

This document is classified as **SMKI PMA Green**. Information can be shared with other SEC Parties and SMIP stakeholders at large, but not published (including publication online).

## Meeting SECPMA\_29\_0811, 8<sup>th</sup> November 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
	Fabien Cavenne
Networks	Sara Neal
Security Sub-Committee (SSC) Representative	Michael Constable
Technical Architecture and Business Architecture Sub-Committee (TABASC) Representative	Julian Hughes

#### Non-Voting Members:

Category	Attendees
BEIS (Representative)	Daryl Flack
	Joe Howard
DCC	Andrew Smith
DCC (TSP)	David Shapland (Teleconference (Part))
SMKI Specialist	Darren Calam (Teleconference (Part))
SMKI PMA Secretary (SECAS)	Joe Davenport

#### Apologies:

Category	Attendees
DCC	Marc Avery
The Authority (Ofgem)	Gwen Cruise

## 1. Minutes of SMKI PMA Meeting 28\_1110

SECAS advised they would include the apologies from the SMKI PMA Chair to the minutes of the October 2016 meeting.

The DCC noted concern with confidential items being recorded within these minutes, and SECAS advised that at draft stage, SMKI PMA Draft Minutes are not circulated further than members of the SMKI PMA. In addition, SECAS noted that, moving forward, confidential items discussed would be recorded in a separate set of Confidential Draft Minutes and distributed via Egress for comment.

The DCC also provided clarification on a number of items from the previous meeting including:

- **Action SECPMA 26/03** – The destruction of Key Material is completed manually and does not automatically rollover.
- **Action SECPMA 27/04** – The reference to ‘offshore’ will be removed, as this location is within the United Kingdom.
- **Action SECPMA 28/09** – The DCC clarified that the Initial Assurance Assessment reports (Stage 1 Assurance Report and Stage 2 Assurance Report) would be lodged within the DCC’s operational SharePoint site.

No further comments were received, and the SMKI PMA **APPROVED** the Minutes as Final Minutes.

**ACTION SECPMA 29/01:** SECAS will make the necessary amendments to the SECPMA\_28\_1110 – Draft Minutes and convert to Final Minutes.

## 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 November 2016 meeting, specifically:

Action Reference	Update
SECPMA 23/01	This action is covered by Agenda Item 3 – SMKI Recovery Desktop Exercise – Use Cases. The action was marked as <b>CLOSED</b> .
SECPMA 25/01	The DCC confirmed that no further clarification has yet been received from their commercial team on costing. The action was marked <b>ONGOING</b> .
SECPMA 26/03	The DCC confirmed that deactivation has been proven to occur one hour after maximum SEC defined capacity <sup>1</sup> has been reached. The Independent Assurance Service Provider had witnessed evidence of deactivation within one hour. The action was marked as <b>CLOSED</b> .
SECPMA 26/05	The Trusted Service Provider (TSP) confirmed that the maintenance window would be from one, to one and half hours, and that this would be undertaken once

<sup>1</sup> After 100,000 Certificates or after 3 Months

Action Reference	Update
	<p>on the live service and then repeated on the backup Hardware Security Modules (HSMs) for SMKI.</p> <p>The action was marked as <b>CLOSED</b>.</p>
SECPMA 26/06	<p>The TSP provided an update on the proposed maximum 24-month window for holding deactivated Key Material. The SMKI PMA were informed that approximately six destruction events would occur over the remaining years of the contract. The TSP advised that a further review was being undertaken and updates would be provided to the SMKI PMA.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 26/07	<p>The DCC advised that the process flow diagram had been produced within the slide deck previously provided to attendees of the DCC workshop on 6<sup>th</sup> October. The diagram will be published within the relevant TSP document, and circulated to SMKI PMA Members by the DCC.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 26/11	<p>The TSP advised the group that it is intending to relocate some key Custodian responsibilities to London, UK so that a key destruction ceremony can be undertaken at this location as an alternative. The group were informed that a HSM would still need to be transported from Cardiff, but would no longer have to travel with Key Custodian personnel, therefore reducing risk, costs and disruption.</p> <p>The action was marked as <b>CLOSED</b>.</p>
SECPMA 27/04	<p>The TSP provided an update to the group in relation to the relocation of the HSM back-up facility in Cardiff, and the TSP advised the SMKI PMA that they had obtained a quotation for the creation of a third HSM in the order of £6,000. The TSP advised that a further cost would be incurred through additional requirements and operational costs.</p> <p>The TSP noted the only requirement for access to both HSMs is during the creation of new HSM material, and therefore it could be possible to move the second HSM from its current location to another, existing secure site to obviate the need for a third HSM. The TSP have also considered a second potential location for moving the HSM that would be easier to travel to from an operational standpoint.</p> <p>Whilst determining the best solution, the TSP advised the group that the third HSM would take a long period of time to acquire and commission. The TSP noted that so far, the backup HSM had never been relied upon or required for technical reasons, but noted however, it is still required for standard operational procedures. The TSP confirmed it was possible to move the second HSM away from its current location to mitigate the immediate risk and then create a third HSM at a later stage at the current location for operational accessibility. The SMKI PMA noted that location of the HSM would need to be a factor for the TSP to consider.</p> <p>The DCC confirmed their preference to the SMKI PMA for a third HSM to be established, due to the low associated costs and the risk mitigation benefits it offered.</p> <p>The TSP noted that the next Key Ceremony is due in February 2017. It was noted that, at this Key Ceremony, it would be beneficial to place a clone of the existing Root CA Key onto the (potentially new) backup HSM.</p>

Action Reference	Update
	The action was marked as <b>CLOSED</b> and superceded by Action <b>SECPMA29/01</b> .
<b>SECPMA 27/12</b>	<p>The TSP advised the SMKI PMA that as part of the Root Cause Analysis, the Open SSL had been deemed not necessary. The group were informed that there are currently two different formats for checking the output of generating Certificate Authorities (CAs). As a result, introducing the Open SSL would mean a third format was added to the process, resulting in additional complexity and risk. The TSP informed the SMKI PMA that it is now easier to undertake a comparison to ensure the correct extensions are in place. The group were informed that sufficient safeguards were in place to ensure the issue that occurred was not repeated.</p> <p>The action was marked as <b>CLOSED</b>.</p>
<b>SECPMA 27/13</b>	<p>The DCC advised that System Integration Testing (SIT) will prove CR101 (DSP Environment to support SMKI Recovery Procedure), the ability to undertake recovery, and the rollover of CAs. The DCC confirmed they were currently unable to confirm a date due to continuing internal discussions.</p> <p>The action was marked as <b>ONGOING</b>.</p>
<b>SECPMA 27/14</b>	<p>A summary of Root Cause Analysis in relation to Certificate Profiles in User Integration Testing (UIT) was sent to SECAS by the DCC. It was confirmed that this document will be published on Egress for SMKI PMA Members.</p> <p>The action was marked as <b>CLOSED</b>.</p>
<b>SECPMA 27/15</b>	<p>The additional tests for the transition over an additional CA hierarchy had been discussed by the DCC Test Team. This test will be described in further detail once the DCC has published the relevant documentation.</p> <p>The action was marked as <b>ONGOING</b>.</p>
<b>SECPMA 27/17</b>	<p>The SMKI PMA were informed that the DCC had clarified with the Authorised Responsible Officer (ARO) Manager that there is currently a process for alerting persons to the revocation of a Certificate. It was confirmed that, when revoked, an email is sent back to the requestor to confirm revocation. This process is described in the SMKI Registration Authority Policies and Procedures (SMKI RAPP).</p> <p>Members of the SMKI PMA advised that in some instances, they had not received notifications. SMKI PMA Members advised they are currently keeping a manual log of leavers and joiners. It was noted that a quarterly report would be beneficial in order to resolve this issue. The DCC advised the group that they would investigate making this available online through the DCC operational SharePoint site.</p> <p>The action was marked as <b>ONGOING</b>.</p>
<b>SECPMA 28/01</b>	<p>This action is covered by agenda item 3 – <i>SMKI Recovery Desktop Exercise Use Cases</i>.</p> <p>The action was marked as <b>CLOSED</b>.</p>

Action Reference	Update
SECPMA 28/03	<p>The DCC advised that information relating to a Recovery Event involving Communication Hubs from the commercial team was pending.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 28/04	<p>The DCC advised they will circulate any additional documentation from the meeting held on Monday, 3<sup>rd</sup> October 2016 to SMKI PMA Members.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 28/05	<p>The SMKI PMA Chair confirmed he had approached CESG (now the National Cyber Security Centre (NCSC)) but had not yet received a response. The DCC and TSP advised they would be ready to assist or implement any changes recommended by NCSC.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 28/08	<p>The documentation for the Root Cause Analysis has been made available and will be published on Egress.</p> <p>The action was marked as <b>CLOSED</b>.</p>
SECPMA 28/09	<p>The DCC advised that the Stage 2 Assurance Report had been made available on the DCC operational SharePoint site. The DCC sought confirmation that the correct version of the Stage 1 Assurance Report had been seen by all SMKI PMA Members prior to its publication and was the correct version.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 28/11	<p>SECAS advised that the Process Flow diagram for the confidential SMKI Recovery Key Guidance document will be developed following the SMKI Recovery Desktop Exercise.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 28/14	<p>This action is to remain ongoing until the completion of the SMKI Recovery Desktop Exercise.</p> <p>The action was marked as <b>ONGOING</b>.</p>
SECPMA 28/17	<p>SECAS had approached the Authority in relation to the SMKI Organisation Certificate issue discussed at a previous SMKI PMA meeting.</p> <p>It was noted that the Authority had raised this question to BEIS. BEIS advised that any amendments to SEC Subsidiary Documents would require a Modification Proposal to be submitted. It was noted that if the DCC User Interface Specification (DUIS) were to be amended through a Section 88 Change, then this would be drafted by someone within BEIS. It was confirmed that this amendment would allow the incorrect SMKI Organisation Certificate to be replaced once.</p> <p>It was noted that the development of a naming convention for the <code>id-at-commonName</code> field within a SMKI Organisation Certificate would assist in future instances. The SMKI PMA were informed that the method for correcting and communicating this naming convention had been fed back to the Energy Networks Association (ENA), and that the ENA were investigating how to implement this.</p>

Action Reference	Update
	The action was marked as <b>CLOSED</b> .
<b>SECPMA 28/18</b>	This action is covered within action <b>SECPMA 28/17</b> . The action was marked as <b>ONGOING</b> .
<b>SECPMA 28/21</b>	The Certificate Signing Request (CSR) forecast had now been included in the SMKI Operational Update. The action was marked as <b>CLOSED</b> .
<b>SECPMA 28/26</b>	DCC had confirmed that the SRT work off elements had been completed and written confirmation received. The action was marked as <b>CLOSED</b> .

**ACTION SECPMA 29/01:** The DCC/TSP will investigate the feasibility of relocating the existing backup HSM to another location within the UK, and then, having an additional third HSM ready for February 2017.

**ACTION SECPMA 29/02:** SECAS will publish the BT documentation relating to Certificate Profiles in UIT on Egress.

**Action SECPMA 29/03:** ENA will look at the proposals for a naming convention and will bring the options to the December 2016 SMKI PMA meeting in order to establish a short term solution prior to either a Modification Proposal or Section 88 change being made to DUIS.

### 3. SMKI Recovery Desktop Exercise – Use Cases

The DCC informed the SMKI PMA that they had previously discussed SMKI Recovery Scenarios and the SMKI Recovery Event with the Service Management Design Forum (SMDF). It was noted that the SMDF would be running their own exercise in either January 2017 or February 2017. The SMKI PMA were advised that the SMDF would be dealing with the operations and processes of a Recovery Event, and that the SMKI PMA would look at the likely sequence, who is involved, and who approves what within the process.

The SMKI PMA Chair noted that the original aim of the SMKI Recovery desktop exercise was to demonstrate the process of recovery, the recovery environment, and enable the SMKI PMA to test the scenarios against the SMKI Recovery Procedure and the SMKI Recovery Key Guidance document. A Large Supplier Representative questioned whether there would be a need to include DCC Key Infrastructure (DCCKI) within any of the scenarios when undertaking the SMKI Recovery desktop exercise. The DCC advised the Private Keys for DCCKI (Root and online intermediate CA) have their own HSMs, and are not shared with Transitional Change of Supplier (TCoS) process (as well as any SMKI Private Keys which are held separately). It was noted that if one of the Smart Metering Implementation Programme (SMIP) Public Key Infrastructures (PKI) were disabled or taken down, other SMIP PKIs would be affected in addition. The SMKI PMA noted it would be useful to consider TCoS within the SMKI Recovery desktop exercise as well.

A Large Supplier Representative questioned whether it would be acceptable for the SMKI PMA to allow DCC Users to invoke Method 1 (use of their own Credentials), and SMKI PMA Members concluded it would be if there was a good understanding of where the risks had originated and how these were handled.



The SMKI PMA considered whether evoking Method 1 (use of their own Credentials) without performing an in-depth review was acceptable. The DCC noted this method was the fastest way of dealing with a potential Compromise (or suspected Compromise) in an effective way. The SMK PMA requested visibility of a Use Case on Method 1, as well as all other Methods available as part of the desktop exercise.

The SMKI PMA reviewed the presentation in relation to the exercise undertaken by the SMDF in February 2016. The SMKI PMA queried whether there would be a scenario related to compromise of the Device Certificate Authority (DCA) Certificates, even though they are not covered within the SMKI environment. The SMKI PMA agreed that DCA Certificates should be included and understood (even though it may not be included within the scope of the SMKI Recovery Procedure).

The SMKI PMA noted that the Use Case Scenarios they would want included within the SMKI Recovery desktop exercise were Methods 1, 2 and 3, DCAs, Single User, False Alarm, and DCC/TSP Compromise (or suspected Compromise).

The SMKI PMA Chair noted the benefit for considering multiple Use Cases and/or test scenarios, confirming this will test the SMKI Recovery Key Guidance produced by the Sub-Committee and the overall use of this document.

It was confirmed that the draft plans and test scenarios and associated Use Cases will be presented at the December 2016 SMKI PMA meeting. The SMKI PMA Chair advised that it would be beneficial to hold this over an entire day, in order to ensure all areas were covered effectively. It was suggested that Tuesday, 10<sup>th</sup> January 2017 would be the most appropriate date. The SMKI PMA Chair confirmed that he would write out the Terms of Reference (ToR) for the SMKI Recovery desktop exercise and provide this to both the DCC and to SMKI PMA Members.

The SMKI PMA:

- **NOTED** the SMKI Recovery Desktop Exercise Use Cases update; and
- **AGREED** to hold the SMKI Recovery desktop exercise on Tuesday, 10<sup>th</sup> January 2017.

**ACTION SECPMA 29/04:** The DCC will present the draft scenarios for the January 2017 Desktop Exercise at the December 2016 SMKI PMA meeting.

**ACTION SECPMA 29/05:** SMKI PMA Chair to draft up ToR for the SMKI Recovery desktop exercise and provide this to the DCC and SMKI PMA Members.

**ACTION SECPMA 29/06:** SECAS to arrange an additional SMKI PMA meeting for the 10<sup>th</sup> January 2017.

## 4. SMKI Recovery Key Guidance - Supporting Confidential Document

SECAS informed the group that the supporting confidential document had been amended to incorporate comments made by BEIS on the original SMKI Recovery Key Guidance Document. The document now included the Smart Metering Business Impact Levels (SMBILS) Table, which was raised as an item to be included by BEIS. It was noted that the flow diagram would be incorporated at a later stage following the SMKI Recovery desktop exercise.

The DCC noted that the confidential supporting document could also be used as input for the desktop exercise.

The SMKI PMA Chair invited SMKI PMA Members to continue providing comments and feedback on the supporting confidential document.

The SMKI PMA:

- **NOTED** the content of the supporting confidential SMKI Recovery Key Guidance document.

## 5. SMKI Operational Update

The DCC provided an update on SMKI operations since their last update at the October 2016 SMKI PMA meeting.

The DCC advised that currently, the CSR forecast was 1.5million Certificates per month for 10 SEC Parties. SMKI PMA Members queried the low number of SEC Parties submitting CSR forecasts as currently 40 Parties have passed SMKI and Repository Entry Process Tests (SREPT). The SMKI PMA noted that although this had no direct impact on the Sub-Committee, the DCC should raise these low forecasts as an area of concern. It was noted that, though this was in part due to SEC Parties fulfilling their obligations by submitting CSR forecasts, the DCC should investigate this further, and the BEIS Representative noted he would raise this internally also.

**Post-Meeting Note:** The DCC have since clarified that the CSR figures came from a report that has since been superseded. The revised monthly figure is 242,000 Certificates from more than 10 SEC Parties.

A BEIS Representative questioned the number of Infrastructure Key Infrastructure (IKI) Certificates issued so far (424 in total), and observed that this number was high. The DCC advised that some organisations had a large number of Senior Responsible Officers (SROs) and AROs, and that multiple SEC Parties may have in excess of 10+ IKI Certificates issued to each SEC Party. The SMKI PMA noted it may be possible there is a risk that IKI Certificates can (and may) be used to obtain Organisation Certificates for malicious purposes.

**Post-Meeting Note:** The DCC have since clarified that there is already a monthly report sent to every SEC Party (SRO) relating to IKI certificates issued to their SEC Party, as defined in the SMKI Registration Authority Policies and Procedures (RAPP). Also in for the notification of IKI revocation, the DCC intend to simplify the process and send notification directly from RA manager. In response to the potential risk; the DCC always contact the SRO to verify the genuine origin and intent for issuance/revoking of an Organisation Certificate.

The SMKI PMA requested that the number of Anomaly Detection Threshold (ADT) signing Certificates be made available to the Sub-Committee, however, the DCC Representative noted he was unsure of the current figure.

The DCC informed the Sub-Committee that when Suppliers are submitting test SMKI RAPP forms, and particularly for ADTs, Suppliers were requested to submit an all zero file prior to sending a file with their actual figures, in order for the DCC to determine whether they have used the correct File Signing Certificate.

The SMKI PMA:

- **NOTED** the SMKI Operational update provided by the DCC.

## 6. SMKI PMA Risk Register

SECAS presented the Sub-Committee with an update on the SMKI PMA Risk Register. SECAS noted that minor amendments had been made to the wording of Risk 4, and that no further risks had been added. It was noted that the SMKI PMA Risk Register would be reassessed after the initial meetings held by the Smart Metering Issue Resolution Forum (SMIRF) following DCC Live (Release 1.2).



The SMKI PMA:

- **NOTED** the Risk Register Update for November 2016.

## 7. SMKI PMA Activity Planner

SECAS provided the SMKI PMA with an updated activity planner outlining the activities expected over the next three months. Additional activities such as SMKI PMA Member nominations, The SMKI Recovery Desktop Exercise, bi-annual SMKI Independent Assurance Scheme follow up assessments, and modifications which may affect the Sub-Committee, had now been included.

The SMKI PMA:

- **NOTED** the Activity Planner for November 2016.

## 8. Modifications Status Report

SECAS informed the SMKI PMA that the modification for increasing the voting members of the SMKI PMA, as well as removing the restrictions on SMKI PMA Alternates being employed by the same organisation, was due to be decided upon at the Change Board meeting being held on Wednesday, 23<sup>rd</sup> November 2016.

The SMKI PMA:

- **NOTED** the Modifications Status update for November 2016.

## 9. DCC Update

The DCC advised the Sub-Committee that DCC Live R1.2 was scheduled to take place on Tuesday, 8<sup>th</sup> November 2016. It was noted that further work was being undertaken in relation to the Self Service Interface (SSI) and Self Service Management Interface (SSMI).

The SMKI PMA:

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

## 10. DCCKI PMA Functions Update

The DCC advised that the DCC Key Infrastructure User Interface (DCCUI) was now ready to 'go live'. The DCC also advised that the audit of DCCKI had been scheduled for three months after live operation. There was currently no fixed date for the audit to be undertaken, however, it was noted that the latest possible date was set as 8<sup>th</sup> February 2017 (if DCC Go live for R1.2 is 8<sup>th</sup> November 2016).

The Sub-Committee were informed that the audit will look at key management within DCCKI, and how it complies with the DCCKI Certificate Policy (CP) and DCCKI RAPP. The DCC clarified that the Data Service Provider (DSP) was ISO27001 Certified, and that subsequent DSP Information Security Management System (ISMS) audits will result in an auditor being able to assess the summary and scope of DCCKI Services.

The DCC agreed to provide further details of their UKAS accredited ISO27001 independent audit of DCCKI at the January 2017 SMKI PMA meeting. The SMKI PMA Chair requested that previous minutes and documentation from DCCKI PMA Functions meetings are also provided at the next SMKI PMA meeting.

The SMKI PMA:

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

**ACTION SECPMA 29/07:** The DCC to provide the SMKI PMA with the minutes and slides from previous DCCKI PMA Functions meetings at the December 2016 SMKI PMA meeting.

## 11. BEIS Update

The Sub-Committee were advised that there was no further update from BEIS for November 2016.

The SMKI PMA:

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

## 12. Any Other Business (A.O.B)

SECAS informed the Sub-Committee that a nomination had been received for the Small Supplier seat on the SMKI PMA. It was noted that the necessary steps would now be undertaken in order to appoint the nominee to the vacant Small Supplier seat.

SMKI PMA Members requested that the invites to the meetings of 2017 are also released.

**ACTION SECPMA 29/08:** SECAS to invite the new Small Supplier Representative to the next SMKI PMA meeting.

**ACTION SECPMA 29/09:** SECAS will release the 2017 meeting schedule to SMKI PMA members.

The SMKI PMA Chair noted that there was no further business and closed the November 2016 SMKI PMA meeting.

## Next Meeting

The next meeting will be held on **Tuesday, 13<sup>th</sup> December 2016**.