Meeting SECPMA_26_0908, 9th August 2016

10:00 – 14:00

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ

SMKI PMA Minutes

Attendees:

Category	SMKI PMA Members
SMKI PMA Chair	Gordon Hextall
Large Suppliers	Geoff Huckerby
Security Sub-Committee (SSC) Representative	Daryl Flack
Technical Sub-Committee (TSC) Representative	Julian Hughes

Non-Voting Members:

Category	Attendees
BEIS (Representative)	Joe Howard (Part meeting)
DCC	Andrew Smith
	David Shapland (TSP)
SMKI PMA Secretary (SECAS)	Joe Davenport

Apologies:

Category	Attendees
SMKI Specialist	Darren Calam
Networks	Sara Neal

Non-attendance:

Category	Attendees
Large Suppliers	Fabien Cavenne
Security Sub-Committee (SSC) Representative	Michael Constable
Ofgem (the Authority)	Nigel Nash

Introductions and Apologies

The Chair noted that with the apologies and non-attendance, it may not be possible to meet the SEC requirement for a quorum. In order to achieve a quorate for the meeting, three SSC members nominated Daryl Flack to act as the SSC Representative for the August 2016 SMKI PMA meeting.

1. Minutes of SMKI PMA Meeting 25_1207

There were no comments received on the July 2016 SMKI PMA Minutes, and the group approved the minutes as an accurate representation and record of the July 2016 meeting.

2. Actions Outstanding

SECAS provided the SMKI PMA with an update on actions outstanding from previous SMKI PMA meetings. The following section sets out items of discussion held during the August 2016 meeting, specifically:

Action Reference	Update
SECPMA 23/01	The DCC informed the SMKI PMA that due to the revised release schedule for DCC 'Live', the intention was to now bring this action item to the December 2016 or January 2017 meeting. The DCC confirmed an update would be provided at the November 2016 SMKI PMA meeting. The action was marked as **ONGOING.**
SECPMA 23/04	The DCC requested that as they had not yet received the final report from the SMKI auditor, this action be deferred until the September 2016 SMKI PMA Meeting. An update on the tScheme Stage 2 Assurance Report and resolutions to minor non-compliances was provided as part of Agenda Item 3 – Stage 2 Assurance Report (SECPMA_26_0908_03CONF). The action was marked as **ONGOING.**
SECPMA 25/01	The DCC are currently awaiting the final costing figures for the running of a single Recovery Event and whether this is on a per incident or per file basis. The DCC will provide an update on the costing once they receive final figures from the DSP. SMKI PMA members questioned whether there was a limit on the number of Devices they can submit on a file (for example 50,000). There is, currently, no designated limit for a Recovery Event, however, there is considered to be an operational limit, although this is not currently determined. A query was also raised on whether there would be a charge to the SMKI PMA if CSPs underwent a Recovery Event on Communication Hubs. The action was marked as **ONGOING**.
	ACTION SECPMA 26/01: The DCC will confirm whether there is a limit on the number of Devices that can be submitted per file and whether there is a proportionate, as well as unit cost.
	ACTION SECPMA 26/02: The DCC will confirm whether there would be a charge to the SMKI PMA should CSPs run a recovery event on Communication Hubs.

SECPMA 25/07	The SMKI Specialist and the DCC had held discussions in relation to the responsible party for setting SMI Statuses following a Recovery Event. It had been determined that the responsibility lay on the DCC. The detail and confirmation of this conversation would be extrapolated into the SMKI Recovery Key Guidance Document. The action was marked as **CLOSED** pending inclusion into the SMKI Recovery Key Guidance Document.
SECPMA 25/11	SECAS had reviewed the SEC to determine whether it was acceptable to publish a link to the Certification Practice Statements (CPS') in the SMKI Repository. A workaround has been tabled by the DCC and this is not in conflict with the SEC. The SMKI PMA agreed with the workaround. The action was marked as **CLOSED**.

3. Stage 2 Assurance Report

The DCC presented the SMKI PMA with a confidential agenda item update on the SMKI tScheme Stage 2 Audit, and the subsequent Stage 2 Assurance Report that would be produced and provide to the SMKI PMA. The DCC confirmed that all three Certificate Authorities (CAs) have now been assessed and approved: The Organisation CA (OCA), Device CA (DCA) and IKI CA (ICA). The DCC are currently working through non-compliances with all due to be complete by the 6th or 7th September 2016.

The group queried the DCA protocol in relation to the maximum number of Keys that could be issued, and the destruction of these once the maximum number of Certificates have been issued by a DCA (from an operational aspect). The group were told that DCA Key destruction is key to protecting the infrastructure. The DCC limits are currently proposed as a maximum of 24 months and minimum of 50 days after the creation of the keys. The keys are pre-generated and stored securely on HSMs but remain unassigned and accessible to the DCA until the key is signed or the certificate is generated. There are 4 Partitions and 500 keys pairs in each partition. Therefore, it is more sensible to remove the partitions entirely and alleviate the risk of human error that would arise from having to remove these manually each time. Once deactivated the key would remain on the HSM, inaccessible to the application, until it is taken offline and destroyed. The group noted it could still be susceptible to Brute Force attacks or through compromised key material.

To meet their SEC obligation, the DCC aim is to inform the SMKI PMA when the DCC intends to move on to the next partition, rather than doing so automatically or requesting permission, and the SMKI PMA were in agreement with this approach. The testing of this process will be undertaken at the same time as recovery testing. The TSP attendee confirmed that the process of generating keys involves creating them onto an offline backup and SMKI Service downtime would be required hence the proposed minimum timescale being set at 50 days. The SMKI PMA Chair advised the group that the original policy developed jointly by CESG and DECC (now BEIS) was originally prescribed due to the large volumes of meters that were expected and the inability to manage Certificate Revocations for over 100 million devices. The policy was to destroy the DCAs and the certificates every three months or when 100,000 Device Certificates had been issued to minimise the risk of compromise to the DCA. This is what happens during the DCC proposed process, except that the key remains deactivated on the HSM and would do for up to 24 months.

The TABASC representative noted that the proposed limit of two years was too long and therefore poses a risk, particularly from Administrators and requires a specific risk assessment to be

undertaken. The Chair re-iterated that the assumption was the DCAs and certificates would be destroyed as soon as they were expended. The TSP attendee advised this would be possible however the operational capability of the SMKI Service would have to be scaled back drastically. The minimum possible timescale for cycling DCA partitions without disruption to the service would be six months, needing to operate for three months and then the material must remain inactive a further three months otherwise there would be numerous errors being fed back from the meters. The Public Key or Certificate for that authority still continues and therefore trust can be established even though it is no longer possible to sign. The DCC confirmed that the DCA is destroyed after issuing 100,000 Device Certificates or after three months whichever comes first. The TSP attendee advised that practically it is possible to lower the maximum amount of days the material remains on the HSM to six months rather than 24 but not possible to go down as low as three months without disrupting the SMKI service.

The TSP attendee noted that key material is always planned to be destroyed and therefore it is the process for secure storage and destruction of this material that is in question. In the absence of Certificate Revocation for Device Certificates, the TSP stated that it has to be possible to retain the key pair but to prevent these being put back into use. The de-activation and storage process itself must be reliable, efficient and low risk. The timescales start from the issuing of a certificate to a device, but could also be taken from when a key in a partition is signed by a Root CA. The current active partition, used for the Key Ceremony that occurred in March 2016 resulted in 14 CAs which have been signed but only 5 used, these have now been marked as inactive as they have surpassed the three months' time limit.

The SMKI PMA were informed of the anticipated maintenance overhead for the overwrite or 'destruction' of a partition involving the removal of the key material entirely from the HSM and guaranteeing it was no longer available in the backup. The TSP attendee noted there will be many steps and check points in process to ensure it is not possible to take away the active keys in error or have the inactive material remaining on the HSM after destruction. The key is made inactive through the application rather than by an individual and the connection between the Key and CA is then broken. However, the control mechanism needs to be reviewed. The SMKI PMA were informed that an appropriate and meticulous risk assessment has been undertaken by the TSP for its Public Key services.

ACTION SECPMA 26/03: The TSP will investigate the Certification Practice Statements and determine the timescales for the deactivating of material once it reaches its maximum operational capacity (originally thought to be one hour).

ACTION SECPMA 26/04: The TSP will provide the risk assessment and feedback on how application management is controlled, the additional controls around the prevention of an inactive DCA being reactivated and the number of person(s) involved and responsible for the processes.

ACTION SECPMA 26/05: The TSP will quantify the actual maintenance impact and downtime of such an event and provide these figures to the SMKI PMA at a future SMKI PMA meeting.

ACTION SECPMA 26/06: The TSP will investigate reducing the proposed maximum 24-month window and the associated costs and overheads for necessary downtime.

ACTION SECPMA 26/07: If it will improve understanding, the TSP will construct a flow diagram or visual representation to identify and demonstrate the process behind the generation, destruction and associated costs of DCAs.

ACTION SECPMA 26/08: The DCC will distribute and share the audit outcome document with SMKI PMA members with the understanding that it will continue to be developed as a result of feedback

from SMKI PMA members. A second version will be distributed to the SMKI PMA prior to the September meeting.

Discussions were held on the planned response to a IKI and OCA compromise. The TSP attendee explained the walkthrough for the process and advised that an offline backup HSM is available, locked within a safe, and is also available for Disaster recovery. A failover event has been practiced and it has been established that the warm standby can be utilised within 4 hours. It was noted that the backup HSM was located within the same building complex as the SMKI production module. The SSC representative noted that, should a Disaster Recovery (DR) event occur that made the production HSM unavailable, then there was a risk that both the backup and production HSM's would both be lost. Leading from previous conversations, it was also questioned about what would happen if the backup HSM was lost or destroyed in transit during a recovery event. It was agreed that these processes would be reviewed and an update provided at the next SMKI PMA meeting.

The SMKI PMA also held discussions on the rollover of ICA and OCAs which occur after 15 years. A new Root would be required after 30 years. It was clarified that after this time the TSP would deactivate the issuing OCA to ensure the deactivated material cannot be reinstated.

ACTION SECPMA 26/09: SMKI PMA members to review an overview Document that outlines the DCA, ICA and OCA lifecycles. This will be issued to SMKI PMA members after the meeting..

ACTION SECPMA 26/10: The TSP/DCC will review the distance between the backup and production HSM, where it is stored, and provide an update to the SMKI PMA at their September 2016 meeting.

ACTION SECPMA 26/11: The TSP/DCC will review and provide an update to the SMKI PMA at their September 2016 meeting in relation to the transport of the backup HSM.

The SMKI PMA:

- **NOTED** the contents of the presentation.

4. SMKI Recovery Key Guidance Consultation Update

The Chair informed the SMKI PMA that a number of comments had been received from industry on the latest consultation of the SMKI Recovery Key Guidance (issued for consultation July 2016). The Chair provided background on the three consultations thus far, and noted that originally, the document had contained a large amount of sensitive data, resulting in a high level document being produced. It was noted that the interim SMKI PMA Chair that held the position between 2014 – 2015 had a minded-to view that the SMKI Recovery Key Guidance Document must not be a SEC Subsidiary Document, in order to ensure SMKI PMA flexibility for adapting the guidance to react to a Compromise (or suspected Compromise) event, and maintaining editorial rights with the SEC governance body. This minded-to view was reflected in DECC's (now BEIS's) consultation response, where DECC confirmed their proposal to adopt the governance model in the July 2015 SEC consultation.

The decision was taken that the document is to be maintained by the SMKI PMA and contain high level information so that it can be published as a public facing document. It was also noted that, following legal advice, this guidance material should contain SMKI PMA ***Must Do's***, (so that liability and accountability may be held against the SMKI PMA for not undertaking the necessary actions) and ***May Do's*** which allows for flexibility in any additional actions they may wish to undertake. The majority of consultation feedback was positive with agreement to the changes made and some helpful proposals that will be included in the updated document for publication. Some of the feedback received included:

(Q1). Do you agree that the decision making factors that the SMKI PMA proposes to apply are appropriate?

- Amendments had been sought in some of the wording relating to 'unverified' information, but this was proposed to be rejected due to the description encompassing the necessary elements already. Queries had also been raised on the maintaining of supply in the event of a recovery event, however it was argued this responsibility lay with Suppliers or Service users rather than the SMKI PMA.

(Q2). Do you consider that the SMKI PMA should take additional factors into account when deciding whether to initiate the Recovery Private Key or Contingency Private Key (including the Contingency Symmetric Key)?

- Some respondents had queried the risk assessments and who was responsible for these. It was confirmed that this is not normally undertaken by the SMKI PMA but by the Parties themselves on what the risks are of using, or not using, Recovery. The SMKI PMA would then analyse these third party risk assessments and then undertake their own risk analysis. The timescales considered as a part of the question 2 comment on risk assessment make it necessary to quantify necessary information as a part of a risk assessment beforehand wherever possible (number of available engineers, meters, how long to replace meters, cost etc.) to ensure the SMKI PMA has what it needs to make a decision. This is the kind of information that would adapt and change at different stages of the rollout and therefore would not be appropriate for a public facing guidance document but rather a more detailed document for internal use.
- Comments were also received on the Key factors and what the nature of the compromise was and the cost of recovery. It was noted that these are two key items that need to be captured by the guidance material. The nature (lost key, confidentiality compromise etc.) is captured through impacts (Supply, Security, Availability, Confidentiality etc.). Furthermore, the nature will affect the factors and considerations the SMKI PMA would need to place on the supplier (Lost v Compromised). Members agreed that this would affect the Must or May factors.

(Q3). What weighting, if any, should the SMKI PMA apply to the decision making factors?

- Some suppliers had commented on the Health and Safety impacts of a recovery event being the prime consideration. However, the SMKI PMA considered that Health and Safety was only a factor in a gas reconnection after a disconnection and rejected this as a priority consideration for all recovery events. However, the safety and continuation of the supply would be a key factor to be determined by the Supplier or Service User.
- One response proposed assigning weighting to consumer factors and the SMKI PMA agreed this a sensible approach.
- One respondent had suggested Smart Metering Business Impact Levels (SMBILS) should be incorporated into the weighting and advised it should be done in advance. It was agreed that thresholds may be appropriate but if a Recovery Event is only a cost of £60,000 total, then it would be a simple equation to establish which would be more financially detrimental to the company. Issues were then raised due to the frequency at which these keys may be used rather than going out and replacing the meters. Once used this information could be out in a public domain and accessible.

The £60,000 DSP cost estimate is awaiting confirmation and may not be correct as it does not seem to have factored in the generation of a new key.

(Q4). Does the document accurately outline the requirements and impact on Parties in relation to SMKI Recovery?

- Some respondents had raised the issue of consequential loss and what the future impact would be should the meters not be recovered; this will be considered for the updated document.
- A question had been raised on informing other persons, parties or organisations. It was noted that these obligations are highlighted in Section G of the SEC so it would be unnecessary to expand the guidance material further.

(Q5). Do you agree that no specific time limit should apply for the SMKI PMA to convene after being notified by the DCC of a Compromise, or suspected Compromise, of a Relevant Private Key?

- Discussions were held on the convening of meetings within 24 hours and the potential public opinion if these were not held in reasonable timeframe. This would be revisited at a time when more SMKI PMA members were in attendance.

(Q6). Do you agree that the document is fit for purpose and appropriate to be utilised in the event of a Compromise?

- Most of the comments were in agreement although some comments are more appropriate to a more granular and confidential guidance document rather than a published version. It was noted that the SMKI Specialist would be tasked with co-ordinating the responses between parties and the SMKI PMA.

The SMKI PMA:

- **AGREED** with a number of suggested amendments that were approved;
- **REJECTED** those that were not appropriate for the published version of the guidance document; and
- **NOTED** the contents of the presentation.

5. SMKI Recovery Scenarios Update

The SMKI PMA were advised that, at the request of the DCC, this item would be deferred, until the November 2016 meeting.

6. SMKI Operational Update

The DCC presented the SMKI PMA with an update on its SMKI operations to date, including the issuance of Certificates and issues arising.

It was noted that one SMKI Subscriber wished to revoke 2 of its 4 Organisation Certificates as they had been requested in error. The DCC confirmed they were progressing this request, going through a meticulous step by step process in order to ensure all necessary governance was in place (due to the likelihood that this would be an event that the tScheme auditor was going to want to assess). The DCC advised that although there is no Recovery Environment at present, this will not be a case of simply deleting the certificates due to the risk of where these certificates have been sent.

The DCC clarified that they are making the SMKI PMA aware of this process and are not seeking approval, as they do not wish for this to become a process that needs to be followed for every revocation.

The SMKI PMA advised that this is useful information that had been presented to them and favoured this approach moving forwards.

The SMKI PMA:

- **NOTED** the contents of this update.

7. DCC Release Strategy & CR Update

The SMKI PMA were advised that, at the request of the DCC, this item would be deferred, until a future meeting.

8. SMKI PMA Risk Register

SECAS provided a presentation on the progress being made for the SMKI PMA Risk Register. The group were informed that this was to be aligned with the SEC Panel's Risk Register, as this was the method currently adopted by the Technical Architecture and Business Architecture Sub Committee (TABASC), and which would be the standard template across the enduring SEC Panel Sub-Committees. It was noted the SMKI PMA Risk Register will cover governance risks only, with SSC covering security risk and the DCC operational risks.

The group were provided with an example of the SEC Panel Risk Register and templates that would be adopted for the SMKI Risk Register and Risk Matrix. The group were informed that in advance of the BEIS Smart Metering Issue Resolution Forum (SMIRF) meeting(s), SECAS would collate and update the SMKI PMA Risk Register. It was noted that SMKI PMA members would then be requested to consider these risks, and their likelihood, impact and severity.

The SMKI PMA:

- **AGREED** on the format of the Risk Register and Risk Matrix; and,
- **NOTED** the contents of this presentation.

ACTION SECPMA 26/12: SECAS to collate and complete the SMKI PMA Risk Register with governance risks and present these to a future SMKI PMA meeting for consideration.

9. SMKI Activity Planner

SECAS provided the SMKI PMA with an updated activity planner outlining the activities expected over the next three months, SECAS advised the group that there had been no significant amendments to the document since the July 2016 meeting.

The SMKI PMA:

- **NOTED** the contents of the Activity Planner.

10. Modifications Status Report

SECAS advised that there had been no further adjustments, or modification submissions, that had an impact on the SMKI PMA.

The SMKI PMA:

- **NOTED** the Modifications Status update.

11. DCC Update

The DCC advised that there was no further update from the DCC for August 2016.

The SMKI PMA:

- **NOTED** the DCC update for August 2016.

12. DCCKI PMA Functions Update

The DCC advised that there was no further update from the DCCKI PMA Functions for August 2016.

The SMKI PMA:

- **NOTED** the DCCKI PMA Functions update for August 2016.

13. BEIS Update

The DCC advised that there was no further update from BEIS for August 2016.

The SMKI PMA:

- **NOTED** the BEIS update for August 2016.

14. Any Other Business (A.O.B)

There was no further business raised and the Chair closed the twenty-sixth SMKI PMA meeting.

15. Next Meeting

The next meeting will be held on **13th September 2016.**