Version: L1.1

Appendix L

SMKI Recovery Procedure

Contents

1 Introduction

1.1 Purpose & Interpretation

Section L10.4 of the Code sets out the principle 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:

a) notwithstanding the definition as set out in Section A of the Code, “Subscriber” means, in relation to any Certificate associated with a Relevant Private Key, a Party which has been Issued with and accepted that Certificate, acting in its capacity as the holder of the 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) “Contingency Symmetric Key” means the Symmetric Key used to encrypt the Contingency Public Key;

d) “Contingency Keys” means the Contingency Symmetric Key and the Contingency Private Key;

e) Relevant Private Key has the meaning set out in Section L10; and

f) 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, that Party, and

   ii. in the case of a Key Custodian appointed by the SMKI PMA or the Panel, that SMKI PMA Member or Panel Member acting in its capacity as such.

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 or suspected Compromise of a Relevant Private Key reported to the DCC by a Party, resulting in an Incident being raised in accordance with sections 2.1 and 2.2 of the DCC's Incident Management Policy;
  ii. notification to the DCC of the Anomaly Detection Thresholds that are required to support replacement of affected Certificates 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 Certificates (where required); and
  v. other steps as set out in this SMKI Recovery Procedure;

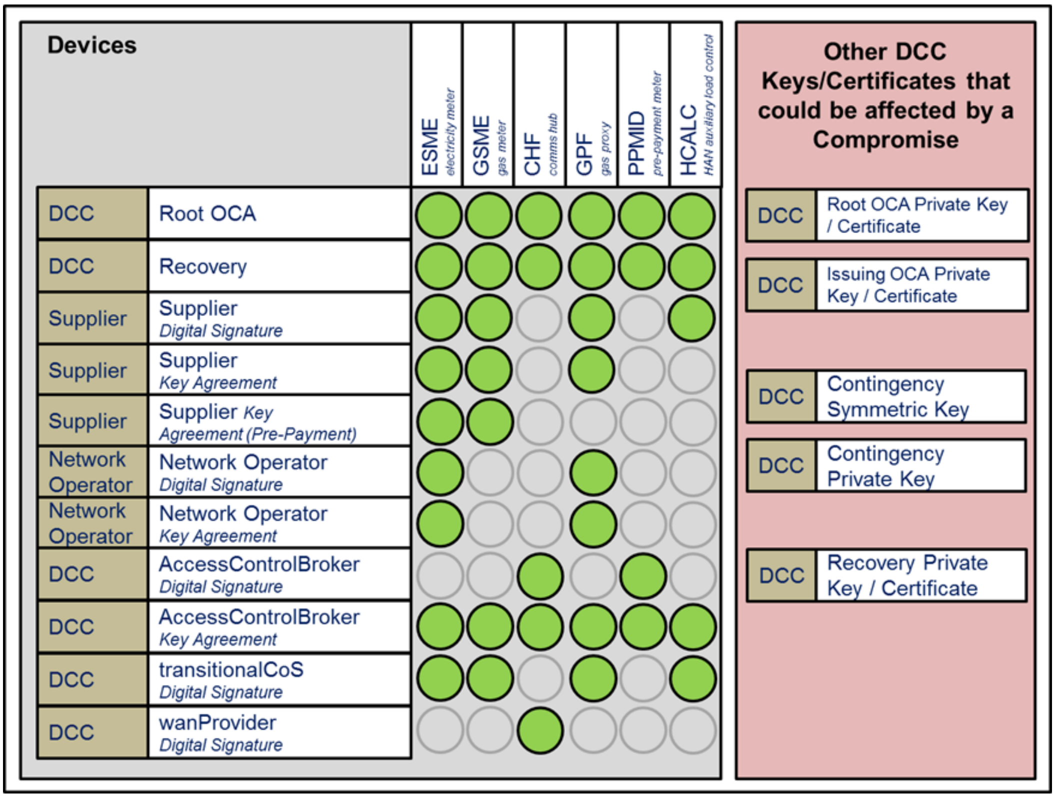
b) **Execution of Recovery**
  i. execution of activities to recover from a Compromise or suspected Compromise of a Relevant Private Key; and

c) **Post-Recovery**:
  i. replacement of 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
  iv. revocation of replaced Certificates (where necessary).

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

a) Private Keys associated with Organisation Certificates stored on Devices (other than those associated with a Recovery Certificate), where such Devices have an SMI Status of 'commissioned';
b) the Contingency Symmetric Key;
c) the Contingency Private Key;
d) the Private Key associated with an Issuing OCA Certificate;
e) the Private Key associated with a Root OCA Certificate; and
f) the Private Key associated with a Recovery Certificate.

Figure 1, immediately below, shows the relevant Certificates that are held on applicable Devices, and the relevant Certificates and Private Keys related to those held on Devices which are covered under the scope of the SMKI Recovery Procedure.



Devices		ESME *electricity meter*	GSME *gas meter*	CHF *comms hub*	GPF *gas proxy*	PPMID *pre-payment meter*	HCALC *HAN auxiliary load control*
DCC	Root OCA	●	●	●	●	●	●
DCC	Recovery	●	●	●	●	●	●
Supplier	Supplier *Digital Signature*	●	●	○	●	○	●
Supplier	Supplier *Key Agreement*	●	●	○	●	○	○
Supplier	Supplier *Key Agreement (Pre-Payment)*	●	●	○	○	○	○
Network Operator	Network Operator *Digital Signature*	●	○	○	●	○	○
Network Operator	Network Operator *Key Agreement*	●	○	○	●	○	○
DCC	AccessControlBroker *Digital Signature*	○	○	●	○	●	○
DCC	AccessControlBroker *Key Agreement*	●	●	●	●	●	●
DCC	transitionalCoS *Digital Signature*	●	●	○	●	○	●
DCC	wanProvider *Digital Signature*	○	○	●	○	○	○

Other DCC Keys/Certificates that could be affected by a Compromise

DCC	Root OCA Private Key / Certificate
DCC	Issuing OCA Private Key / Certificate
DCC	Contingency Symmetric Key
DCC	Contingency Private Key
DCC	Recovery Private Key / Certificate

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

2 Overview of the SMKI Recovery Procedure

In the event of an incident which:

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 (and in the case of the Contingency Symmetric Key, the DCC) 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 or suspected 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).

Compromise or Suspected Compromise of:	Section(s) of this document containing the procedure(s)
Private Key associated with Organisation Certificate held on one or more Devices (other than the Recovery Certificate)	**4.1 Method 1 - recovery by the affected Subscriber using its Private Key to replace affected Organisation Certificates on Devices** 4.1.1 Pre-Recovery 4.1.2 Execution of Recovery Procedure 4.1.3 Post-Recovery **4.2 Method 2 - recovery by the DCC using the Recovery Private Key to place DCC Access Control Broker Certificates on affected Devices (only available to a Supplier Party)** 4.2.1 Pre-Recovery 4.2.2 Execution of Recovery Procedure 4.2.3 Post-Recovery **4.3 Method 3 - recovery by the DCC using the Recovery Private Key to place new Organisation Certificates on 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

Compromise or Suspected Compromise of:	**Section(s) of this document containing the procedure(s)**
Issuing OCA Private Key	6.3.1 Pre-Recovery 6.3.2 Execution of Recovery Procedure 6.3.3 Post-Recovery

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, or suspected Compromise;
c) where the DCC attempts but fails to replace one or more Certificates as part of operating these procedures, execute as many retries to replace such Certificates as 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, or suspected 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 (or suspected Compromise), and the Devices and Subscribers affected by such Compromise; and
f) within three Working Days of the recovery from a Compromise or suspected 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, analysis of which communications have been submitted to 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. any proposed modifications to the SMKI Recovery Procedure that the DCC believes are necessary for the SMKI Recovery Procedure to more effectively meet the objectives as set out in the SEC.

3.2 Notification and confirmation of a suspected Compromise

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

Where the DCC is notified or becomes aware of a Compromise or suspected Compromise of a 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 or suspected Compromise has been notified. The DCC shall contact the Subscriber for the 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 member of SMKI Registration Authority Personnel on behalf of the DCC.

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 or suspected Compromise from a representative of the Subscriber as is defined in section 3.2 of this document, for a Certificate associated with a Compromised Private Key or from the DCC in respect of a Compromised Contingency Symmetric Key, 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.

Subject in either case to the approval of the SMKI PMA, where steps are taken to appoint a Key Custodian, or where (after such appointment) steps are taken by a Key Custodian, and in either case those steps would have been valid in accordance with this document if they were taken after its designation by the Secretary of State, they shall be treated as valid in accordance with this document, and therefore effective for the purposes of the Code, even if they were taken before its designation.

3.4.1 Responsibilities in respect of Key Custodians

Each Party, 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 do so as soon is as reasonably practicable following the request from 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 a 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 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;

b) the relevant Party, the SMKI PMA or Panel shall 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, provided that subject to the approval of the SMKI PMA, any action taken by DCC prior to the date of the designation of this SMKI Recovery Procedure shall, if the equivalent action taken after that date would have satisfied a requirement of this SMKI Recovery Procedure for the purposes of appointing a Key Custodian, be treated as if it had taken place after that date.

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 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 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

Step	When	Obligation	Responsibility	Next Step
3.4.3.3 (continued)		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: i. for a Party, an employee or Director of the Party; ii. for the DCC, an employee of the DCC or a DCC Service Provider; iii. for the SMKI PMA, an appointed member of the SMKI PMA; or iv. 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: i. British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or ii. 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: a) using publicly available information, whether the Director, Company Secretary, 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 b) whether the information supplied in the Key Custodian nomination form is complete and accurate.	DCC	If complete, 3.4.3.5; if not complete, 3.4.3.3

Step	When	Obligation	Responsibility	Next Step
		Where there are omissions/discrepancies, agree actions with the nominating Director, Company Secretary, SMKI PMA Chair or Panel Chair, via secured electronic means or in writing.		
3.4.3.5	As soon as reasonably practicable, following 10 Working Days after issuance of request for nominations	The DCC shall collate nominations received and shall provide to SMKI PMA: 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.	DCC	3.4.3.6
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 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 Level 3 (Verified) pursuant to the CESG GPG45 RSDOPS framework, or to such equivalent level within a comparable authentication framework as may be agreed by the SMKI PMA.	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 not at that point be appointed as a Key Custodian.	DCC	3.4.3.6
3.4.3.10	As soon as reasonably practicable, following 3.4.3.8	The DCC shall notify, in writing via secured electronic means: a) the individual, in person, that they are eligible to become a Key Custodian; and b) 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

Step	When	Obligation	Responsibility	Next Step
3.4.3.11	As soon as reasonably practicable, following 3.4.3.10	The DCC shall: a) 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 b) 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

4 Procedure to recover from the Compromise of a Private Key corresponding with a Public Key contained within an Organisation Certificate held on a Device (other than the Recovery Private Key)

This section sets out the procedures that may be used in order to recover from the Compromise (or suspected Compromise) of a Private Key associated with an Organisation Certificate held on a Device other than the Recovery Private Key, where a Subscriber wishes to recover from the Compromise (or suspected Compromise) using this procedure.

Where a Subscriber wishes to recover from the Compromise (or suspected Compromise) of such an 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 Private Key to replace the Organisation Certificate to which the Relevant Private Key relates on all affected Devices;

b) **Method 2:** (only applicable where the Subscriber is a Supplier Party), the DCC shall use the Recovery Private Key to replace affected Certificates on 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

c) **Method 3:** the DCC shall recover using the Recovery Private Key to replace affected Certificates on Devices with new Organisation Certificates provided by the Subscriber.

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

a) Where method 1 has been selected, perform the procedure as set out in Section 4.1 of this document;

b) Where method 2 has been selected, perform the procedure as set out in Section 4.2 of this document; or

c) 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 its Private Key to replace affected Organisation Certificates on Devices

4.1.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected 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.

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 Private Key	The affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates that are affected by the Compromise (or suspected Compromise). The DCC shall revoke such Certificates in accordance with the provisions of Appendix B of the Code and the SMKI RAPP.	Subscriber, DCC	4.1.1.2
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 Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex 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 relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot 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 or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure;	Subscriber	4.1.1.3

Step	When	Obligation	Responsibility	Next Step
		b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; 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 Threshold Anomaly Detection Procedure.		
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; and c) of details relating to the Compromise, comprising the Subscriber and the number of Devices affected, which will include the Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC.	DCC	4.1.1.4
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 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 using its own Private Key to recover. 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 Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC, which together contain details of the 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.

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 temporarily amend the Anomaly Detection Thresholds for the affected Subscriber to allow submission of Service Requests to replace affected Organisation Certificates, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure.. 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
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 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 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 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 Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E.	Subscriber	4.1.2.5
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 Device that is notified in step 4.1.1.1, he DCC shall notify the Responsible Supplier for affected Devices, via secured electronic means, which Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC.	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, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure 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 Threshold Anomaly Detection Procedure.	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: a) the completion of the affected Subscriber's activities in respect of the procedure as set out in this section 4.1; and b) the 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 Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex 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 Devices

4.2.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected 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.

Step	When	Obligation	Responsibility	Next Step
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 shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates. The DCC shall revoke Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP.	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 Annex 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 or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot 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 or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; 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 Threshold Anomaly Detection Procedure.	Subscriber	4.2.1.3

Step	When	Obligation	Responsibility	Next Step
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 (or suspected Compromise) of an Organisation Certificate or Organisation Certificates, using the 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 Devices). The DCC shall disable processing of communications destined for 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 Devices to 'recovery' The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	4.2.1.4
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 (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices, which may be provided in in one or more Organisation Compromise Notification Files that comply with Annex 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 (or suspected Compromise); 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 Device IDs to which the Compromise relates, which shall submitted in one or more Organisation Compromise Notification Files that comply with Annex B of this document.	DCC	4.2.1.6
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	DCC, Key Custodians	4.2.1.7

Step	When	Obligation	Responsibility	Next Step
		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.		
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 (or suspected 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. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	4.2.1.8
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.	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 devices where communications have previously been disabled by setting the SMI Status of any Device that had been set to "recovery" pursuant to Step 4.2.1.3 back to the SMI Status each such 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 necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of recovery Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in section 4.2.1 of this document; and b) for the affected Subscriber, to allow submission of Service Requests to replace DCC Access Control Broker Certificates with new Organisation Certificates. 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)	4.1.2.3
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 Device, Digitally Signed using the Recovery Private Key, in order to replace Organisation Certificates in all of the Supplier slots on Devices as notified in step 4.2.1.2, with a DCC Access Control Broker Certificate. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise.	DCC	4.2.2.5
4.2.2.5	As soon as reasonably practicable, following 4.2.2.4	Upon completion of step 4.2.2.4 for each Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status to 'recovered'.	DCC	4.2.2.6

Step	When	Obligation	Responsibility	Next Step
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 Devices: a) upon replacement of affected Certificates on each Device, using a DCC Alert issued via the DCC User Interface; and b) upon completion of attempts to replace all affected Certificates on relevant Devices, in one or more Organisation Compromise Recovery Progress Files that comply with Annex 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 Device slot with a replacement Organisation Certificate, for each Device as established in step 4.2.1.1 within section 4.2 of this document. Upon successful completion of such replacement for a Device, the DCC shall set the SMI Status for that 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
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 Annex C of this document.	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, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure that is Digitally Signed using the Private Key corresponding with a File Signing Certificate issued to the affected 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 Threshold Anomaly Detection Procedure. 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: 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 Annex C of this document; and b) the number of Devices for which recovery was not successful.	DCC	End of procedure

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

4.3.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected 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 (or suspected Compromise) using the procedure set out in this section.

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 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 Certificates in accordance with the provisions of the Appendix B of the Code and the SMKI RAPP.	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 Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex 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 relates; and c) for each Organisation Certificate that is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the Device IDs and the Device anchor slot which is populated with information from the affected Organisation Certificate.	Subscriber	4.3.1.3

Step	When	Obligation	Responsibility	Next Step
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 (or suspected 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 Certificates on Devices). Where the Compromise affects Supplier or CSP Certificates the DCC shall disable processing of communications destined for those 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 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 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 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 Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC.	DCC	4.3.1.5

Step	When	Obligation	Responsibility	Next Step
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 be taken in order to recover from the Compromise (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices, which may be provided in one or more one or more files which shall be Organisation Compromise Notification Files as set out in Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex D where the Subscriber is the DCC; 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 (or suspected 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	4.3.1.6
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): 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 environments that are required to support activation and use of the Recovery Private Key.	DCC, Key Custodians	4.3.1.7

Step	When	Obligation	Responsibility	Next Step
4.3.1.7	As soon as reasonably practicable, following 4.3.1.6	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 (or suspected Compromise); and 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. The SMKI PMA shall inform the DCC of its decision via a secured electronic means.	SMKI PMA, DCC	4.3.1.8
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. Where the affected Subscriber is not the Responsible Supplier for a 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 Device that had been set to "recovery" pursuant to Step 4.3.1.3 back to the SMI Status each such Device held immediately prior to the execution of step 4.3.1.3 of this procedure	DCC	4.3.2.2

Step	When	Obligation	Responsibility	Next Step
4.3.2.2	As soon as possible, following 4.3.2.1	Where necessary, the DCC shall temporarily amend the Anomaly Detection Thresholds, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected 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 number of the replacement Organisation Certificate that should be used to populate a Device and specify the Device slot 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 Annex B for Subscribers that are not the DCC, or Other Compromise Notification Files as set out in Annex 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 Devices, Digitally Signed using the Recovery Private Key, in order to replace affected Organisation Certificates on relevant Devices as notified in step 4.3.1.1 with replacement Certificates as notified by the affected Subscriber. In doing so, the DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of Devices affected by the Compromise.	DCC	4.3.2.6

Step	When	Obligation	Responsibility	Next Step
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 Devices: a) upon replacement of affected Certificates on each Device, using a DCC Alert issued via the DCC User Interface; and b) upon completion of attempts to replace all affected Certificates on relevant Devices, in one or more files which shall be Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex 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 Device, the DCC shall restore processing of communications destined for the affected Device by setting the SMI Status for that 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 Devices, by secured electronic means, which 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 Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex 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: a) 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 Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E where the Subscriber is the DCC; and b) the number of 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:

a) the notification of the Compromise (or suspected Compromise) of the Root OCA Private Key, in accordance with section 3.2 of this document; or

b) 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.

Step	When	Obligation	Responsibility	Next Step
5.1.1	As soon as reasonably practicable, following notification of the Compromise (or suspected Compromise) of the Root OCA Private Key or escalation due to failure of recovery using the Recovery Private Key, in accordance with section 3.2 of this document	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 could require use of the Contingency Private Key. The DCC shall also provide details to affected Subscribers of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Annex D of this document. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	5.1.2

Step	When	Obligation	Responsibility	Next Step
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 (or suspected Compromise), where such information may include (but shall not be limited to): a) the affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Annex 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) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) 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; 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.	DCC, Key Custodians	5.1.4

Step	When	Obligation	Responsibility	Next Step
5.1.4	As soon as reasonably practicable, following 5.1.3	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 (or suspected Compromise); and 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. 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 5.1.5
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 soon as reasonably practicable, following 5.1.5	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 Issuing OCA Certificate The DCC shall update and lodge the relevant ARL in the SMKI Repository and shall destroy affected Private Keys and Symmetric Keys, which may include: a) the old Root OCA Private Key; b) the old Issuing OCA Private Key; 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 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
5.2.2	As soon as possible, following 5.2.1	A SMKI ARO acting on behalf of each 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 or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; 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 Threshold Anomaly Detection Procedure.	Subscriber	5.2.3

Step	When	Obligation	Responsibility	Next Step
5.2.3	As soon as possible, following 5.2.2	The DCC shall temporarily amend the Anomaly Detection Thresholds, as required and including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for: a) the DCC that relate to the issuance of Commands to replace Certificates on Devices, to enable replacement of affected Certificates as notified in step 5.1.2; and b) affected Subscribers to allow submission of Service Requests to replace DCC Access Control Broker Certificates with new Organisation Certificates. 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 CPS, in order to generate:
		a) a new Contingency Symmetric Key;
		b) a new Contingency Key Pair;
		c) a new wrappedApexContingencyKey;
		d) a new Root OCA Key Pair ; and
		e) a new Issuing OCA Key Pair.
			DCC	5.2.5

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

Step	When	Obligation	Responsibility	Next Step
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 Contingency Private Key and the plain text version of the Contingency Symmetric Key that were used to generate the wrappedApexContingencyKey that is stored within the Root OCA Certificate that has been deployed to Devices. To facilitate this, the DCC shall bring together all parts of the Contingency Symmetric Key.	DCC	5.2.8

5.2.8	As soon as reasonably practicable, following 5.2.7	The DCC shall send Commands to all Devices, Digitally Signed using the Contingency Private Key and including the Contingency Symmetric Key to enable activation, attaching the following Certificates (where applicable according to the Device type) to the corresponding 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 Device slot or Network Operator Device slot in the corresponding 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 Device, the DCC shall restore processing of communications destined for the affected 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 Devices affected by the Compromise.	DCC	5.2.11

Step	When	Obligation	Responsibility	Next Step
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 Devices: a) upon replacement of affected Certificates on each 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 Certificates (for each affected Subscriber) on relevant Devices, in one or more Other Compromise Recovery Progress Files that comply with Annex 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 Devices, via secured electronic means, in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, which 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 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	5.3.2

Step	When	Obligation	Responsibility	Next Step
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: a) the DCC Access Control Broker Certificate in each Supplier Device slot with a replacement Organisation Certificate that is Issued under the new Issuing OCA, for each 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 Device slot with an Organisation Certificate to which the Network Operator is the Subscriber that is Issued under the new Issuing OCA, for each Device as established in step 5.2.2 within section 5.2 of this document. Upon successful completion of such replacement for a Device, the DCC shall set the SMI Status for that 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 Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document.	Subscriber	5.3.3

Step	When	Obligation	Responsibility	Next Step
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 Threshold Anomaly Detection Procedure 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 Threshold Anomaly Detection Procedure. 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 Annex E of this document.; and b) the number of Devices for which recovery was not successful.	DCC	End of procedure

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

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

6.1.1 Pre-Recovery

The DCC shall execute the procedure as set out immediately below, following notification of the Compromise (or suspected Compromise) of the Contingency Private Key or the Contingency Symmetric Key in accordance with section 3.2 of this document.

Step	When	Obligation	Responsibility	Next Step
6.1.1.1	As soon as reasonably practicable, following notification of the Compromise (or suspected 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 notify all affected Subscribers, via a secured electronic means, as soon as reasonably practicable, that a Compromise of the Contingency Private Key or Contingency Symmetric Key has been notified and shall provide details of the affected Devices and Certificates, in one or more Other Compromise Notification files which comply with Annex D of this document.	DCC	6.1.1.3

Step	When	Obligation	Responsibility	Next Step
6.1.1.3	As soon as reasonably practicable, following 6.1.1.2	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 (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Annex D of this document; b) the extent to which the vulnerabilities that caused the Compromise have been addressed; c) the extent to which DCC's monitoring indicates that there has been unauthorised use of the Contingency Private Key; d) the steps that DCC reasonably believes should be taken to recover from the Compromise (or suspected Compromise); and e) anticipated timescales for recovery.	DCC, SMKI PMA	6.1.1.4
6.1.1.4	As soon as reasonably practicable, following 6.1.1.3	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 either take such steps or instruct Parties 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 Key Pairs is required and the date, time and location of each the Key Generation Ceremony; b) notifying Key Custodians to attend the location at which a relevant Key Generation Ceremony may be required; and c) activities required to prepare such systems environment required to support generation of a new Contingency Key Pair, Contingency Symmetric Key, Root OCA Key Pair and replacement Root OCA Certificate, Issuing OCA Key Pair and Issuing OCA Certificate that may be required.	DCC, Key Custodians	6.1.1.5

Step	When	Obligation	Responsibility	Next Step
6.1.1.5	As soon as reasonably practicable, following 6.1.1.4	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 (or suspected Compromise); and b) confirm whether the timescales proposed by the DCC (following consultation with the affected Subscriber(s)) in step 6.1.1.3 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 6.1.1.6
6.1.1.6	As soon as reasonably practicable, following 6.1.1.5	The DCC shall notify all affected Subscribers, via a 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 6.1.2.	DCC	Procedure as set out in section 6.1.2 of this document

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	A SMKI ARO acting on behalf of each 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 or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; 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 Threshold Anomaly Detection Procedure.	Subscriber	6.1.2.2
6.1.2.2	As soon as reasonably practicable, following 6.1.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds; including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for the DCC and affected Responsible Suppliers to allow submission of Service Requests to replace the Root OCA Certificate on Devices. The DCC shall inform, via secured electronic means, a SMKI SRO and the SMKI ARO that provided the details in step 6.1.2.1, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	6.1.2.3

Step	When	Obligation	Responsibility	Next Step
6.1.2.3	As soon as reasonably practicable, following 6.1.2.2	The DCC shall conduct relevant Key Generation Ceremonies, in order to generate the following, in accordance with the Organisation CPS and the Great Britain Companion Specification (GBCS): a) a new Contingency Symmetric Key; b) a new Contingency Key Pair c) a new Root OCA Key Pair; d) a new Issuing OCA Key Pair and e) a new wrappedApexContingencyKey.	DCC (as TSP) for Contingency Symmetric Key; DCC (as DSP) for Contingency Key Pair	6.1.2.4
6.1.2.4	As soon as reasonably practicable, following 6.1.2.4	The DCC shall generate a replacement Root OCA Certificate, embedding the new wrappedApexContingencyKey that has been generated as part of the process as set out in step 6.1.2.3 of this document. The replacement Root OCA Certificate shall be Digitally Signed by the existing Root OCA Private Key and the new Root OCA Private Key. The DCC shall generate a replacement Issuing OCA Certificate, which shall be Digitally Signed by the new Root OCA Private Key.	DCC (as TSP)	6.1.2.5
6.1.2.5	As soon as reasonably practicable, following 6.1.2.4	The DCC shall lodge the replacement Root OCA Certificate and Issuing OCA Certificate in the SMKI Repository.	DCC	6.1.2.6

Step	When	Obligation	Responsibility	Next Step
6.1.2.6	As soon as reasonably practicable, following 6.1.2.5	The DCC shall notify, via secured electronic means: a) the target deadline for the submission of Service Requests to replace affected Root OCA Certificates on affected Devices, which shall be assessed by the DCC based on the number of Devices affected; and b) the replacement Root OCA Certificate serial number, which shall be provided in one or more Other Compromise Notification Files as set out in Annex D of this document. Such notification shall be provided by the DCC to the organisation responsible, which shall be: a) for all Communications Hub Functions, the DCC (the Service Provider that is the provider of the WAN for the relevant Region); or b) for all other Devices, shall be the Responsible Supplier that is the Subscriber for the Organisation Certificate held in the supplier digital signing slot on that Device, for that Device.	DCC	6.1.2.7
6.1.2.7	As soon as reasonably practicable, following 6.1.2.6	The organisation as defined in step 6.1.2.6, shall retrieve the replacement Root OCA Certificate from the SMKI Repository and shall send such Service Requests, in accordance with the provisions of the DCC User Interface Specification, (or in the case of the DCC, issue such Commands) as are required to replace the existing Root OCA Certificate on all affected Devices with the new Root OCA Certificate.	Supplier	6.1.2.8

Step	When	Obligation	Responsibility	Next Step
6.1.2.8	As soon as reasonably practicable, following 6.1.2.7	The DCC shall monitor its Command acknowledgement records, to determine the progress of recovery in respect of replacement of the Root OCA Certificate. The DCC shall also monitor for unauthorised use of the Contingency Private Key and shall take all reasonable steps to keep the SMKI PMA informed as to such unauthorised use. Where directed to amend the recovery steps based on unauthorised use, the DCC execute steps as notified by the SMKI PMA. Following the deadline for Root OCA Certificate replacement as set out in step 6.1.2.7, the DCC shall identify whether recovery for all affected Devices has been successfully completed. Where recovery of all affected Devices has not been completed, the DCC shall notify, via a secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, to each organisation as established in step 6.1.2.7 of the list of Devices where the replacement of Root OCA Certificates has not been successfully completed.	DCC (as DSP)	6.1.2.9
6.1.2.9	As soon as reasonably practicable, following 6.1.2.8	The DCC shall notify each Responsible Supplier for affected Devices which Devices were not recovered successfully, using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, via secured electronic means.	DCC	Procedure as set out in Section 6.1.3 of this document

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	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 Threshold Anomaly Detection Procedure 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 an affected Subscriber, including performing the checks and validations set out in the Threshold Anomaly Detection Procedure. 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 6.1 of this document.	DCC (DSP TAD)	6.1.3.2
6.1.3.2	As soon as reasonably practicable, following 6.1.3.1	The DCC shall destroy the replaced Root OCA Private Key, Issuing OCA Private Key, Contingency Private Key and Contingency Symmetric Key.	DCC (as DSP, TSP)	6.1.3.3
6.1.3.3	As soon as reasonably practicable, following 6.1.3.2	The DCC shall notify the SMKI PMA, 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 Annex E of this document; and b) the number of Devices for which recovery was not successful.	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 (or suspected 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 Compromise (or suspected Compromise) of the Recovery Private 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 Recovery Private Key has been notified. The DCC shall request a decision from the SMKI PMA as to whether recovery should be carried out.	DCC	6.2.1.2
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 Devices and Certificates, in one or more Other Compromise Notification Files which comply with Annex D of this document.	DCC	6.2.1.3

Step	When	Obligation	Responsibility	Next Step
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 (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification Files which comply with Annex 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 (or suspected 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 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; and 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	6.2.1.5

Step	When	Obligation	Responsibility	Next Step
6.2.1.5	As soon as reasonably practicable, following 6.2.1.4	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 (or suspected Compromise); and b) 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
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 Certificates on Devices, to enable replacement of affected 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

Step	When	Obligation	Responsibility	Next Step
6.2.2.4	As soon as reasonably practicable, following 6.2.2.3	The DCC shall send Commands to all Devices to replace the Recovery Certificate held on such 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. Once submitted, the DCC shall confirm for each affected 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.	DCC (as DSP)	6.2.2.5
6.2.2.5	As soon as reasonably practicable, following 6.2.2.4	The DCC shall notify each Responsible Supplier for affected Devices, by secured electronic means, which Devices were not recovered successfully, in one or more Other Compromise Recovery Progress Files that comply with Annex 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	The DCC shall destroy 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.	DCC (as DSP)	6.2.3.3

Step	When	Obligation	Responsibility	Next Step
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 Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Annex 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 (or suspected 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 (or suspected 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 Devices and Certificates, in one or more Other Compromise Notification files which comply with Annex D of this document	DCC	6.3.1.3

Step	When	Obligation	Responsibility	Next Step
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 (or suspected Compromise), where such information may include (but shall not be limited to): a) the number of affected Devices and Subscribers, which may be provided in one or more Other Compromise Notification files which comply with Annex 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 (or suspected 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; and 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

Step	When	Obligation	Responsibility	Next Step
6.3.1.5	As soon as reasonably practicable, following 6.3.1.4	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 (or suspected Compromise); and b) 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	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 DSP)	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 confirmation of Compromise and instruction from the SMKI PMA that this recovery procedure should be carried out	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, which shall include amended Anomaly Detection Thresholds that they estimate will be required to resolve the Compromise or suspected Compromise. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File is: a) submitted using the mechanism specified in the Threshold Anomaly Detection Procedure; b) in the format as set out in section 5.3 of the Threshold Anomaly Detection Procedure; 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 Threshold Anomaly Detection Procedure.	Subscriber	6.3.2.2
6.3.2.2	As soon as reasonably practicable, following 6.3.2.1	The DCC shall temporarily amend the Anomaly Detection Thresholds; including performing the checks and validations set out in the Threshold Anomaly Detection Procedure, for affected Subscribers to allow submission of Service Requests to replace affected Organisation Certificates on 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 Certificates on Devices, to enable replacement of the affected Recovery Certificate on 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

Step	When	Obligation	Responsibility	Next Step
6.3.2.4	As soon as reasonably practicable, following 6.3.2.3	The DCC shall: a) determine the number of Key Custodians required to attend a Key Generation Ceremony for the relevant Recovery Private Key; b) 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 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, Digitally Signed using the new Issuing OCA Private Key.	DCC, Key Custodians	6.3.2.5
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

Step	When	Obligation	Responsibility	Next Step
6.3.2.6	As soon as reasonably practicable, following 6.3.2.5	The DCC shall send Commands to all Devices to replace the Recovery Certificate held on such 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 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 Annex E of this document, of the list of 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 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 Certificates on Devices, each affected Subscriber shall notify the DCC in respect of replacement of affected Certificates with new Organisation Certificates, via secured electronic means and in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document.	Subscriber	6.3.2.9

Step	When	Obligation	Responsibility	Next Step
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 Devices, via secured electronic means and using one or more Other Compromise Recovery Progress Files that comply with Annex E of this document, the 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
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, which shall be submitted as a file as set out in section 5.1 of the Threshold Anomaly Detection Procedure 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 Threshold Anomaly Detection Procedure. 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)	6.3.3.2
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 Devices for which recovery was not successful, which may be provided in one or more Other Compromise Recovery Progress Files that comply with Annex E of this document.	DCC	End of procedure

7 Periodic testing of the SMKI Recovery Procedure

7.1 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:

g) 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 or suspected 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;
   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 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.

h) 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 Certificates on Devices that are initiated via Service Requests issued by Subscribers.

i) 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;

j) agree such testing scenarios with the SMKI PMA;

k) create test data based upon data collected by the DCC and, where necessary, acquired from Parties;

l) maintain a test environment in order to carry out such periodic testing of the SMKI Recovery Procedure;

m) carry out testing of the SMKI Recovery Procedure for agreed scenarios; and

n) 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:

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

Annex 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
- 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 Threshold Anomaly Detection Procedure.

Annex B: Organisation Compromise Notification File

Each Organisation Compromise Notification File shall be in the format set out in this Annex 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 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 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 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 100,000 such records permitted within any file)* ▲
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 Threshold Anomaly Detection Procedures.

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 Certificate serial number of the Certificate affected by the Compromise that is used to populate the Digital Signing anchor slot on affected Devices.

d) The Affected_Certificate_Serial_Number_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Key Agreement Key anchor slot on affected Devices.

e) The Affected_Certificate_Serial_Number_KAKPP field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the prepayment Key Agreement Key anchor slot 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 Certificate serial number for the Certificate to be used to populate the Digital Signing Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

g) The Replacement_Certificate_Serial_Number_KAK field contains the Certificate serial number for the Certificate to be used to populate the Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

h) The Replacement_Certificate_Serial_Number_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the prepayment Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots 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.

Annex C: Organisation Compromise Recovery Progress File

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

a) *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:
  - 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 100,000 such records permitted within any file)* ▲

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 Threshold Anomaly Detection Procedures.▲,

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 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 Certificate serial number of the Certificate affected by the Compromise that is used to populate the Digital Signing anchor slot on affected Devices, where applicable.

f) The Affected_Certificate_Serial_Number_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Key Agreement Key anchor slot on affected Devices, where applicable.

g) The Affected_Certificate_Serial_Number_KAKPP field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the pre-payment Key Agreement Key anchor slot on affected Devices, where applicable.

h) The Replacement_Certificate_Serial_Number_DS field contains the Certificate serial number for the Certificate to be used to populate the Digital Signing Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

i) The Replacement_Certificate_Serial_Number_KAK field contains the Certificate serial number for the Certificate to be used to populate the Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots using the Recovery Private Key or Contingency Private Key.

j) The Replacement_Certificate_Serial_Number_KAKPP field contains the Certificate serial number for the Certificate to be used to populate the prepayment Key Agreement Key Device anchor slot. This field shall not be populated where the relevant step of the SMKI Recovery Procedure does not require an affected Subscriber to provide replacement Certificates that the DCC will use to populate Devices' anchor slots 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement information from the affected Certificate in the Digital Signing anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Key Agreement Key anchor slot on a Device.

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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the prepayment Key Agreement Key anchor slot 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.

Annex D: Other Compromise Notification File

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

a) *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 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 100,000 such records permitted within any file)* ▲

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 Certificate serial number of the Root OCA Certificate affected by the Compromise that is used to populate the Root anchor slot on affected Devices, where applicable.

d) The Affected_Certificate_Serial_Number_Recovery field contains the Certificate serial number of the Recovery Certificate affected by the Compromise that is used to populate the Recovery anchor slot on affected Devices, where applicable.

e) The Affected_Certificate_Serial_Number_Supplier_DS field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Supplier Digital Signing anchor slot on affected Devices, where applicable.

f) The Affected_Certificate_Serial_Number_Supplier_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Supplier Key Agreement Key anchor slot on affected Devices, where applicable.

g) The Affected_Certificate_Serial_Number_Supplier_KAKPP field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Supplier pre-payment Key Agreement Key anchor slot on affected Devices, where applicable.

h) The Affected_Certificate_Serial_Number_NetworkOperator_DS field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Network Operator Digital Signing anchor slot on affected Devices, where applicable.

i) The Affected_Certificate_Serial_Number_NetworkOperator_KAK field contains the Certificate serial number of the Certificate affected by the Compromise that is used to populate the Network Operator Key Agreement Key anchor slot on affected Devices, where applicable.

j) The Affected_Certificate_Serial_Number_COS_DS field contains the Certificate serial number of the TCoS Certificate affected by the Compromise that is used to populate the TCoS anchor slot on affected Devices, where applicable.

k) The Affected_Certificate_Serial_Number_WAN_DS field contains the Certificate serial number of the WAN Provider Certificate affected by the Compromise that is used to populate the WAN Provider anchor slot on affected Devices, where applicable.

l) The Replacement_Certificate_Serial_Number_Root field contains the Certificate serial number for the Certificate to be used to populate the Device Root anchor slot, where applicable.

m) The Replacement_Certificate_Serial_Number_Recovery field contains the Certificate serial number for the Certificate to be used to populate the Device Recovery anchor slot, where applicable.

n) 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 anchor slot, where applicable.

o) 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 anchor slot, where applicable.

p) 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 anchor slot, where applicable.

q) 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 anchor slot, where applicable.

r) 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 anchor slot, where applicable.

s) The Replacement_Certificate_Serial_Number_COS_DS field contains the Certificate serial number for the Certificate to be used to populate the Device TCoS anchor slot, where applicable.

t) 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 anchor slot, where applicable.

Annex E: Other Compromise Recovery Progress File

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

a) *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.
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 100,000 such records permitted within any file)* ▲

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 Threshold Anomaly Detection Procedures.

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 Certificate serial number for the Certificate to be used to populate the Device Root anchor slot.

f) The Replacement_Certificate_Serial_Number_Recovery field contains the Certificate serial number for the Certificate to be used to populate the Device Recovery anchor slot.

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 anchor slot.

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 anchor slot.

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 anchor slot.

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 anchor slot.

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 anchor slot.

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 anchor slot.

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 anchor slot.

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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Root anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Recovery anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Digital Signing anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier Key Agreement Key anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Supplier prepayment Key Agreement Key anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Digital Signing anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the Network Operator Key Agreement Key anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the TCoS anchor slot 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 4.1.3.3 of the Message Mapping Catalogue, in relation to the replacement of information from the affected Certificate in the WAN Provider anchor slot 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.

Annex 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
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 Annex 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 Annex C of the SMKI Recovery Procedure
Other Compromise Notification File	A CSV file used to support recovery from a Compromise that is specified in Annex D of the SMKI Recovery Procedure
Other Compromise Recovery Progress File	A CSV file used to support recovery from a Compromise that is specified in Annex E of the SMKI Recovery Procedure
Trusted Service Provider, or TSP	Means the DCC acting using systems identified in part (d) of the definition of DCC Live Systems

Annex G: SMKI Recovery Procedure Test Scenarios

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

8.1 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

8.2 DCC / Subscriber and DCC / Party Interactions and Processes

8.2.1 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 Subscriber communicates decision in the form of a Certificate ID to the DCC through the DCC Service Desk
Objective	• To prove the Subscriber can request new Organisation Certificates or identify and obtain existing Organisation Certificates to be placed on affected Devices during the Recovery process • To prove Subscriber communications with the DCC Service Desk in respect of the replacement Organisation Certificates

8.2.2 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**

8.2.3 Subscriber notification of Compromise (or suspected 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 Threshold Anomaly Detection Procedures**
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**

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

ID	SMKI 204
Title:	**Method 1 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 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**

8.3 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 Annex 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**

8.4 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 4.1 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 Annex 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 3of Organisation Certificate Recovery** • **To prove interactions between Responsible Suppliers and DCC Service Desk during Method 3 of Organisation Certificate Recovery**

8.5 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**

Description	**As set out in section 4.1 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**

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**