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

SMKI PMA Guidance: Recovering from a Compromise of SMETS1 Keys

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.0
Date	25 July 2019
Document Status	SMKI PMA Approved
Date of Next Review	TBD
Classification	White

Change Record

Date	Author	Version	Change Reference
25/07/2019	SECCo	0.1	Draft version created for review by SMKI Specialist, BEIS and DCC.
25/07/2019	SECCo	1.0	Final version after comment from DCC and SMKI Specialist.

Table of Contents

1. Introduction

Section L10.4 of the Smart Energy Code (SEC) sets out the principle rights and obligations for compliance with any requirements set out in the SMKI Recovery Procedure. The detailed SMKI Recovery Procedures are set out in SEC Appendix L.

The SEC Appendix L is being modified by the SMKI PMA, subject to consultation by BEIS, to include the Recovery Procedures that apply to the Private Keys associated with the SMETS1 Service Provider (S1SP) Held Signing Device Security Credentials in the event of a Compromise after Enrolment and Adoption into the DCC.

Until the SMETS1 Recovery Procedures are implemented into the SEC, the SMKI PMA have provided the guidance set out in this document in line with SEC Appendix L which states "*The procedures as set out in this document* [SEC Appendix L] *shall be executed in the event of a Compromise (or suspected Compromise) of a Relevant Private Key,* ***other than as directed by the SMKI PMA, in accordance with the procedures set out in this document****."*

The procedures as set out in this document shall be executed in the event of a Compromise (or suspected Compromise) of a Relevant Private Key,

For the purposes of these procedures:

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

b) a Private Key is "associated" with an Organisation Certificate where that Private Key is associated with the Public Key contained within that Organisation Certificate;

2. Scope and Purpose

The purpose of these procedures is to provide guidance for the DCC, Parties and the SMKI PMA in the event of a Compromise to the Private Keys associated with the S1SP Held Signing Device Security Credentials.

In this document, the use of defined terms (where capitalised) have the same meaning as those defined in the Smart Energy Code and are not redefined within this document.

3. SMETS1 Cryptography

SMETS1 Enrolment and Adoption uses SMKI and DCCKI where appropriate. SMKI is used to allow signing and authentication of SMETS1 messages both by DCC Users and all other components which form part of the solution (except for communications to CHs and Devices where existing cryptographic protections will be used as the basis for the solution).

Unlike SMETS2, the SMETS1 Devices do not hold all the cryptographic credentials. The S1SP holds the Organisation Certificates for the SMETS1 security credentials for SMETS1 Devices.

Figure 1 below, shows the relevant Organisation Certificates that form part of the S1SP Held Signing Device Security Credentials for SMETS1 Devices that are enrolled into the DCC:

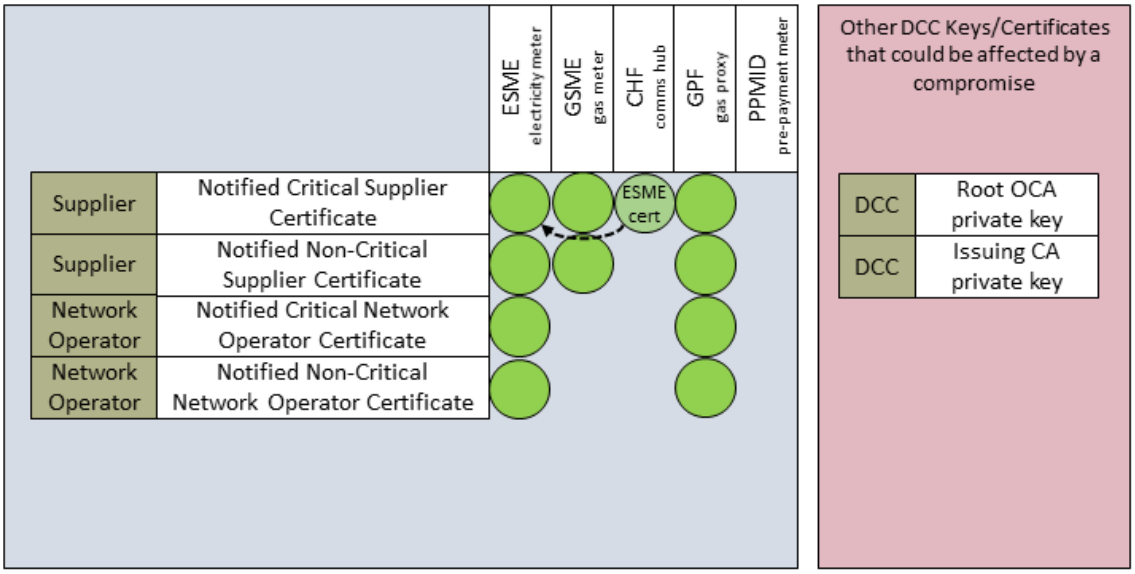

Figure 1: Organisation Certificates used by S1SPs for security credentials for SMETS1 Devices

The Check of Cryptographic Protection applied by an S1SP to a Critical Service Request targeting a SMETS1 CHF is carried out using the Notified Critical Supplier Certificate for the corresponding SMETS1 ESME. No separate certificate is stored

4. Notification and confirmation of a suspected Compromise

This section is taken directly from SEC Appendix L Section 4.

Any person may notify the DCC that there is a Compromise or suspected Compromise of a Relevant Private Key or a Private Key associated with an Organisation Certificate containing the related Public Key, where that Private Key is used by a User to Digitally Sign any Service Request.

Where the DCC is notified or becomes aware of a Compromise or suspected Compromise of a Relevant Private Key or a Private Key associated with an Organisation Certificate that is used by a User to Sign any Service Request or Signed Pre-Command, 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 Organisation Certificate associated with that Private Key or Contingency Symmetric Key (which may include the DCC itself as the Subscriber), as soon as reasonably practicable, via telephone and email using the contact details held by the SMKI Registration Authority. The DCC shall provide the Subscriber, via secured electronic means, with the appropriate Incident reference number and information relating to the notified Compromise. The DCC shall request confirmation from the Subscriber as to whether the Subscriber reasonably believes that a Compromise has occurred, and wishes to proceed with one or more of the recovery processes, which shall be confirmed by:

a) A SMKI Senior Responsible Officer (SMKI SRO) on behalf of a Party; or

b) A SMKI SRO, SMKI Registration Authority Manager or 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.

4 (continued)

Procedure to recover from the Compromise of a Private Key corresponding with a Public Key which forms part of any S1SP Held Device Security Credentials

This section will, subject to consultation, be included in SEC Appendix L in due course and will be Section 4.1A.

4.1A Method 1A – replacement by the affected Subscriber using its Compromised Private Key (or one suspected of being Compromised) of associated S1SP Held Device Security Credentials

4.1A.1 Pre-Recovery

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

Informative:

- This section does not apply to User Role Signing Private Keys. Please see Section 5 [the Modified SEC version will be Section 7] of this document for further guidance on the User Role Signing Keys.
- This section is only applicable to Responsible Suppliers, Electricity Distributors, Gas Transporters and the DCC.
- All S1SP Held Device Security Credentials are Organisation Certificates.
- In accordance with the definition included within Section A of the Code, S1SP Held Device Security Credentials include the Notified Critical Supplier Certificate ID, Notified Non-Critical Supplier Certificate ID, Notified Critical Network Operator Certificate ID, Notified Non-Critical Network Operator Certificate ID, Notified Critical Supplier ID, Notified Non-Critical Supplier ID, Notified Critical Network Operator ID and Notified Non-Critical Network Operator ID identified by the Organisation Certificates contained within the ReplacementCertificates (with its DUIS meaning) of a Service Request. . These are held by the DCC S1SP and not on the SMETS1 Device.

Step	When	Obligation	Responsibility	Next Step
4.1A.1.1	As soon as possible, following notification that the Subscriber wishes to recover using its own Compromised (or one suspected of being Compromised) Private Key associated with the Public Key contained within an Organisation Certificate that forms part of any S1SP Held Device Security Credentials	The affected Subscriber shall consider the security risks arising from the Compromise or suspected Compromise of its Private Key and be aware that, until the Private Key is destroyed, there is a risk of the Private Key being used to achieve adverse consequences for the consumer. However, it should be noted that revoking the Organisation Certificate (that forms part of any S1SP Held Device Security Credentials) containing the Public Key associated with the Compromised (or one suspected of being Compromised) Private Key will prevent the Private Key from being used to send authorised Commands to a SMETS1 Device. This is due to the fact that once a CRL is published, the DSP/S1SP/DCO will reject Service Requests destined for SMETS1 Devices signed using a Private Key with an associated Revoked Organisation Certificate. Due consideration should be given before destroying a Compromised (or one suspected of being Compromised) Private Key and its associated Organisation Certificate if the recovery steps detailed in 4.1A.2.1 to 4.1A.2.5 of this section have not yet been carried out. Destroying the Private Key and/or its associated Organisation Certificate prior to carrying out these steps may put pre-payment customers at risk. It is advisable to conduct the replacement of Organisation Certificates that form part of any S1SP Held Device Security Credentials as quickly as possible in accordance with 4.1A.2.2 of this document.	Subscriber,	4.1A.1.2
4.1A.1.2	As soon as reasonably practicable, following 4.1A.1.1	A SMKI ARO acting on behalf of the affected Subscriber shall submit to the DCC, via secured electronic means, one or more files which shall be Organisation Compromise Notification Files as set out in Annex B. The affected Subscriber should ensure that such files together contain details of: a) the Incident to which the submission relates;	Subscriber	4.1A.1.3

		b) the EUI-64 identifiers for the organisation that is the affected Subscriber to which the Compromise, or suspected Compromise of the Private Key relates; and c) for each Organisation Certificate that forms part of any S1SP Held Device Security Credentials and is affected by the Compromise or suspected Compromise, the serial number of the Organisation Certificate, the SMETS1 Device IDs and the nature of the affected S1SP Held Device Security Credentials. In addition, a SMKI ARO acting on behalf of the affected Subscriber shall, as soon as reasonably practicable, submit an Anomaly Detection Thresholds File to the DCC, which shall include amended Anomaly Detection Thresholds that they estimate will be required to replace the affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials. The affected Subscriber shall ensure that the Anomaly Detection Thresholds File 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.		
4.1A.1.3	As soon as reasonably practicable, following 4.1A.1.2	The DCC shall notify the SMKI PMA, via a secured electronic means, as soon as reasonably practicable: a) that a Compromise of an Organisation's Private Key has been notified; b) that the Subscriber intends to use method 1 (as set out in section 4.1A of this document) to recover; and c) of details relating to the Compromise, comprising the Subscriber and the number of Organisation Certificates that form a part of any S1SP Held Device Security Credentials affected, which will include the Organisation Compromise Notification Files as set out in 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	4.1A.1.4

4.1A.1.4	As soon as reasonably practicable, following 4.1A.1.3	Where the affected Subscriber is not the Responsible Supplier for a SMETS1 Device that is notified in step 4.1A.1.1, the DCC shall notify the Responsible Supplier, via secured electronic means, that a Subscriber wishes to recover from Compromise using its own Private Key. The DCC shall also provide to the Responsible Supplier, via a secured electronic means, one or more Organisation Compromise Notification Files as set out in 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 SMETS1 Device IDs to which the Compromise relates.	DCC	Procedure as set out in section 4.1A.2 of this document

4.1A.2 Execution of Recovery Procedure

The procedure as set out immediately below, amended as instructed by the SMKI PMA, shall be used following execution of the process as set out in section 4.1A.1 of this document.

Step	When	Obligation	Responsibility	Next Step
4.1A.2.1	As soon as reasonably practicable, following procedure as set out in section 4.1A.1	The DCC shall 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 4.1A.1.2, that the Anomaly Detection Threshold values have been successfully amended.	DCC (DSP TAD)	4.1A.2.2
4.1A.2.2	As soon as reasonably practicable, following 4.1A.2.1	The affected Subscriber shall either: a) identify replacement Organisation Certificates that form a part of any S1SP Held Device Security Credentials; or b) submit such Certificate Signing Requests (CSRs) that are required in order to acquire new Organisation Certificates that form a part of any S1SP Held Device Security Credentials.	Subscriber	4.1A.2.3
4.1A.2.3	As soon as reasonably practicable, following 4.1A.2.2	The affected Subscriber shall submit Service Requests as required, in accordance with the provisions of the DCC User Interface Specification, to replace affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials and shall, in doing so, monitor replacement of such affected Organisation Certificates.	Subscriber	4.1A.2.4
4.1A.2.4	As soon as reasonably practicable, following 4.1A.2.3	Upon completion of its activities to replace affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials, the affected Subscriber shall inform the DCC, via a secured electronic means: a) that its activities in respect of the replacement of Organisation Certificates that form a part of any S1SP Held Device Security Credentials have been completed; and	Subscriber	4.1A.2.6 or 4.1A.2.5 if appropriate

		b) of the Organisation Certificates that form a part of any S1SP Held Device Security Credentials for which replacement has not been completed, which shall be submitted as one or more Organisation Compromise Recovery Progress Files as set out in Annex C for Subscribers that are not the DCC, or Other Compromise Recovery Progress Files as set out in Annex E.		
4.1A.2.5	As soon as reasonably practicable, following 4.1A.2.4	Where the affected Subscriber is not the Responsible Supplier for a SMETS1 Device that is notified in step 4.1A.1.1, the DCC shall notify the Responsible Supplier for affected SMETS1 Devices, via secured electronic means, which SMETS1 Devices were not recovered successfully, in one or more Organisation Recovery Progress Files as set out in 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 4.1A.2.6 of this document
4.1A.2.6	As soon as reasonably practical following 4.1A.2.4	The affected Subscriber shall submit Certificate Revocation Requests (CRRs), as set out in the SMKI RAPP, in order to revoke affected Organisation Certificates that form a part of any S1SP Held Device Security Credentials. The DCC shall revoke Organisation Certificates that form a part of any S1SP Held Device Security Credentials in accordance with the provisions of Appendix B of the Code and the SMKI RAPP. The affected Subscriber shall destroy the Private Key associated with the revoked Organisation Certificate that forms a part of any S1SP Held Device Security Credentials.	Subscriber, DCC	Procedure as set out in section 4.1A.3 of this document

4.1A.3 Post-Recovery

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

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

5. Replacement of a User Role Signing Private Key

The procedures for revoking an Organisation Certificate associated with a User Role Signing Private Key that is compromised or suspected of being compromised are laid out in SEC Appendix D – SMKI RAPP and SEC Appendix B – Organisation Certificate Policy.

User Role Signing Private Key destruction considerations

In accordance with Section 3.3.1 of Appendix AD of the SEC, each User Role Signing Private Key must be a separate dedicated Key that is not be used for communication with Devices (i.e. different to that used to sign the GBCS Payload held within Signed Pre-Commands).

Should a User Role Signing Private Key be destroyed and the associated Organisation Certificate be revoked prior to either Method 1 or Method 2 recovery method (as set out in SEC Appendix L) activities being carried out, this will prevent the User from having Service Requests and Signed Pre-Commands being successfully processed by the DCC until User Role Signing Private Key has been replaced and the corresponding replacement Organisation Certificate has been created and has been notified to the DCC. This is the case even if the Private Key used to Digitally Sign the GBCS Payload held within Signed Pre-Commands has not been destroyed and the corresponding Organisation Certificate has not been revoked.

Therefore, it is important for Subscribers to consider the sequence of Private Key destruction and Organisation Certificate revocation when in a recovery scenario.

Appendix A Communication Formats

In Appendices B to E of SEC Appendix L, 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.

Appendix B Organisation Compromise Notification File

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

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

a) *OC_Priority_UserID_IncidentID_N_FileNum*.csv

Where:

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