Meeting SECPMA_22_1204, 12th April 2016

11:30 – 15:00

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ

SMKI PMA Minutes

Attendees:

Category	SMKI PMA Members
SMKI PMA Chair	Gordon Hextall
Large Supplier	Geoff Huckerby
Networks	Sara Neal
Small Supplier	Rob Kinson
Technical Sub-Committee (TSC) Representative	Julian Hughes (Part)

Non-Voting Members:

Category	Attendees
DCC	Marc Avery
Ofgem (the Authority)	Nigel Nash
DECC (Representative)	Joe Howard (Part)
SECAS	James Simmonds
SMKI PMA Secretary	Joe Davenport

Apologies:

Category	Attendees
Large Supplier	Fabien Cavenne
Security Sub-Committee (SSC) Representative	Michael Constable

1. Minutes of SMKI PMA Meeting 21_0803

SECAS informed SMKI PMA that in respect of the outstanding actions recorded within Appendix B of the Draft Minutes from the March 2016 (Appendix B – SMKI PMA and TAG Briefing Note), an update would be provided at the next meeting (10th May 2016).

SECAS noted a format amendment would be made, and that no further suggested changes were raised by SMKI PMA Members. The SMKI PMA agreed the minutes as written.

2. Actions Outstanding

SECPMA 21/01 – SMKI PMA Members provided comments on the SMKI Recovery - Procedures Document, and which had been incorporated within the SMKI Recovery Key Guidance (Agenda item 3 of the April 2016 SMKI PMA meeting).

This action was marked as **CLOSED**.

SECPMA 21/02 – SECAS informed the SMKI PMA that they were still investigating the methods for monitoring and reviewing SMKI documentation, and the types of trigger points that may result in the group reviewing a SMKI document.

This action was marked as **ONGOING** and an update will be provided at future SMKI PMA meetings.

3. SMKI Recovery Key Guidance Document

SECAS presented the group with the amended draft SMKI Recovery Key Guidance, and a number of further considerations for the group to review. SMKI PMA Members provided the following points, which are outlined below, and were asked to provide further comment(s) (if any) to SECAS within 10 Working Days (26th April 2016):

- **3.1 - Additional Person(s) to be consulted and included:** The SMKI PMA were requested to consider and identify additional person(s) that may need to be consulted and included within the consultation of the draft SMKI Recovery Key Guidance. The SMKI PMA agreed to consider this point, and provide a response to SECAS within 10 Working Days.
- **3.2 - Risk Evaluation:** The SMKI PMA were requested to consider whether to adopt the same metrics and methods used in the Industry Security Risk Assessment when evaluating risk in relation to whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). Members questioned the role separation between Security Sub-Committee (SSC) and SMKI PMA, and the ways in which in risk(s) would be assessed and recorded by both the SSC and the SMKI PMA. The SMKI PMA agreed that, as the SSC are notified of a Recovery Event as part of the Major Security Incident process, the roles and responsibilities were separate between the SSC and the SMKI PMA. The SMKI PMA were reminded that their role within the Recovery Event was to consider whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key) only. The group agreed that any decision(s) would be based on the material being provided to the SMKI PMA, rather than the group having to follow-up and request information themselves following notification. SMKI PMA considered it appropriate that, in the event of a Compromise (or suspected Compromise) being notified to the DCC, that the DCC, the SSC (in its role as DCC Service Provider), and any other SEC Party begin gathering information following said notification, in order to assist the process and the SMKI PMA making a decision. The group also identified the possibility that situations may arise where the SSC and/or the SMKI PMA were notified of a Compromise (or suspected Compromise) informally prior to the DCC being notified, through the SEC Parties that hold a position within the SSC and/or the SMKI PMA. The SMKI PMA

considered and agreed that it would be sensible to approach DECC, in order to understand the metrics and methodology used as part of the Industry Security Risk Assessment, and to then subsequently consider whether to adopt said metrics and methodology when considering whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key).

- **3.3 - SMKI PMA Risk Assessment and Timescales:** The SMKI PMA were requested to consider the associated timescales, and risk assessment process, in relation to the SMKI PMA convening on whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). SECAS presented the Incident Categories which were based upon the DCC's Incident Management Policy in order to provide a level of continuity. The SMKI PMA agreed that the final decision on whether or not the SMKI PMA should convene would lie with the SMKI PMA Chair, and SECAS agreed to review and provided an updated Members Pack to the SMKI PMA. The SMKI PMA Chair noted that voting members of the SMKI PMA should revise and nominate an Alternate, in order for a quorum to be present in the Recovery Event decision making process. The SMKI PMA considered timescales, and the possible time required in order for the DCC, the SSC and any SEC Party (or SEC Parties) that would be required to provide information to the group to make an informed decision on whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). The SMKI PMA identified that Suppliers may only notify a selection of Devices (e.g. Pre-Payment Devices) that are Compromised (or suspected of being Compromised), rather than their entire portfolio of Devices that have been Compromised (or suspected of being Compromised) (e.g. Pre-Payment and Credit Devices), and agreed that the DCC may wish to consider whether they accept the Devices they Supplier(s) wish to Recover, or the possible entire portfolio of Devices that are Compromised (or suspected of being Compromised). The SMKI PMA agreed that guidance and supporting documentation should be investigated, in order to state the information that would be considered by the SMKI PMA on deciding whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key)[1].
- **3.4 - Notification following a SMKI PMA Decision:** The SMKI PMA were requested to consider and identify additional person(s) that should be notified following the group making a decision on deciding whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). The SMKI PMA agreed to consider this point, and provide a response to SECAS within 10 Working Days.
- **3.5 - Co-ordination of the SMKI PMA with other Response Processes:** The SMKI PMA were requested to consider and identify any additional response processes that would need to be incorporate both before, and after, a decision by the SMKI PMA in relation to a decision being made on whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). The SMKI PMA agreed to consider this point, and provide a response to SECAS within 10 Working Days.
- **3.6 - Business Impact Level Rating Consideration:** The SMKI PMA were requested to consider whether the Business Impact Level (BIL) rating methodology should be adopted when considering whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). DECC enquired as to whether there was a way of simplifying the *Key Decision Factors* in the draft SMKI Recovery Key Guidance, and

[1] Further information in the ways information is collected and provided to the SMKI PMA is found in section 3.7 of these Minutes.

the SMKI PMA identified a number of risks within the *Key Decision Factors* that could be merged and/or replaced. The SMKI PMA agreed to provide a response to SECAS within 10 Working Days. The group requested that the DCC provide the latest cost(s) associated with the Recovery Event, specifically in using the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key to the SMKI PMA to assist in the decision making process.

- **3.7 - The ways in which information is provided to the SMKI PMA:** The SMKI PMA were requested to consider the benefit(s) of making the *Key Decision Factors* table of the SMKI Recovery Key Guidance a public-facing pro-forma, which could then be used by the DCC, the SSC and a SEC Party (or SEC Parties) to collate and submit information to the SMKI PMA when it considers whether or not to use the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key). The DCC noted that if the SMKI PMA considered adopting a pro-forma, that the SMKI PMA (via the DCC or SECAS) receive the completed pro-forma via an Authorised SMKI Senior Responsible Officer (SMKI SRO). The SMKI PMA agreed that a secure platform may need to be considered for completed pro-forma to be submitted to the SMKI PMA.
- **3.8 - DCC Obligation - Report Publication:** The SMKI PMA were requested to consider whether the report produced by the DCC[2] should be taken to the next available SMKI PMA meeting as a Confidential agenda item, or whether the SMKI PMA should hold an ex-committee meeting following the DCC providing said report. The SMKI PMA agreed that, unless indicated by the DCC as a matter of urgency, the report should be submitted by the DCC to the next available SMKI PMA meeting. The SMKI PMA noted that this report would provide information known to the DCC at the time, and that additional analysis and assessment may be required. SECAS noted the SMKI PMA's ability to direct the DCC to assess SMKI Participant's for compliance against the SMKI Document Set, if this was deemed appropriate. The DCC agreed to investigate whether the contract in place between the DCC and the Independent SMKI Assurance Service Provider would allow for ad-hoc assessments of compliance against SMKI Participants.

ACTION SECPMA 22/01: SMKI PMA to provide comment(s) (if any) to SECAS within 10 Working Days (26th April 2016).

ACTION SECPMA 22/02: The DCC will investigate the construction of Scenarios for Recovery and the development of checklists for what information should be provided to the DCC/SMKI PMA and other involved Parties.

ACTION SECPMA 22/03: SECAS will continue to assess the BIL factors within the Key Factors table and which are relevant and which can possibly be merged or removed.

ACTION SECPMA 22/04: The DCC/CGI will establish an initial scope and cost of recovery and the variances dependent on the level of recovery required.

ACTION SECPMA 22/05: The DCC will examine the possibility of enforcing suppliers to commission reports or compliance assessments against the SMKI Document Set in order to mitigate possible risks.

ACTION SECPMA 22/06: The DCC will investigate 'Operation Categories' for the remedy of implementation in order to establish a reporting structure and determine who needs to conduct reports.

[2] In accordance with their obligations set out in Section 3.1 of the SMKI Recovery Procedure (DCC Obligations)

ACTION SECPMA 22/07: SMKI PMA Members advised to attend the DCC Recovery Procedure Workshop where possible and provide feedback on the SMKI Recovery Key Guidance material.

4. Responsible Officer Guidance

SECAS presented the SMKI PMA with the draft Responsible Officer Guidance, which set out the roles and responsibilities of the a SMKI SRO, and a SMKI Authorised Responsible Officer (SMKI ARO), and provides guidance in relation to what a SEC Party, the DCC (in its role as DCC Service Provider) or an RDP may wish to consider when nominating SMKI SROs and SMKI AROs. The SMKI PMA held initial discussions, with the DCC identifying expanding the SMKI ARO role to include the signing of Anomaly Detection Threshold files, as set out within the Threshold Anomaly Detection Procedures (TADP).

ACTION SECPMA 22/08: The SMKI PMA agreed to provide comments to SECAS within 10 Working Days, which will be compiled and assessed before being applied to the document.

5. Amendments to the SMKI RAPP and SMKI Interface Design Specification

This agenda item was deferred for discussion at a future SMKI PMA meeting.

6. SMKI PMA Activity Planner

SECAS provided the SMKI PMA with an updated activity planner outlining the activities expected over the next three months (April 2016 – June 2016). It was noted that at a future SMKI PMA meeting, the DCC would be required to provide an update on the process in which the initial Key Custodians who took part in the initial Key Ceremony held 24th February 2016 would transfer their Key Shares to new Key Custodians (on the basis that they did not wish to remain Key Custodians following this initial Key Ceremony).

A SMKI PMA Member enquired as to whether the DCC were required to hold a second Key Ceremony, following a recent firmware update to the Hardware Security Module (HSM) used by the DCC. The DCC noted an internal review was ongoing, and that the DCC would provide an update at future SMKI PMA meeting.

SECAS informed the SMKI PMA that following the April 2016 meeting, the nomination (and voting process if require) for the Small Supplier seat and one Large Supplier seat would commence.

ACTION SECPMA 22/09: The DCC will examine and assess the necessary steps, for those Key Custodians who had initially expressed a 'temporary position' for the Key Ceremony with the intention to transfer responsibility to an enduring participant.

ACTION SECPMA 22/10: The DCC will check to confirm the latest upgrade to BT's HSM breaks compliance and whether a reconvening of the Key Custodians will be required as a result of this.

7. Modifications Update

SECAS presented the group with the standing agenda item, the Modifications Update Report. SECAS noted that one new Modification had been raised since the March 2016 SMKI PMA meeting, and that the initial review of the Modification had no direct impact to the SMKI PMA, nor the SMKI Services. SECAS noted that, during the Refinement Stage of the Modification Process, if a Working Group identified a possible impact to the SMKI PMA, or the SMKI Services, the group would be informed by SECAS. SMKI PMA Members noted their interest in a number of Modifications currently in the

Refinement Stage, and requested that SECAS investigate if the Working Group(s) assigned to these Modifications consider whether there is an impact to the SMKI PMA, or the SMKI Services.

ACTION SECPMA 22/11: SECAS will consult with the modifications team on possible implications of any current, and recently submitted, modifications may have on SMKI.

8. DCC Update

The DCC advised the group that at the next SMKI PMA meeting, and thereafter, the DCC would provide a monthly update on any changes to the DCC's Registration Authority Personnel.

The DCC informed the group of their intention to submit the Stage 1 Assurance Report at the May 2016 SMKI PMA meeting.

9. DCCKI PMA Functions Update

The DCC informed the SMKI PMA that the second DCCKI PMA Functions meeting had not yet occurred. An update shall be provided at the May 2016 SMKI PMA meeting.

10. DECC Update

The SMKI PMA **NOTED** that there was no additional information to be updated from DECC for April 2016.

11. Any Other Business

The SMKI PMA were informed by SECAS of an open consultation on the SMKI Recovery Procedure document, and of a DCC workshop on 20th April 2016 to explain the detail of the proposed changes within this consultation. SMKI PMA Members were provided details on the key changes, and were asked to consider whether a formal response by the SMKI PMA was required. SECAS identified that SMKI PMA Members should provide comment(s) following the DCC workshop on 20th April 2016, whereby SECAS shall compile a draft response for the SMKI PMA Chair to consider. If the SMKI PMA Chair agreed the consultation warranted a response, SECAS would circulate the draft response from the SMKI PMA on the SMKI Recovery Procedure consultation to SMKI PMA Members, taking into account any comments prior to its submission to the DCC on 29th April 2016.

The group were also reminded of their opportunity to nominate Alternates when SMKI PMA Members were unable to attend meetings, and SECAS agreed to circulate the Alternates nomination form to SMKI PMA Members. SECAS advised that the SSC and TSC representatives could be re-assessed for a 12 or 24month basis moving forwards, depending on the decision of the group.

ACTION SECPMA 22/12: SMKI PMA Members will have 10 days after the DCC Recovery Workshop on 20th April to provide comment on the current consultation on SMKI Recovery procedure. SECAS will compile these responses and provide them to the DCC.

ACTION SECPMA 22/13: As per the related SEC Clauses, SECAS will send out nominations forms for the election of alternatives for voting Members.

12. Next Meeting

The next meeting will be held on **10th May 2016**.