This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

SMKI Recovery Key Guidance

Version 1.3

Contents

Change History 3
Document Controls 4
1. Introduction 4
2. The SMKI Recovery Procedure 5
3. Requirements of the SMKI Recovery Key Guidance 7
4. Advance Information Required by the SMKI PMA 8
5. Decision Making Factors 9
6. Approach to Decision Making 12

APPENDIX 1 - Template of Factors that the SMKI PMA 'MUST' and 'MAY' take into account 18

Change History

VERSION	STATUS	ISSUE DATE	AUTHOR	COMMENTS
0.1	Draft	08/09/2015	SECAS	Draft for consultation with Parties
0.2	Draft	10/11/2015	SECAS	Updated in line with consultation feedback for Panel approval
0.3	Draft	10/05/2016	SMKI PMA	Post consultation submitted to SMKI PMA for approval
0.4	Draft	14/06/2016	SMKI PMA	Re-drafted Guidance document approved for consultation.
0.5	Draft	12/07/2016	SMKI PMA	Amended post re-consultation
0.6	Final Draft	13/09/2016	SMKI PMA	Comments received on final draft from SMKI PMA
1.0	Final	30/09/2016	SECAS	Final for Publication
1.01	Draft	05/04/17	SECAS	Amendments following SMKI Recovery Exercise
1.02	Draft	12/07/17	SECAS	Amendments following SMKI PMA comments
1.1	Final	18/10/17	SECAS	Amendments following consultation
1.12	Draft	16/02/21	SECAS	Amendments following SMKI Recovery Exercise
1.2	Final	16/02/21	SECAS	SMKI PMA approved for publication

1.21	Draft	13/08/2021	SECAS	Further use of the SMKI Recovery Private Key
1.3	Final	08/09/2021	SECAS	SMKI PMA approved for publication

Document Controls

REVIEWER	ROLE	RESPONSIBILITY	DATE
SMKI PMA	Document Approver	Owner of the SMKI Recovery Key Guidance Document	19/09/2017

1. Introduction

1.1 This document is the Smart Meter Key Infrastructure (SMKI) Recovery Key Guidance, published by the SMKI Policy Management Authority (PMA), in accordance with Section L10.13(d) of the Smart Energy Code (SEC).

1.2 Section L10.10(a) of the SEC requires the SMKI PMA to act in accordance with the SMKI Recovery Key Guidance in making any decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key), for the purposes of this document a "**Decision**".

1.3 The need for any Decision to be made arises only as a consequence of the application of the SMKI Recovery Procedure.

1.4 In addition to this published SMKI Recovery Key Guidance, the SMKI PMA may also maintain a more detailed working document that may contain current information that will be updated and maintained by the SMKI PMA. Such a working document may, for example, refer to relevant information defined by the SMKI PMA such as: relevant risk assessments; Business Impact Levels (BILs); process diagrams; and lessons learned from actual recovery scenarios.

1.5 The SMKI PMA has committed to undertake periodic exercises, at least annually, to test the effectiveness of the SMKI Recovery Key Guidance against a range of Use cases that reflect all the likely SMKI Recovery scenarios that may arise.

2. The SMKI Recovery Procedure

2.1 The SMKI Recovery Procedure is a document that comprises Appendix L of the SEC. In accordance with Section L10.2 of the SEC, the SMKI Recovery Procedure is a document that:

(a) "shall make provision for the use of the Recovery Private Key and Contingency Private Key (including the use of the Contingency Symmetric Key) only where such use has been required in accordance with a decision of the SMKI PMA;

(b) shall make provision for the DCC, if it has reason to believe that the use of the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) is likely to be required by the SMKI PMA, to take or instruct any Party, any SMKI PMA Member or any Panel Member to take such preparatory steps in respect of that use as it considers appropriate; and

(c) may make provision:

(i) that, in specified circumstances, certain requirements of the SMKI Recovery Procedure, or of decisions made under and in accordance with the provisions of the SMKI Recovery Procedure, may take precedence over the other provisions of the Code;

(ii) for the operation of procedures which, in specified circumstances, require that decisions over whether or not to take certain steps are referred to the SMKI PMA for its determination;

(iii) for the SMKI PMA to require any Party to nominate individuals for the purpose of performing specified tasks."

2.2 Section L10.3 of the SEC requires the DCC to notify, as soon as is reasonably practicable, the SMKI PMA of any steps that it has taken when following any of the procedures specified in the SMKI Recovery Procedure, and to provide such additional supporting information as the SMKI PMA reasonably requests.

2.3 Furthermore, the procedures within the SMKI Recovery Procedure require the DCC to seek the SMKI PMA's approval prior to any use of the Recovery Private Key or the Contingency Private Key (including the Contingency Symmetric Key), i.e. prior to the making of any Decision.

2.4 For each Organisation Certificate that may be affected by a Compromise or suspected Compromise, the SMKI Recovery Procedure requires User Parties to provide the DCC with an Organisation Compromise Notification File as set out in SEC Appendix L, Annex B.

2.5 The Organisation Compromise Notification File must include 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. DCC Users therefore need to ensure that their User System and any back-up system has the capability to produce such reports in the event of a Compromise or suspected Compromise. It will not be possible to recover Devices if this information cannot be provided.

3. Requirements of the SMKI Recovery Key Guidance

3.1 Section L10.9 of the SEC sets out the requirements of the SMKI Recovery Key Guidance and is reproduced below for reference purposes:

"L10.9 For the purposes of this Section L10, the "**SMKI Recovery Key Guidance**" shall be a document of that name which makes such provision as is appropriate, in relation to any incident in which a Relevant Private Key is (or is suspected of being) Compromised, for any one or more of the following:

(a) any factors which shall be taken into account by the SMKI PMA in deciding whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key);

(b) any other factors which may in particular be taken into account by the SMKI PMA for the purposes of that decision;

(c) any weighting or order of priority which shall, or may, be given by the SMKI PMA to any of the factors referred to in paragraphs (a) and (b); and

(d) any criteria that are to be applied by the SMKI PMA, any approach that is to be followed by it, or any steps that are to be taken by it, prior to making a decision whether or not to require the use of the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key)."

4. Advance Information Required by the SMKI PMA

Introduction

4.1 This section sets out the information that the SMKI PMA has required in advance of making any Decision.

SEC Provisions

4.2 Section L10.10(b) of the SEC states that:

"the SMKI PMA may request such information and assistance from the DCC, the Security Sub-Committee or any Party as it reasonably considers appropriate for the purposes of making any such decision or ensuring that it will be prepared to make any such decision that may fall to be made by it at a future date."

Information Required

4.3 In accordance with L10.10(b), the SMKI PMA has required the DCC to provide estimates of the total cost of Method 2 and 3 recoveries that would be borne by the DCC and which it would consequently seek to recover through Regulated Revenue (as defined in the DCC Licence) in either of the scenarios below as a consequence of carrying out recovery using either:

(i) the Recovery Private Key; or

(ii) the Contingency Private Key (including the Contingency Symmetric Key).

4.4 The SMKI PMA may request additional information depending on the prevailing circumstances when use of the SMKI Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) is requested. In particular, the SMKI PMA will wish to have been provided with details of any prepayment consumers who may be adversely affected by a SMKI PMA decision and any measures in place to protect them.

4.5 In accordance with L10.10(b), the Security Sub-Committee (SSC) has agreed that reports of Major Security Incidents and Vulnerabilities related to SMKI that Users and the DCC are required to report to the SSC, may also be promptly made available to the SMKI PMA. A secure Egress webform has been designed to capture all the information required for reports of Major Security Incidents, Vulnerabilities and SMKI Compromises or suspected Compromises to be reported using a single report form for SSC and for SMKI PMA purposes.

5. Decision Making Factors

Introduction

5.1 This section sets out the factors that the SMKI PMA **must** and **may** take into account when making a Decision and the weighting that the SMKI PMA shall give to those factors.

5.2 It also sets out the criteria that are to be applied by the SMKI PMA, the approach that is to be followed by it and the steps that are to be taken by it, prior to making a Decision.

Uncertainty of Information

5.3 It is recognised that some or all of the information made available to the SMKI PMA may not have been verified or validated and a Decision may need to be made based on the information available at the time. It is also possible that the circumstances of any particular Compromise might require a Decision to be taken in relatively short timescales. In exceptional circumstances, it may be the case that little or no verified or validated information pertaining to one or more of the factors that the SMKI PMA is to take into account in making the Decision is available. The absence of any such information should not, in itself, prevent the SMKI PMA making a Decision in relation to any particular Compromise.

5.4 In other cases, the SMKI PMA may rely on information provided by risk assessments that may be made available to it by affected parties or which it carries out itself or which are carried out on its behalf by third parties. An example would be when assessing the possible detrimental consequences associated with using either the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key), or the impact that a decision to use or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) may have on public confidence in smart metering.

5.5 In general, the SMKI PMA will seek to wait to make any Decision where waiting is likely to allow it to be provided with more complete and accurate information which may form the basis of its Decision. However, where circumstances dictate, for example in situations where a Compromise has occurred and it is considered that the adverse impact of the Compromise will increase over time or in situations where waiting is unlikely to result in materially more comprehensive information, the SMKI PMA will seek to make a Decision as soon as it is practicable for them to do so.

Factors that the SMKI PMA **MUST** Take into Account

5.6 The factors that the SMKI PMA **must** take into account when making a Decision are as follows:

i. The extent to which any actual or likely adverse impacts of the Compromise on energy consumers may be addressed by using the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key), including:

- maintaining the safety of any energy supply;
- maintaining the continuation of any energy supply;
- preventing unauthorised access to personal data;
- preventing loss of data;
- avoiding presentation of misinformation to any consumer;
- the nature of the compromise i.e. whether the compromise relates to the loss of key material or to a known or suspected compromise;
- the number of compromised devices;
- the security impact of the compromise;
- the number of energy consumers that the use of the key may benefit; and
- the duration of any such beneficial effect.

ii. the total costs of the replacement of Devices that would be avoided in the event that the SMKI PMA decides to instruct DCC to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key);

iii. the costs of running the recovery procedure using the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key, and whichever is relevant in the circumstances);

iv. the possible detrimental consequences of using either the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) to the extent that to do so would increase the probability of future Compromise of such keys;

v. to the extent not already implicit in the factors above, the impact that a decision to use or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) may have on public confidence in smart metering;

vi. the extent to which any impact of the Compromise on SEC Parties not already accounted for in the factors above might be mitigated by a decision to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key); and

vii. the extent to which any adverse consequences of the Compromise might be mitigated by means other than the use of the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) and the costs associated with carrying out such other means.

Factors that the SMKI PMA MAY Take into Account

5.7 The factors that the SMKI PMA **may** take into account when making any particular Decision are as follows:

i. the views of the Secretary of State, the Authority, SEC Parties, the Security Sub-Committee (SSC), the DCC, any other person or body that the SMKI PMA considers should be taken into account; and

ii. any other factors that the SMKI PMA decides are relevant in the circumstances which may include:

- remediation timescales if use of the SMKI Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) is used;
- remediation timescales if recovery is not authorised e.g. the time to physically replace affected devices; the availability of replacement devices; the availability of installation resources et cetera;
- the number of any pre-payment meters affected and any provision being made to protect prepayment consumers;
- the need to use the SMKI Recovery Private Key to replace Device Security Credentials in circumstances where is not possible to rectify incorrectly populated data comprising Device Security Credentials using the Private Key(s) associated with the Public Key(s) contained in the Organisation Certificate(s) from which the incorrectly populated data originated;
- the opportunity to test the effectiveness of the processes for using of the SMKI Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key).

Weighting of the Factors

5.8 It is recognised that the prevailing circumstances of a recovery scenario will be different over time and the SMKI PMA needs to have the flexibility to weight factors based on the situation that exists when a Decision is required. However, as a general rule where a weighting is applied, the SMKI PMA will apply a weighting to any factors that affect the consumer beyond factors that affect an individual Party or Parties.

5.9 Where the SMKI PMA decides that in the circumstances of a particular Compromise a weighting should be attributed to the factors that the SMKI PMA must or may take into account, then that weighting shall be attributed to the factors. Otherwise, no weighting shall apply, and the SMKI PMA shall balance the factors equally in making any decision to use or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key).

Criteria to be Applied

5.10 Section L10.9(d) allows the SMKI PMA to apply specific criteria if considered appropriate. Where the SMKI PMA decides that in the circumstances of a particular Compromise, specific criteria should be applied prior to making any Decision then those criteria shall be applied. Otherwise, no such criteria shall be applied.

Approach to be Followed and Steps to be Taken

5.11 Similarly, where the SMKI PMA decides that in the circumstances of a particular Compromise, a particular approach should be followed and/or particular steps should be taken prior to making a Decision then that approach shall be followed and those steps shall be taken. Otherwise, the approach set out in Section 6 of this document shall be followed.

6. Approach to Decision Making

Introduction

6.1 This section sets out the approach that the SMKI PMA will follow when making a Decision.

Notification of the need for a Decision

6.2 In addition to the notifications referred to in paragraph 2.2 above, the SMKI Recovery Procedure requires the DCC to notify the SMKI PMA by secure electronic means prior to any use of the Recovery Private Key or the Contingency Private Key (including the Contingency Symmetric Key) as follows:

i. in relation to the Recovery Private Key, in accordance with steps 4.2.1.3, 4.3.1.3, 6.1.1.1, 6.2.1.1 or 6.3.1.1 of the SMKI Recovery Procedure; or

ii. in relation to the Contingency Private Key (including the Contingency Symmetric Key) in accordance with step 5.1.1 of the SMKI Recovery Procedure.

6.3 As explained in paragraph 4.5, SECAS may also receive a notification on behalf of the SSC directly from the affected Party using the Major Security Incident and Vulnerability Reporting Form provided on the SEC website. The SSC has agreed that details of incidents that relate to SMKI Compromise shall be promptly made available by SECAS to the SMKI PMA. The SEC Section G 3.5 requires:

"G3.5 Each User shall, on the occurrence of a Major Security Incident in relation to its User Systems, promptly notify the Panel and the Security Sub-Committee".

6.4 The DCC must await a Decision by the SMKI PMA before initiating the use of the Recovery Private Key or the Contingency Private Key (including the Contingency Symmetric Key). However, the DCC should start to make sensible preparations such as alerting the relevant DCC staff and by checking the availability of Key Custodians.

Steps to be followed in making a Decision Step

Step 1 - SMKI PMA Convenes a Meeting

6.5 Following the receipt of a notification from DCC in accordance with the SMKI Recovery Procedure (SEC Appendix L) in one of the circumstances identified in Section 2 above, SECAS will inform the SMKI PMA Chair (or Alternate) by telephone and by making the relevant information available by secure electronic means. If a Decision is required, the SMKI PMA Chair (or Alternate) shall convene a meeting of the SMKI PMA. This meeting may be by teleconference or in person as may be determined by the SMKI PMA Chair (or Alternate).

6.6 The meeting will be convened on the same day or as soon as is reasonably practicable after the receipt of the notification from the DCC, taking into account the need for SECAS to establish a quorum of the SMKI PMA to participate in the meeting.

6.7 Individuals who are likely to be able to provide information to the SMKI PMA on the nature and likely effects of the Compromise or the steps that have already been taken to attempt to deal with the Compromise will normally be invited to attend this SMKI PMA meeting. This will include staff of the DCC who are managing the Major Security Incident and staff of the organisation whose Certificate has been Compromised (if different).

6.8 Where a Shared Resource Provider is being used, consideration will be given to SEC Section G5.25 to assess the potential adverse effect of any Compromise to the User Systems of the customers of the

Shared Resource Provider which may be greater than it would have been had a User not employed a Shared Resource Provider. Staff from both the User organisation(s) and the Shared Resource Provider organisation will be invited to the meeting.

Step 2 - SMKI PMA establishes the facts

6.9 At the SMKI PMA meeting that has been convened pursuant to Step 1, the SMKI PMA shall seek to understand the relevant facts associated with the Compromise including:

i. which Private Keys and which OCA and/or Organisation Certificates are affected;
ii. what is known about the cause of the Compromise;
iii. what impact there may be for consumers and, in particular for prepayment consumers;
iv. whether the SMKI Organisation Certificate associated with the Compromise has been revoked at this stage and, if not, when revocation is planned to take place;
v. whether Method 1 has been tried and if so, what prevented this from successfully replacing the affected Certificates and if not, why Method 1 is considered not to be appropriate;
vi. what effects are being manifested in relation to the Compromise, for example what efforts to recover from the Compromise using other means have been tried and what success has there been in doing this, are any adverse effects being experienced by consumers;
vii. whether there is a need to act quickly in order to maximise the extent to which using the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) is likely to mitigate any adverse impact of the Compromise;
viii. what information is known (and with what level of confidence) about each of the factors that the SMKI PMA must take into account in making the Decision; and
ix. any other relevant matters.

Step 3 – SMKI PMA Confirms the Decision Making Process

6.10 Following Step 2, the SMKI PMA shall consider whether the circumstances of the Compromise are such that:

i. the SMKI PMA should take into account any of the factors set out in Section 5 and, if so, which of those factors should be included and, what information is known (and with what level of confidence) about those additional factors;
ii. any particular weighting should be applied to the factors that are to be taken into account and if so, what that weighting is;

iii. any criteria should be applied prior to taking any decision to use or not to use the Recovery Private Key or Contingency Private key (including the Contingency Symmetric Key), and if so, what those criteria are; and

iv. any particular approach that should be followed and/or particular steps should be taken prior to making a Decision.

Step 4 – SMKI PMA Determines whether or not to make a Decision

6.11 Where, under Step 3 above, the SMKI PMA has decided to follow a particular approach and/or particular steps when making a Decision, then it shall follow that approach and/or take those steps. Otherwise the PMA shall determine whether:

i. it is appropriate for the SMKI PMA to make a Decision; or

ii. it is appropriate for the SMKI PMA to seek additional information prior to making a Decision.

6.12 Where the SMKI PMA decides that it is appropriate for it to make a Decision, it shall proceed to Step 5 of this procedure.

6.13 Where the SMKI PMA decides to seek additional information, it shall take the necessary steps to establish such information and convene a future meeting in timescales in which it may reasonably expect to obtain the relevant information, including where appropriate by relying upon the provisions of L10.10(b) of the SEC.

6.14 If new information becomes available prior to the date upon which the subsequent meeting has been set, the SMKI PMA Chair (or Alternate) may convene the subsequent meeting earlier than the date set under 6.12 above.

6.15 At the subsequent SMKI PMA Meeting, the SMKI PMA shall resume the decision making process from Step 2.

Step 5 – SMKI PMA Makes a Decision

6.16 Where under Step 4, the SMKI PMA has determined that it is appropriate for it to make a Decision, the SMKI PMA shall:

i. consider any criteria that it has decided should be applied pursuant to paragraph 6.9 above;

ii. discuss and consider the factors that are to be taken into account in making the Decision seeking to balance the factors in the round, or weighted in accordance with any weighting that the SMKI PMA has decided should be applied (and in either event taking into account the reliability of the information available in relation to each factor). The Table in Appendix 1 of this document may be completed by the SMKI PMA in carrying out this exercise and the

contents of any more detailed and current working documents as defined by the SMKI PMA may be taken into account e.g. relevant risk assessments, current Business Impact Levels and recent lessons learned;

iii. communicate the Decision made by the SMKI PMA to the DCC and other persons as considered appropriate by the SMKI PMA;

iv. give special consideration to prioritise consumers who have particular requirements such as priority service customers and those with Pre-Payment Meters. Users should note that more than one CSV file can be submitted at the same time which can enable the prioritisation of certain Meters ahead of others;

v. request that the User notifies the DCC of the impact of replacing any unrecovered Devices following recovery when completing the report required in SEC Appendix L, Clause 4.1.2.4 e.g. explaining the cost, any geographical impact, any PPM impact etc.;

vi. request that the DCC notifies the SMKI PMA of any repeated recovery failures to enable the SMKI PMA to consider the cost of ongoing recovery attempts versus the impact of replacing any unrecovered Devices following recovery when completing the report required in SEC Appendix L, Clause 4.1.3.2 4 e.g. explaining the cost, any geographical impact, any PPM impact etc.

Step 6 – Post Decision Making Review

6.17 Following the making of any Decision in accordance with this SMKI Recovery Key Guidance, the SMKI PMA shall, in timescales that it determines, undertake a review of:

i the circumstances that led to the Compromise and what steps might be taken to reduce the probability of any similar Compromise in the future;

ii the reports from the DCC provided under SEC Appendix L, Clauses 4.1.3.2; 4.2.3.2; 4.3.3.2; 5.3.4; and 6.1.3.3; and

iii the effectiveness of the application of the SMKI Recovery Key Guidance.

6.18 Following the review referred to in paragraph 6.16 above, the SMKI PMA shall, to the extent that it determines that it is appropriate to do so:

i communicate the lessons learned from the review to relevant persons; and

ii propose amendments to the SMKI Recovery Key Guidance in accordance with paragraph L10.13(c) of the SEC;

iii consider whether an assessment of any SMKI Participant involved in the Compromise should be undertaken by the Independent SMKI Assurance Service Provider under SEC

Appendix C (SMKI Compliance Policy) Clause 3.2 (c) and (d) and for the SMKI PMA to consider the subsequent report;

iv consider the estimated costs associated with replacing Devices that could not be recovered and whether any actions are required to reduce the number of unrecovered Devices in the future.

APPENDIX 1 - Template of Factors that the SMKI PMA 'MUST' and 'MAY' take into account

Private Key Compromised			
Which of Recovery or Contingency Private Key (including the Contingency Symmetric Key) is being considered for use?			
	Factors	**Evidence Provided**	**SMKI PMA Assessment**
Factors that MUST be taken into account			
5.6 i	The extent to which any actual or likely adverse impacts of the Compromise on energy consumers may be addressed by using the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key), including: • maintaining the safety of any energy supply; • maintaining the continuation of any energy supply; • preventing unauthorised access to personal data; • preventing loss of data; • avoiding presentation of misinformation to any consumer; • the nature of the compromise i.e. whether the compromise relates to the loss of key material or to a known or suspected compromise; • the number of compromised devices; • the security impact of the compromise; • the number of energy consumers that the use of the key may benefit; and • the duration of any such beneficial effect.		

Private Key Compromised			
Which of Recovery or Contingency Private Key (including the Contingency Symmetric Key) is being considered for use?			
Factors		**Evidence Provided**	**SMKI PMA Assessment**
Factors that MUST be taken into account			
5.6 ii	the total costs of the replacement of Devices that would be avoided in the event that the SMKI PMA decides to instruct DCC to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key).		
5.6 iii	the costs of running the recovery procedure using the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key, and whichever is relevant in the circumstances).		
5.6 iv	the possible detrimental consequences of using either the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key), and to the extent that to do so would increase the probability of future Compromise of such keys.		
5.6 v	to the extent not already implicit in factor a. above, the impact that a decision to use or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) may have on public confidence in smart metering.		

Private Key Compromised			
Which of Recovery or Contingency Private Key (including the Contingency Symmetric Key) is being considered for use?			
Factors		**Evidence Provided**	**SMKI PMA Assessment**
Factors that MUST be taken into account			
5.6 vi	the extent to which any impact of the Compromise on SEC Parties not already accounted for in the factors above might be addressed by a decision to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key).		
5.6 vii	the extent to which any adverse consequences of the Compromise might be addressed by means other than the use of the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) and the costs associated with carrying out such other means.		
Factors		**Evidence Provided**	**SMKI PMA Assessment**
Factors that MAY be taken into account			
5.7 i	the views of the Secretary of State, the Authority, SEC Parties, the Security Sub-Committee (SSC), the DCC, any other person or body that the SMKI PMA considers should be taken into account;		

Private Key Compromised			
Which of Recovery or Contingency Private Key (including the Contingency Symmetric Key) is being considered for use?			
Factors		**Evidence Provided**	**SMKI PMA Assessment**
Factors that MUST be taken into account			
5.7 ii	any other factors that the SMKI PMA decides are relevant in the circumstances which may include: – remediation timescales if use of the SMKI Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) is used; – remediation timescales if recovery is not authorised e.g. the time to physically replace affected devices; the availability of replacement devices; the availability of installation resources, etc.; – the number of any pre-payment meters affected;		
5.7 iii	the need to use the SMKI Recovery Private Key to replace Device Security Credentials in circumstances where is not possible to rectify incorrectly populated data comprising Device Security Credentials using the Private Key(s) associated with the Public Key(s) contained in the Organisation Certificate(s) from which the incorrectly populated data originated; and		

Private Key Compromised			
Which of Recovery or Contingency Private Key (including the Contingency Symmetric Key) is being considered for use?			
Factors		**Evidence Provided**	**SMKI PMA Assessment**
Factors that MUST be taken into account			
5.7 iv	the opportunity to test the effectiveness of the processes for using of the SMKI Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key).		