SMKI PMA Meeting 64

10:00 – 14:15, 17 December 2019

Gemserv Office, 8 Fenchurch Place, London, EC3M 4AJ

SECPMA_64_1712 – Final Minutes

Attendees:

Representing	SMKI PMA Attendees
SMKI PMA Chair	Gordon Hextall (GH)
BEIS	Russell Kent-Smith (RKS)
DCC	Anthony Bistacchi (AB)
	Richard Harvey (RHa)
	Scott Valentine (SV) (Part)
SECAS	Fiona Bond (FB)
	Hollie McGovern (HM) (Meeting Secretary)
	James Hosen (JHo)
	Nick Blake (NB)

Voting Members:

Category	Attendees
Technical Architecture and Business Architecture Sub-Committee (TABASC) Representative	Julian Hughes (JH)
SMKI Specialist	Darren Calam (DC)
Gas Networks	Earl Richards (ER)
Large Suppliers	Ashley Pocock (APo)

Apologies:

Category	SMKI PMA Attendees
Large Suppliers	Crispin Brocks (CB)
Electricity Networks	Paul Fitzgerald (PF)
BEIS	Daryl Flack (DF)

Matters Arising

The SMKI PMA Chair (GH) welcomed the attendees to the December 2019 meeting, noting the running order of the agenda.

Progressing enforced XML signing

The SMKI PMA Chair (GH) updated Members on proposals previously raised by the SMKI PMA for the use an XML Signing Key for SMETS2. The SMKI PMA and SSC have considered whether to require an enforced separation of the XML Signing Key for DUIS Commands from the use of a SMKI digital Signing Key for Pre-Commands. The current wording in the DCC User Interface Specification (DUIS) doesn't currently check that a separate Signing Key has been used to sign the different Commands.

The SMKI PMA Chair (GH) advised on the progress of the proposals, stating that that SSC has initiated a SEC Modification for the DCC to introduce a technical control to validate that different Signing Keys have been used. BEIS is to consult in January 2020 on an XML Signing role to be included in SEC Section L3.18.

TABASC Representative (JH) questioned if any communication will be sent out to DCC Users to inform them that the functionality is available for them to begin using the XML Signing Key, noting that the intention is for Users to begin using it as soon as it becomes available to enable a gradual migration. The SMKI PMA Chair (GH) noted that SECAS should include the communication as a policy intent in the SECAS newsletter for the awareness of Users, with further formal guidance once the consultation response has been published by BEIS. BEIS (RKS) confirmed BEIS consultation is due to begin on week commencing 6 January 2020 and the consultation response is due for 26 March 2020.

TABASC Representative (JH) also highlighted the importance of the DCC to be ready to create the new XML Signing Roles, on the assumption that BEIS approve the functionality in their consultation response.

SECPMA64/01: SECAS to issue guidance to DCC Users to advise them of the proposal to create new XML Signing Roles and issue formal guidance following publication of the BEIS consultation response, due on 26 March 2020.

SECPMA64/02: DCC to confirm that it will be ready to create new XML Signing Roles following publication of the BEIS consultation response, due on 26 March 2020.

1. Previous Meeting Minutes and Actions Outstanding

The Draft Minutes and Confidential Draft Minutes from the November 2019 SMKI PMA meeting were **APPROVED** as written.

SECAS, the SMKI PMA Chair and the DCC provided the Sub-Committee with an update on six actions outstanding from previous SMKI PMA meetings. The following table sets out key items of discussion:

Action Reference	Action	Owner
SECPMA 61/01	TABASC Representative (JH) to provide the SMKI PMA with an update on the outcome of Section 6 of the Effectiveness Review questionnaire at the October SMKI PMA meeting.	**TABASC Representative (JH)**
The outcome of the Effectiveness Review questionnaire will be provided at the next SMKI PMA meeting on Tuesday 21 January 2020. Status: **Open.**		
SECPMA 62/01	SECAS to clarify contradictory information with the NCSC regarding GPG13 and GPG43 being withdrawn but still appearing on the NCSC website.	**SECAS**
The SMKI PMA Chair (GH) advised that feedback had been received from NCSC and the subsequent actions were discussed under Agenda Item 7. Status: **CLOSED.**		
SECPMA 62/03	SMKI PMA to consider a transitional period from FIPS 140-3 to the ISO standards ISO/IEC 19790:2012 and ISO/IEC 24759:2017.	**SMKI PMA Chair (GH)**
The SMKI PMA Chair (GH) emailed NCSC to confirm it was comfortable with the approach to adopt the relevant ISO standards rather than FIPS. NCSC have responded to advise they should have an answer in due course. An update will be provided at the next meeting on Tuesday 21 January 2020. Status: **Open.**		
SECPMA 63/01	DCC to provide a timeline for confirming the Trusted Service Provider (TSP) re-procurement requirements.	**DCC**
DCC (IS) advised the intention is to extend the current TSP contract for another two years and the DCC will formally convey this to the SMKI PMA. The DCC (IS) will monitor the re-procurement to ensure the requirements are met. Status: **CLOSED.**		

<table>
<tr><th>Action Reference</th><th>Action</th><th>Owner</th></tr>
<tr><td><b>SECPMA 63/02</b></td><td>SECAS (KAA) to review the guidance on moving from NIST SP 800-56A Revision 2 to Revision 3, upon receipt from NCSC.</td><td><b>SECAS (KAA)</b></td></tr>
<tr><td colspan="3">The SMKI PMA Chair (GH) advised that an email from NCSC was received on 10 December 2019, advising it is NCSC’s view that not much has changed for the elliptic curve elements of the specification. However, GBCS may already define precisely how to derive keys, or state which one to use, as everyone will need to do it the same way. NCSC did not spot any obvious impactful changes, however, noted it is possible that some changed detail might impact some devices, but this is hard to establish without examination of the technical specifications of individual meter models. There are quite a lot of textual changes between the revisions which would take quite some time to exhaustively review, however it would appear the general technical detail remains consistent between the revisions. NCSC added that they did not assess the impact of the changes on the Zigbee crypt as this is not used to authenticate critical messages from the DCC. Status: <b>CLOSED.</b></td></tr>
<tr><td><b>SECPMA 63/03</b></td><td>DCC to confirm what actions have been taken to prevent Device Manufacturers from having access to SPOTI.</td><td><b>DCC</b></td></tr>
<tr><td colspan="3">DCC confirmed they have advised Device manufacturers that they can no longer access SPOTI. Status: <b>CLOSED.</b></td></tr>
</table>

2. SEC Amendments – Appendix L (GREEN)

Appendix L – Section 6

The SMKI PMA Chair (GH) highlighted the proposed updates to SEC Appendix L – SMKI Recovery Procedure, following a meeting held on 2 December 2019 between DCC, BT, CGI, BEIS, the SMKI Specialist (DC) and SMKI PMA Chair (GH), to discuss the ability of DCC, BT and CGI to operate the proposed changes to SEC Appendix L, Section 6.

It was noted that the main changes are for the DCC rather than Users to Recover from a Compromise of the Contingency Private Key and/or the Contingency Symmetric Key. A number of actions were taken by Service Providers BT and CGI to clarify certain processes, to update documents for SMKI PMA approval and to clarify what tests have been done/scheduled. Both Service Providers confirmed that it should be possible for them to operate Recovery should it be necessary.

SMKI PMA Members **NOTED** that, once the SEC is amended following consultation and when SMKI PMA has approved the updated DCC documentation, the DCC and its Service Providers need to conduct a ‘walkthrough’ simulation of the recovery processes to ensure they are robust and accurate.

The SMKI PMA **APPROVED** the draft of SEC Appendix L (SMKI Recovery Procedure) for BEIS consultation.

SMKI RAPP

The DCC highlighted the proposed updates to SEC Appendix D - SMKI Registration Authority Policies and Procedures (RAPP) following the tScheme audit finding that there are discrepancies between the DCC Work Instructions and the SMKI RAPP. The DCC has highlighted 12 proposed changes that are necessary to align the SMKI RAPP with the DCC's actual working practices.

The SMKI PMA:

- **APPROVED** proposed amendments to SEC Appendix D (SMKI Registration Authority Policies and Procedures); and
- **AGREED** to raise a Problem Statement to initiate a SEC Modification.

SECPMA64/03: SMKI PMA to raise a Problem Statement to initiate a SEC Modification to align SEC Appendix D - SMKI Registration Authority Policies and Procedures, to the DCC's actual working practices.

3. SMKI Operational Recovery for Users (AMBER)

As the SMKI Operational Recovery Procedure for Users document has not yet been provided, this agenda item was deferred until the next SMKI PMA meeting on 21 January 2020.

4. Replacing SMKI Organisation Certificates (RED)

A Large Supplier presented the SMKI PMA with lessons learned from an experience regarding replacing SMKI Organisation Certificates. The discussion was classified as **RED** and therefore recorded in the confidential minutes.

The SMKI PMA **NOTED** the update.

5. SMKI Root Roll-Over Testing (RED)

As the SMKI Root Roll-Over Testing Plans have not yet been provided, this agenda item was deferred until the next SMKI PMA meeting on 21 January 2020.

6. PKI for SMETS 1 FOC (RED)

The SMKI PMA considered the Public Key Infrastructure (PKI) for Final Operating Capability (FOC). The discussion was classified as **RED** and therefore recorded in the confidential minutes.

7. SMKI Standards and Guidance Review (GREEN)

The SMKI PMA Chair (GH) updated Members on the SMKI Standards and Guidance review, which had been carried out by SECAS in October 2019. Upon review it was noted that the NCSC Good Practice Guides (GPG) 13, GPG 43 and GPG 45 have been updated or discontinued since their original referencing in the SEC.

The SMKI PMA Chair (GH) advised Members that GPG 13 has been discontinued by the NCSC and provided a suggestion that SMKI PMA Members bring proposals to the next meeting to adopt an internal standard based on the good industry practice outlined in GPG 13.

GPG 43 has also been discontinued, however the NCSC website page for the guidance currently directs to a publication of nine assurance principles, titled "Government Identity Assurance Principles Privacy and Consumer Advisory Group (PCAG) V3.1 (for publication)". The SMKI PMA Chair (GH) noted that the published principles do not appear to align to smart metering processes, and a potential option may be to replace the SEC references to GPG 43 with GPG 45.

The SMKI PMA Chair (GH) noted that GPG 45 has been updated to version 4.1.1. In the new version, the Levels of identity verification outlined in the previous version have been replaced by Scores of 1 to 4 based on confidence: low confidence (Score 1); medium confidence (Score 2); high confidence (Score 3); and very high confidence (Score 4). The SMKI PMA Chair (GH) reminded Members that the SEC currently requires Level 3 identity verification from the referenced version of GPG 45, and recommended that the Members consider which Score to adopt using the new version – suggesting either Score 3 or 4.

TABASC Representative (JH) proposed that the SMKI PMA consider creating its own independent good practice guides, in order to place less reliance on the NCSC's guidance strategy and have better control over the referenced guidance. The SMKI PMA Chair (GH) advised that further consideration is required for the three guidance documents and they will discuss the different options with the SMKI Specialist (DC) to bring back to the SMKI PMA for the next meeting on 21 January 2020.

The SMKI PMA:

- **AGREED** to consider replacing SEC references to GPG 43 with GPG 45;
- **AGREED** to consider the replacement of identity assurance Level 3 with the equivalent score as stipulated in the new version of GPG 45

SECPMA64/04: SMKI PMA Chair (GH) to present options on replacing the updated/discontinued NCSC Good Practice Guides to the SMKI PMA at the next meeting on 21 January 2020.

8. SMKI PMA Quarterly Work Package Q4 2019-20

SECAS (FB) presented the SMKI Quarterly Work Package and clarified the activities and associated costs for the SECAS core team and project resource for the period of January – March 2020.

The SMKI PMA **AGREED** to recommend the work package for SECCo Board approval.

9. SMKI PMA Risk Register Review (RED)

The SMKI PMA reviewed the SMKI Risk Register and amended the risks where appropriate. The discussion was classified as **RED** and therefore recorded in the Confidential Minutes.

The SMKI PMA **AGREED** amendments to the Risk Register.

10. Standing Agenda Items

The following sub-sections of this agenda item provide an update on the monthly activities that are reported to the SMKI PMA by DCC, SECAS and BEIS:

6.1 SMKI Operational Update (RED)

The SMKI PMA was provided a confidential SMKI Operational update. The discussion was classified as **RED** and therefore recorded in the confidential minutes.

6.2 DCC Update

DCC representative (AB) informed the SMKI PMA that the DCC's Next Generation programme has commenced. It was noted that the DCC had presented a programme update to the SEC Panel on 13 December,

6.3 DCCKI PMA Function Update

It was noted that the next DCCKI PMA meeting will take place in the second week of January 2020.

6.4 BEIS Update

BEIS (RKS) provided the SMKI PMA with an update on recent and upcoming consultations, noting that BEIS will publish its consultation conclusion on the changes previously agreed by SMKI PMA to SEC Appendix L on 16 January 2020.

11. Any Other Business (AOB)

DCC representative (AB) questioned whether the Communication Service Providers (CSPs) are subject to SEC obligations. The SMKI PMA confirmed that all DCC sub-contractors are subject to SEC obligations.

Next Meeting: 21 January 2019