to the DCC; or
 - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to a Subscriber by the DCC; or
 - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
- b) The Device_ID field contains the Device ID.
- c) The Overall_status field indicates acceptance or rejection by the DCC of each device identified in the Compromise Notification form
- d) The Overall_status_description field indicates the reason for any rejection
- e) The Affected_Certificate_Serial_Number_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Digital Signing Trust Anchor Cell on affected Devices, where applicable.
- f) The Affected_Certificate_Serial_Number_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.
- g) The Affected_Certificate_Serial_Number_KAKPP field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the pre- payment Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.
- h) The Replacement_Certificate_Serial_Number_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Digital Signing Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.
- i) The Replacement_Certificate_Serial_Number_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.
- j) The Replacement_Certificate_Serial_Number_KAKPP field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the prepayment Key Agreement Key Device Trust Anchor Cell. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Organisation Certificates that the DCC will use to populate Devices' Trust Anchor Cells using the Recovery Private Key or Contingency Private Key.
- k) The Replacement_Status_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement information from the affected Organisation Certificate in the Digital Signing Trust Anchor Cell on a Device.
- l) The Replacement_Status_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Organisation Certificate in the Key Agreement Key Trust Anchor Cell on a Device.

SEC - Appendix L

- m) The Replacement_Status_KAKPP field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Organisation Certificate in the prepayment Key Agreement Key Trust Anchor Cell on a Device.
- n) The File_Signing Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.
- o) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Appendix D: Other Compromise Notification File

Each Other Compromise Notification File shall be in the format set out in this Appendix and shall have a filename of the form:

- p) *OTH_UserID_IncidentID_N_FileNum.csv*

Where:

- a) *OTH* denotes that the file relates to notification of affected Devices for a Compromise not applicable to Appendices B or C of this document.
- b) *UserID* contains the EUI-64 Compliant identifier for:
 - the Subscriber to which the file is being provided unless the file is being submitted to the SMKI PMA; or
 - the EUI-64 Compliant identifier for the DCC where the file is being submitted to the SMKI PMA.
- c) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
- d) *N* denotes that the file is a notification of affected Organisation Certificates and Devices.
- e) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Other Compromise File shall contain the following records:

- a) UserID ▲
- b) Device_ID, Affected_Certificate_Serial_Number_Root,
Affected_Certificate_Serial_Number_Recovery,
Affected_Certificate_Serial_Number_Supplier_DS,
Affected_Certificate_Serial_Number_Supplier_KAK,
Affected_Certificate_Serial_Number_Supplier_KAKPP,
Affected_Certificate_Serial_Number_NetworkOperator_DS,
Affected_Certificate_Serial_Number_NetworkOperator_KAK,
Affected_Certificate_Serial_Number_COS_DS,

Affected_Certificate_Serial_Number_WAN_DS,
 Replacement_Certificate_Serial_Number_Root,
 Replacement_Certificate_Serial_Number_Recovery,
 Replacement_Certificate_Serial_Number_Supplier_DS,
 Replacement_Certificate_Serial_Number_Supplier_KAK,
 Replacement_Certificate_Serial_Number_Supplier_KAKPP,
 Replacement_Certificate_Serial_Number_NetworkOperator_DS,
 Replacement_Certificate_Serial_Number_NetworkOperator_KAK,
 Replacement_Certificate_Serial_Number_COS_DS,

Replacement_Certificate_Serial_Number_WAN_DS (*repeated for each affected Device, with no more than 1 million such records permitted within any file or any larger number of records as directed by the SMKI PMA*) ▲

Where:

- a) The UserID field contains the EUI-64 Compliant identifier for:
 - the Subscriber to which the file is being provided unless the file is being submitted to the SMKI PMA; or
 - the EUI-64 Compliant identifier for the DCC where the file is being submitted to the SMKI PMA.
- b) The Device_ID field contains the Device ID.
- c) The Affected_Certificate_Serial_Number_Root field contains the Root OCA Certificate serial number of the Root OCA Certificate affected by the Compromise that is used to populate the Root Trust Anchor Cell on affected Devices, where applicable.
- d) The Affected_Certificate_Serial_Number_Recovery field contains the Recovery Certificate serial number of the Recovery Certificate affected by the Compromise that is used to populate the Recovery Trust Anchor Cell on affected Devices, where applicable.
- e) The Affected_Certificate_Serial_Number_Supplier_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Supplier Digital Signing Trust Anchor Cell on affected Devices, where applicable.
- f) The Affected_Certificate_Serial_Number_Supplier_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Supplier Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.
- g) The Affected_Certificate_Serial_Number_Supplier_KAKPP field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Supplier pre-payment Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.
- h) The Affected_Certificate_Serial_Number_NetworkOperator_DS field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Network Operator Digital Signing Trust Anchor Cell on affected Devices, where applicable.

SEC - Appendix L

- i) The Affected_Certificate_Serial_Number_NetworkOperator_KAK field contains the Organisation Certificate serial number of the Organisation Certificate affected by the Compromise that is used to populate the Network Operator Key Agreement Key Trust Anchor Cell on affected Devices, where applicable.
- j) The Affected_Certificate_Serial_Number_COS_DS field contains the TCoS Certificate serial number of the TCoS Certificate affected by the Compromise that is used to populate the TCoS Trust Anchor Cell on affected Devices, where applicable.
- k) The Affected_Certificate_Serial_Number_WAN_DS field contains the WAN Provider Certificate serial number of the WAN Provider Certificate affected by the Compromise that is used to populate the WAN Provider Trust Anchor Cell on affected Devices, where applicable.
- l) The Replacement_Certificate_Serial_Number_Root field contains the Root OCA Certificate serial number for the Root OCA Certificate to be used to populate the Device Root Trust Anchor Cell, where applicable.
- m) The Replacement_Certificate_Serial_Number_Recovery field contains the Recovery Certificate serial number for the Recovery Certificate to be used to populate the Device Recovery Trust Anchor Cell, where applicable.
- n) The Replacement_Certificate_Serial_Number_Supplier_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Supplier Digital Signing Device Trust Anchor Cell, where applicable.
- o) The Replacement_Certificate_Serial_Number_Supplier_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Supplier Key Agreement Key Device Trust Anchor Cell, where applicable.
- p) The Replacement_Certificate_Serial_Number_Supplier_KAKPP field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Supplier prepayment Key Agreement Key Device Trust Anchor Cell, where applicable.
- q) The Replacement_Certificate_Serial_Number_NetworkOperator_DS field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Network Operator Digital Signing Device Trust Anchor Cell, where applicable.
- r) The Replacement_Certificate_Serial_Number_NetworkOperator_KAK field contains the Organisation Certificate serial number for the Organisation Certificate to be used to populate the Network Operator Key Agreement Key Device Trust Anchor Cell, where applicable.
- s) The Replacement_Certificate_Serial_Number_COS_DS field contains the TCoS Certificate serial number for the TCoS Certificate to be used to populate the Device TCoS Trust Anchor Cell, where applicable.
- t) The Replacement_Certificate_Serial_Number_WAN_DS field contains the WAN Provider Certificate serial number for the WAN Provider Certificate to be used to populate the Device WAN Provider Trust Anchor Cell, where applicable.

Appendix E: Other Compromise Recovery Progress File

Each Other Compromise Recovery Progress File shall be in the format set out in this Appendix and shall have a filename of the form:

- u) *OTH_UserID_IncidentID_P_FileNum.csv*

Where:

- a) *OTH* denotes that the file relates to notification of affected Devices for a Compromise not applicable to Appendices B or C of this document.

SEC - Appendix L

- b) *UserID* contains the EUI-64 Compliant identifier for:
 - the Subscriber submitting the file, where a Subscriber is submitting the file to the DCC;
 - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to the Subscriber by the DCC; or
 - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
- c) *IncidentID* contains the Incident reference number provided as set out in section 3.2 of this document.
- d) *P* denotes that the file is a notification of progress in respect of replacement of affected Certificates and Devices.
- e) *FileNum* is an integer value, used to distinguish between data that is split across multiple files due to exceeding the maximum permitted number records per file, which is set out immediately below.

Each Other Compromise File shall be generated in accordance with the procedure set out immediately below:

- a) an "initial" CSV file shall be created, which shall contain the following records:
 - UserID ▲
 Device_ID, Overall_status, Overall_status_description,
 Replacement_Certificate_Serial_Number_Root,
 Replacement_Certificate_Serial_Number_Recovery,
 Replacement_Certificate_Serial_Number_Supplier_DS,
 Replacement_Certificate_Serial_Number_Supplier_KAK,
 Replacement_Certificate_Serial_Number_Supplier_KAKPP,
 Replacement_Certificate_Serial_Number_NetworkOperator_DS,
 Replacement_Certificate_Serial_Number_NetworkOperator_KAK,
 Replacement_Certificate_Serial_Number_COS_DS,
 Replacement_Certificate_Serial_Number_WAN_DS, Replacement_Status_Root,
 Replacement_Status_Recovery, Replacement_Status_Supplier_DS,
 Replacement_Status_Supplier_KAK, Replacement_Status_Supplier_KAKPP,
 Replacement_Status_NetworkOperator_DS,
 Replacement_Status_NetworkOperator_KAK, Replacement_Status_COS_DS,
 Replacement_Status_WAN_DS (*repeated for each affected Device, with no more than 1 million ~~100,000~~ such records permitted within any file or any larger number of records as directed by the SMKI PMA*) ▲
- b) a File Signing Certificate_ID shall be appended to the end of the "initial" CSV file, comprising:

SEC - Appendix L

- all of the attributes contained within the 'Issuer' field in the File Signing Certificate, including attribute names, equals signs and values, which shall be encoded in URL format such that it does not contain any special characters, followed by a comma; and
 - the Certificate serial number obtained from the 'serialNumber' field in the File Signing Certificate, followed by a 0x0A character; and
- c) a Digital_Signature shall be generated from the "initial" CSV file and appended as a record to the end of the CSV file, in accordance with the procedure set out in Section 6 of the TADP.

Where:

- a) The UserID field contains the EUI-64 Compliant identifier for:
- the Subscriber submitting the file, where a Subscriber is submitting the file to the DCC;
 - the Subscriber to which the file is being provided, unless the file is being submitted to the SMKI PMA, where the file is being submitted to the Subscriber by the DCC; or
 - the DCC, where the file is being submitted to the SMKI PMA by the DCC.
- b) The Device_ID field contains the Device ID.
- c) The Overall_status field indicates acceptance or rejection by the DCC of each device identified in the Compromise Notification File
- d) The Overall_status_description field indicates the reason for any rejection
- e) The Replacement_Certificate_Serial_Number_Root field contains the Root OCA Certificate serial number for the Root OCA Certificate to be used to populate the Device Root Trust Anchor Cell.
- f) The Replacement_Certificate_Serial_Number_Recovery field contains the Certificate serial number for the Certificate to be used to populate the Device Recovery Trust Anchor Cell.
- g) The Replacement_Certificate_Serial_Number_Supplier_DS field contains the Certificate serial number for the Certificate to be used to populate the Supplier Digital Signing Device Trust Anchor Cell.
- h) The Replacement_Certificate_Serial_Number_Supplier_KAK field contains the Certificate serial number for the Certificate to be used to populate the Supplier Key Agreement Key Device Trust Anchor Cell.
- i) The Replacement_Certificate_Serial_Number_Supplier_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the Supplier prepayment Key Agreement Key Device Trust Anchor Cell.
- j) The Replacement_Certificate_Serial_Number_NetworkOperator_DS field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Digital Signing Device Trust Anchor Cell.
- k) The Replacement_Certificate_Serial_Number_NetworkOperator_KAK field contains the Certificate serial number for the Certificate to be used to populate the Network Operator Key Agreement Key Device Trust Anchor Cell.
- l) The Replacement_Certificate_Serial_Number_COS_DS field contains the Certificate serial number for the Certificate to be used to populate the Device TCoS Trust Anchor Cell.
- m) The Replacement_Certificate_Serial_Number_WAN_DS field contains the Certificate serial number for the Certificate to be used to populate the Device WAN Provider Trust Anchor Cell.

SEC - Appendix L

- n) The Replacement_Status_Root field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Root Trust Anchor Cell on a Device.
- o) The Replacement_Status_Recovery field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Recovery Trust Anchor Cell on a Device.
- p) The Replacement_Status_Supplier_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Digital Signing Trust Anchor Cell on a Device.
- q) The Replacement_Status_Supplier_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Key Agreement Key Trust Anchor Cell on a Device.
- r) The Replacement_Status_Supplier_KAKPP field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier prepayment Key Agreement Key Trust Anchor Cell on a Device.
- s) The Replacement_Status_NetworkOperator_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Digital Signing Trust Anchor Cell on a Device.
- t) The Replacement_Status_NetworkOperator_KAK field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Key Agreement Key Trust Anchor Cell on a Device.
- u) The Replacement_Status_COS_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the TCoS Trust Anchor Cell on a Device.
- v) The Replacement_Status_WAN_DS field contains a value which is one of the permitted response code values for Service Request 6.15.1, as set out in the first column of Table 7 in section 4.1A.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the WAN Provider Trust Anchor Cell on a Device.
- w) The File_Signing_Certificate_ID field contains the File Signing Certificate ID, which shall not contain a value when the file is issued by the DCC.
- x) The Digital_Signature field contains the Digital Signature, which shall not contain a value when the file is issued by the DCC.

Appendix F: Definitions

Term	Definition
Chief Information Security Officer	Means a senior security officer within a Party who is responsible for activities including (but not limited to) establishing and maintaining the security vision, strategy, information security governance framework, secure asset and infrastructure control framework, and security risk management program
Data Services Provider, or DSP	Means the DCC acting from those systems identified in part a) of the definition of DCC Live Systems
DSP Threshold Anomaly Detection, or DSP TAD	Means the DCC acting using those systems identified in Part (b) of the definition of DCC Live Systems
<u>Global ADT</u>	<u>Means an Anomaly Detection Threshold set by the DCC.</u>
Key Activation Ceremony	Means a meeting at which a Private Key or Symmetric Key is activated by the DCC and/or Key Custodians, such that the Private Key or Symmetric Key may be used
Key Generation Ceremony	Means a meeting at which a Private Key or Contingency Symmetric Key is generated by the DCC and Key Custodians
Key Component	Means part of a Key or part of Activation Data used to protect a Key.
Key Custodian	Means an individual, appointed in accordance with section 3.4 of the SMKI Recovery Procedure, to hold a key which may be used as part of the process to access a Key Component.
Organisation Compromise Notification File	A CSV file used to support recovery from a Compromise that is specified in Appendix B of the SMKI Recovery Procedure
Organisation Compromise Recovery Progress File	A CSV file used to support recovery from a Compromise that is specified in Appendix C of the SMKI Recovery Procedure
Other Compromise Notification File	Means a CSV file used to support recovery from a Compromise that is specified in Appendix D of the SMKI Recovery Procedure
Other Compromise Recovery Progress File	Means a CSV file used to support recovery from a Compromise that is specified in Appendix E of the SMKI Recovery Procedure
S1SP Held Device Security Credentials	Means, in relation to a SMETS1 Device and as the context requires, any or all of the Notified Critical Supplier Certificate, the Notified Non-Critical Supplier Certificate, the Notified Critical Network Operator Certificate and the Notified Non-Critical Network Operator Certificate, in each case as defined in Appendix AM of the SEC (SMETS1 Supporting Requirements).
Trust Anchor Cell	Shall have its GBCS meaning.

SEC - Appendix L

Trusted Service Provider, or TSP	Means the DCC acting using systems identified in part (d) of the definition of DCC Live Systems
wrappedApexContingencyKey	Means the value used in the <code>WrappedApexContingencyKey</code> extension (with the meaning of IETF RFC 5934 section 9) in a Root OCA Certificate

Appendix G: SMKI Recovery Procedure Test Scenarios

Each scenario set out in this Appendix G can be tested in isolation, or combined as part of a more extensive test.

9.1 DCC and SMKI PMA Interactions

These scenarios cover the testing of interactions between the DCC Service Desk and the SMKI PMA in the event of a (suspected) Compromise.

ID	SMKI 200
Title:	Notification of (suspected) Compromise and SMKI PMA Response
Description	DCC service Desk completes Compromise Notification Report DCC service Desk communicates Compromise Notification Report DCC Service Desk requests SMKI PMA Decision (not applicable to the Method 1 of the Organisation Recovery process) SMKI PMA acknowledge receipt of Compromise Notification Report SMKI PMA provides instruction / guidance to the DCC through the DCC Service Desk in response to the Compromise Notification Report as to whether Recovery should be carried out and if so, which steps of the chosen approach
Objective	- To prove DCC processes in regard to the Compromise Notification Report preparation - To prove communication of (suspected) Compromise process to the SMKI PMA by the DCC Service Desk - To prove SMKI PMA instruction / guidance to the DCC Service Desk processes - To prove SMKI PMA decision making processes in response to the Compromise Notification Report and request for guidance / instruction
ID	SMKI 201
Title:	Notification of outcome of Recovery processes
Description	DCC Service Desk prepares Organisation Compromise Recovery Report for the SMKI PMA DCC Service Desk communicates Recovery Report to the SMKI PMA SMKI PMA acknowledges receipt of Organisation Compromise Recovery Report
Objective	- To prove DCC processes for the preparation of the Organisation Compromise Recovery Report - To prove communication of the Organisation Compromise Recovery Report to the SMKI PMA by the DCC Service Desk - To prove SMKI PMA processes in respect of receipt of the Organisation Compromise Recovery Report

9.2 DCC / Subscriber and DCC / Party Interactions and Processes

9.2.1 Organisation Certificate Revocation and Replacement

ID	SMKI 214
-----------	----------

Title:	Organisation Certificate Revocation
Description	Subscriber submits Certificate Revocation Request(s) (CRR) through the DCC Service Desk DCC revokes Organisation Certificates identified in the CRR(s) DCC Service Desk communicates outcome of Revocation request to Subscriber
Objective	- To prove Subscriber processes in response to a (suspected) Compromise of one its Organisation Private Keys - To prove DCC and Subscriber interactions to revoke an Organisation Certificate
ID	SMKI 202
Title:	Replacement Organisation Certificates
Description	Subscriber obtains new or identifies existing Organisation Certificates to replace on affected Devices or those that form a part of any S1SP Held Device Security Credentials Subscriber communicates decision in the form of a Certificate ID to the DCC through the DCC Service Desk
Objective	- To prove, during the Recovery process, that the Subscriber can request new Organisation Certificates or identify and obtain existing Organisation Certificates to be placed on affected Devices, or the notification of the Certificate ID to the DCC where they form a part of any S1SP Held Device Security Credentials. - To prove Subscriber communications with the DCC Service Desk in respect of the replacement Organisation Certificates

9.2.2 Communication of SMKI PMA Decision to Subscriber

ID	SMKI 203
Title:	DCC Communicates SMKI PMA Recovery Decision to Subscriber
Description	DCC Service Desk communicates the decision of the SMKI PMA in respect of whether Recovery will be used and if so, which methods and steps are to be carried out
Objective	To prove DCC Service Desk and Subscriber interactions in respect of SMKI PMA decisions

9.2.3 Subscriber notification of Compromise

ID	SMKI 215
Title:	Send DCC Organisation Notification and Anomaly Detection Threshold changes

Description	Subscriber / Supplier submits through the DCC Service Desk Organisation Compromise Notification Files or Other Compromise Notification Files and Anomaly Detection Thresholds amendments for the purposes of Recovery, in accordance with the TADP
--------------------	--

Objective	- To prove Subscriber / Supplier processes and interactions with the DCC Service Desk in regard to the submission of information relating to impacted devices, incident - To prove Subscriber / Supplier processes and interactions with the DCC Service Desk in regard to the temporary amendment of Anomaly Detection Thresholds to support Recovery
------------------	---

ID	SMKI 216
-----------	----------

Title:	Threshold Anomaly Detection – Post-recovery – applies to Method 1 of Organisation Certificate Recovery from Compromise only
---------------	---

Description	Subscriber / Supplier submits through the DCC Service Desk Anomaly Detection Thresholds for re-instatement following recovery
--------------------	---

Objective	To prove Subscriber / Supplier processes and interactions with the DCC Service Desk in regard to the re-instigation of Anomaly Detection Thresholds following Recovery
------------------	--

ID	SMKI 217
-----------	----------

Title:	DCC amends Anomaly Detection Thresholds
---------------	---

Description	DCC amends Anomaly Detection Thresholds in response to Recovery process to enable communications to Devices to be processed by the DSP DCC informs Subscriber of Threshold Anomaly Detection value change
--------------------	--

Objective	- To prove DCC processes in respect of Threshold Anomaly Detection value change during Recovery - To prove DCC and Subscriber interactions in respect of Threshold Anomaly Detection value change during Recovery
------------------	--

ID	SMKI 218
-----------	----------

Title:	DCC re-instates Anomaly Detection Thresholds
---------------	--

Description	DCC Service Desk amends Anomaly Detection Thresholds to those set before the Recovery process commenced DCC Service Desk informs Anomaly Detection Thresholds change
--------------------	---

Objective	- To prove DCC processes in respect of Anomaly Detection Thresholds reinstatement following Recovery - To prove DCC and Subscriber interactions in respect of Anomaly Detection Thresholds reinstatement during Recovery
------------------	---

9.2.4 DCC Notification to Parties other than the (suspected) Compromised Subscriber

ID	SMKI 204
Title:	Method 1, Method 1A and Method 3 – Responsible Supplier Notification of (suspected) Compromise
Description	DCC Service Desk identifies affected Devices for which the Subscriber is not the Responsible Supplier DCC Service Desk notifies Responsible Supplier(s) for those Devices using Organisation Compromise Notification file
Objective	To prove DCC Service Desk and Responsible Supplier processes with regard to notification of (suspected) Compromise to Responsible Suppliers for Devices which are affected by the (suspected) Compromise
ID	SMKI 205
Title:	Method 1, Method 1A and Method 3 - Responsible Supplier Notification of Progress / Outcome of Recovery
Description	DCC Service Desk identifies affected Devices for which the Subscriber is not the Responsible Supplier DCC Service Desk notifies Responsible Supplier(s) for those Devices using Organisation Compromise Progress file and therefore the cessation of communications with affected Devices during Recovery
Objective	To prove DCC Service Desk and Party processes with regard to notification of progress of Recovery to Responsible Suppliers for Devices which are affected by the (suspected) Compromise
ID	SMKI 206
Title:	Method 2 – Network Operator Notification of (suspected) Compromise
Description	DCC Service Desk identifies Network Operators for affected Devices reported by the Subscriber DCC Service Desk notifies using the Organisation Notification file Network Operators for those Devices of the Subscriber's intent to Recover using Method 2 and cessation of communications during Recovery
Objective	To prove DCC Service Desk and Network Operator Party processes with regard to notification of (suspected) Compromise to Network Operators for Devices which are affected by the (suspected) Compromise
ID	SMKI 207
Title:	Method 2 – Network Operator Notification of Progress / Outcome of Recovery

Description	DCC Service Desk identifies Network Operators for affected Devices reported by the Subscriber DCC Service Desk notifies Network Operator(s) for those Devices of Recovery progress / outcome of Recovery using the Organisation Compromise Progress file
Objective	To prove DCC Service Desk and Network Operator Party processes with regard to notification of progress of Recovery to Network Operators for Devices which are affected by the (suspected) Compromise

9.3 Method 1 - Subscriber Service Requests and Alert Responses

This scenario is applicable only to Method 1 of the Recovery of Organisation Certificate held on a Device (section 4.1 of the SMKI Recovery Procedures). Its execution will be through the combination of individual test scenarios as set out above in section 8.2 of this Appendix G.

ID	SMKI 208
Title:	Method 1 - Subscriber Recovers using own Private Key
Description	Subscriber sends Service Requests to replace Organisation Certificates on affected Devices, signed using its own private key which is the subject of the (suspected) Compromise Subscriber monitors progress of Recovery through Alerts received from affected Devices in response to the instruction to replace Organisation Certificates Subscriber informs DCC through DCC Service Desk of the progress of Recovery through an Organisation Compromise Progress Report File
Objective	To prove Subscriber processes in response to a (suspected) Compromise of one its Organisation Private Keys

9.4 Method 1A Compromise of any S1SP Held Device Security Credentials

This scenario is applicable only to Method 1A to recover from a Compromise of the Private Key associated with the Public Key contained within an Organisation Certificate that forms part of any S1SP Held Device Security Credentials, in accordance with section 3.2 and 4.1A of this document.

ID	SMKI 208A
Title:	Method 1A -Subscriber Recovers using own Private Key
Description	Subscriber sends Service Requests to replace Organisation Certificates that form a part of any S1SP Held Device Security Credentials , signed using its own private key which is the subject of the Compromise Subscriber monitors progress of Recovery through Alerts received from the SMETS1 Service Provider in response to the instruction to replace Organisation Certificates Subscriber informs DCC through DCC Service Desk of the progress of Recovery through an Organisation Compromise Progress Report File

Objective	To prove Subscriber processes in response to a Compromise of one its Organisation Private Keys related to an Organisation Certificate that forms a part of any S1SP Held Device Security Credentials
------------------	--

9.5 Methods 2 & 3 – Communications with affected Devices in Response to the Supplier / Subscribers Service Requests

These scenarios are applicable to Methods 2 and / or 3 of the Recovery of Organisation Certificate held on a Device (section 4.1A of the SMKI Recovery Procedures). Their execution will be through the combination of individual test scenarios as set out above in section 8.2 of this Appendix G.

ID	SMKI 209
-----------	----------

Title:	Suspension of Communications with Devices
---------------	---

Description	DCC suspends communications to Devices where the Compromise impacts Supplier and / or Communication Service Provider Certificates on those Devices DCC confirms decision of the SMKI PMA with regard to the suspension or if reinstates communication according to the decision of the SMKI PMA
--------------------	---

Objective	To prove DCC Service Desk and DCC processes with regard to the suspension of communications with affected Devices
------------------	---

ID	SMKI 210
-----------	----------

Title:	Set status of affected Devices to Recovery
---------------	--

Description	Where the affected Subscriber is not a Network Provider, DCC sets status in the Smart Metering Inventory of affected Devices to 'Recovery'
--------------------	--

Objective	To prove DCC Service Desk and DCC processes with regard to the SMI status change during Recovery processes
------------------	--

ID	SMKI 211
-----------	----------

Title:	Commands sent to affected Devices to effect Recovery – Method 2 only
---------------	--

Description	DCC issues Commands as set out in the GBCS signed with the Recovery Private Key and containing ACB Certificates as the replacement Supplier Certificate DCC monitor for Alerts received from Devices and forwards the Alert to the affected Supplier DCC sets SMI status of affected Devices that have reported successful Recovery to 'Recovered' DCC notifies affected Subscriber of progress of the Recovery Processes using the DCC Alert and Organisation Recovery Progress file Supplier Issues Service Requests to replace the ACB Certificate in the Supplier slot with a new Supplier Certificate DCC processes these Service Requests Supplier notifies the outcome of Supplier Certificate Replacement using the Organisation Recovery Progress file
--------------------	---

	DCC sets SMI status of the Device to the pre-Recovery State on receipt of the Response from the Device indicating successful Certificate Update
Objective	- To prove DCC and DCC Service Desk processes during Method 2 of Organisation Certificate Recovery - To prove Suppliers processes during Method 2 of Organisation Certificate Recovery - To prove interactions between Supplier and DCC Service Desk during Method 2 of Organisation Certificate Recovery
ID	SMKI 213
Title:	Commands sent to affected Devices to effect Recovery – Method 3 only
Description	DCC issues Commands as set out in the GBCS signed with the Recovery Private Key and containing the Certificate identified by the Subscriber as the replacement Certificate DCC monitor for Alerts received from Devices and forwards the Alert to the affected Subscriber DCC sets SMI status of affected Devices that have reported successful certificate replacement to the pre-recovery status DCC notifies affected Subscriber of progress of the Recovery Processes using the Organisation Recovery Progress file DCC notifies the Device's Responsible Supplier (if not the Subscriber) of failed certificate replacement events using the Organisation Recovery Progress file
Objective	- To prove DCC and DCC Service Desk processes during Method 3 of Organisation Certificate Recovery - To prove Subscribers processes during Method 3 of Organisation Certificate Recovery - To prove interactions between Subscribers and DCC Service Desk during Method 3 of Organisation Certificate Recovery - To prove interactions between Responsible Suppliers and DCC Service Desk during Method 3 of Organisation Certificate Recovery

9.6 End to End Tests

These Test Scenarios constitute full Tests of each Recovery Process set out in the sections 4 and 6 of the SMKI Recovery Procedures. It is intended that these tests are carried out periodically as set out in section 7.1 of this SMKI Recovery Procedures.

ID	SMKI 101
Title:	Recovery from Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 1 and Method 1A
Description	As set out in section 4.1 and 4.1A of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)
Objective	To prove in an end to end test the processes to Recover from the Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 1 and Method 1A

ID	SMKI 102
Title:	Recovery from Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 2
Description	As set out in section 4.2 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)
Objective	To prove in an end to end test the processes to recover from the Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 2
ID	SMKI 103
Title:	Recovery from Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 3
Description	As set out in section 4.3 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)
Objective	To prove in an end to end test the processes to recover from the Compromise of an Organisation Private Key (other than the Recovery Private Key) – Method 3
ID	SMKI 104
Title:	Recovery from Compromise of a Recovery Private Key
Description	As set out in section 6.2 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)
Objective	To prove in an end to end test the processes to recover from the Compromise of the Recovery Private Key
ID	SMKI 105
Title:	Recovery from Compromise of an Issuing OCA Private Key
Description	As set out in section 6.3 of the SMKI Recovery Procedures (except for the standing-up of the Recovery Environment)
Objective	To prove in an end to end test the processes to recover from the Compromise of an Issuing OCA Private Key
ID	SMKI 106
Title:	Recovery from Compromise of a Contingency Private Key or the Contingency Symmetric Key

Description	As set out in section 6.1 of the SMKI Recovery Procedures
Objective	To prove in an end to end test the processes to recover from the Compromise of a Contingency Private Key or Contingency Symmetric Key