

## Meeting SECPMA\_20\_0902, 9<sup>th</sup> February 2016

12:00 – 16:00

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ

### SMKI PMA Minutes

#### Attendees:

Category	SMKI PMA Members
SMKI PMA Chair	Gordon Hextall
Large Suppliers	Fabien Cavenne
	Geoff Huckerby
Networks	Sara Neal
Technical Sub-Committee (TSC) Representative	Julian Hughes

#### Non-Voting Members:

Category	Attendees
SEC Panel Chair	Peter Davies (Part)
SMKI Specialist	Darren Calam
DCC	Marc Avery
	Phillip Twiddy (Part)
	Paul Evans (Teleconference) (Part)
Ofgem (the Authority)	Nigel Nash
DECC (Representative)	Joe Howard
SMKI PMA Secretary	Joe Davenport
SECAS	James Simmonds
	Sebastian Rattansen (Part)

#### Apologies:

Category	Attendees
Small Supplier	Rob Kinson
Security Sub-Committee (SSC) Representative	Michael Constable

## 1. Minutes of SMKI PMA Meeting 19\_1201

There were no suggested amendments to the draft minutes and the SMKI PMA agreed the minutes as written.

## 2. Actions Outstanding

**SECPMA 19/01** – The DCC confirmed that they had contacted the SEC Parties that had made multiple nominations to become Key Custodians, and informed them that only two nominations could be submitted. This action was marked as **CLOSED**.

**SECPMA 19/02** – The DCC confirmed that an updated, confidential Key Custodian report would be presented as a part of Agenda Item 04 (*SECPMA\_20\_0902\_CONF04 – Key Custodian Nominations*). This action was marked as **CLOSED**.

**SECPMA 19/03** – After discussion between DECC, the DCC and the Panel Chair, it was confirmed that the Key Custodian nominations received from RWE Generation (UK) could be accepted. This action was marked as **CLOSED**.

**SECPMA 19/04** - The DCC and DECC had met following the January 2016 SMKI PMA meeting and agreed that the SMKI & Repository Testing (SRT) Approach Document consultation period would be two weeks. A further update was provided as part of agenda item 06 (*SECPMA\_20\_0902\_06 - SRT Approach Document*). This action was marked as **CLOSED**.

**SECPMA 19/05** - The DCC and DECC confirmed they had investigated paragraph 124 (page 46) of the December 2015 Consultation Response document and clarified its relevance to the enduring world. This action was marked as **CLOSED**.

**SECPMA 19/06** - In relation to the SMKI Recovery Key Guidance document, and accompanying confidential processes document, SECAS confirmed that they had attended a DCC workshop on the SMKI Recovery Procedure and process flows, and as such, would update both documents for submission at the March 2016 SMKI PMA meeting. This action was marked as **ONGOING**.

**SECPMA 19/07** - The DCC advised that they had amended the necessary DCC KI PMA Function documentation so that the word 'Function' now appeared after every mention of DCC KI PMA, and that they would re-issue an amended Terms of Reference (ToR) to the SMKI PMA. This action was marked as **CLOSED**.

## 3. SECPMA\_20\_0902\_CONF03 – IKI Certification Practice Statement (CPS)

The DCC provided the SMKI PMA with the amended and confidential Infrastructure Key Infrastructure (IKI) CPS, and were advised that the document required approval in order to issue live SMKI Certificates on 9<sup>th</sup> March 2016. The DCC further informed the group that the IKI CPS had been amended to align the document with the current version of the IKI Certificate Policy, and requested that SMKI PMA Members review the amended IKI CPS and provide feedback within 10 Working Days to SECAS following the February 2016 meeting (19<sup>th</sup> February 2016). SECAS agreed to forward any comments received on the IKI CPS to the DCC.

The DCC noted that, following the review of comments received, the DCC would submit the final version of the IKI CPS to the March 2016 SMKI PMA meeting for approval.

The SMKI PMA **AGREED** to provide comments (if any) to SECAS on the IKI CPS by the 19<sup>th</sup> February 2016.

The DCC advised that the IKI Authority Revocation List (ARL) had been voided for IKI Certificate Authority Certificates and IKI Certificate Revocation List (CRL) had been voided for IKI Certificates.

The DCC requested for the removal of the requirement to publish the IKI ARL and CRL to the SMKI Repository which had previously been agreed between DECC and the DCC. This amendment will be reflected in the latest version of the SEC.

The SMKI PMA **AGREED** with the removal of the aforementioned requirement.

**ACTION SECPMA 20/01:** SECAS to compile responses on the IKI CPS and provide these to the DCC by 19<sup>th</sup> February 2016.

## 4. SECPMA\_20\_0902\_CONF04 – Key Custodian Nominations

The DCC provided the SMKI PMA with an updated confidential report on the nominations received to date to become Key Custodians. The DCC confirmed that they had undertaken identity verification of nominated individuals approved to be Key Custodians by the SMKI PMA, and in addition had received further submissions from SEC Parties, and provided these submissions to the SMKI PMA for approval. The group were informed that 15 nominations was the absolute minimum required for the Key Ceremony to take place in February 2016. It was advised that if 19 attend the Key Ceremony, then four individuals must be made aware that they are acting as reserves and will therefore not take place in the Key Ceremony itself.

The DCC and DECC confirmed they were satisfied with the RWE Generation (UK) nominations that had been received prior to the January 2016 meeting, and as a result, could be included as part of the total nominations submitted as part of the February 2016 report. The DCC informed the group that a briefing note had been published on the DCC's SharePoint and sent to each of the approved Key Custodians to inform them of their upcoming responsibilities. The group enquired as to the 'Go/No Go decision' for the Key Ceremony and were advised this would take place on 22<sup>nd</sup> February 2016. The SMKI PMA were in agreement that the DCC should inform Key Custodians as soon as possible after the 'Go/No Go decision'.

The group were informed that they would be receiving one further nomination which would bring the total Key Custodians to 20. The SMKI PMA **APPROVED** the appointment of the nominations that were received and deemed valid, as well as the nomination yet to be received by a Large Supplier.

**ACTION SECPMA 20/02:** DCC to inform all Key Custodians (both travelling and reserved) on the outcome of the 'Go/No Go decision' for the Key Ceremony being held, following their meeting on 22<sup>nd</sup> February 2016.

## 5. SECPMA\_20\_0902\_05 – Service Provider Performance Measures

Following a request by the SEC Panel Chair, the group discussed the DCC's consultation on contract changes which alter the DCC's Service Provider Performance Measures used to support the SMKI Services. The group were advised that the consultation closes on 16<sup>th</sup> February 2016 and feedback would be required to be presented to the SEC Panel on 12<sup>th</sup> February 2016.

The SMKI PMA had no disagreement with the proposed changes within the consultation on the basis that it would align the DCC's Service Provider contracts with the SEC Obligations, and **AGREED** to provide a recommendation to the SEC Panel.

**ACTION SECPMA 20/03:** SMKI PMA Chair to write to the SEC Panel Chair to confirm that the SMKI PMA are in agreement with the proposed amendments within the DCC's Service Provider Performance Measures consultation.

## 6. SECPMA\_20\_0902\_06 – SMKI and Repository Testing (SRT) Approach Document

The DCC provided an update on the amendments being made to the SRT Approach Document and walked the SMKI PMA through the updates that had been made following the consultation window.

A SMKI PMA Member questioned whether there was a case for the Symmetric Key itself being compromised as without this the scope of the Recovery and Contingency Scenarios is insufficient.

Discussions were held on Section 11.11 '*Recovery – Apex Contingency Key*' of the SRT Approach Document, specifically SMKI 53 Test Scenario, which looks at the use of the Contingency Key (but is written in a way that suggests it is testing compromise of the Symmetric Key that wraps the Contingency Key). The DCC noted that this would be covered in SRT Part 3 and had therefore been removed from the SRT Approach Document v3.5.

The SMKI PMA Chair informed the group that CR129 (DSP Recovery Environment Certificate Validation Requirements) is currently being developed in order to prove it is capable of being used on Devices, however, this is not shown within the SMKI 53 Test Scenario. The DCC noted that Meter Manufacturers will have the ability to support CR129 during SRT3, but that this had not been explicitly stated within the SMKI 53 Test Scenario. The DCC confirmed that these Test Scenarios were not falling out of scope, and would be tested within SRT Part 3. The DCC further noted that this test highlighted the use of the DCC's Contingency Request, as per DECC's Senior Responsible Officer's letter in December 2015.

The group concluded that the DCC should rewrite SMKI 53 Test Scenario accordingly to test use of the Contingency Key in various scenarios.

The group queried the Requirement Traceability Matrix and whether the ability to test the Apex Contingency Key had been reviewed. DECC advised that test scripts are reviewed regularly, and that work is underway between DECC and the DCC to ensure each test script is tested in full.

Following the identification of a gap within the SMKI 53 Test Scenario, the SMKI PMA requested the DCC conduct a root cause analysis of how this gap appeared.

The SMKI PMA agreed in principle to the updated SRT Approach Document (subject to the DCC making the amendments suggested) and **AGREED** to provide a recommendation to the SEC Panel accordingly.

**ACTION SECPMA 20/04:** The DCC to run root cause analysis on SMKI 53 and ensure that it reflects the scenarios that are valid for use of the Contingency Key.

**ACTION SECPMA 20/05:** SMKI PMA Chair to write to the SEC Panel Chair to confirm that the SMKI PMA are in agreement that the SEC Panel should approve the SRT Approach Document (subject to the amendments being made and agreed).

**ACTION SECPMA 20/06:** DCC to consider (upon request) allowing access to the Test Scenarios spreadsheets in order to identify the method for testing CR129.

## 7. SECPMA\_20\_0902\_07 – SRT Completion Report

The DCC informed the SMKI PMA of an obligation to review an SRT completion report, in conjunction with the Testing Advisory Group (TAG), which will set out the ways in which the DCC has successfully exited each test element and part of SRT (prior to the SRT completion report being submitted to the SEC Panel for approval), as per SEC Section T5.19. The Secretary of State Direction letter had previously stated that before live SMKI Certificates can be issued, the DCC must undertake adequate and appropriate testing to ensure the Apex Contingency Key's functionality.

The group were informed that an interim report shall be submitted to TAG and the SMKI PMA for discussion.

**[Post-meeting note: following the February 2016 SMKI PMA meeting, an ex-committee teleconference has been scheduled for SMKI PMA members to join the February 2016 TAG meeting (29<sup>th</sup> February 2016) in order to discuss the SRT completion report as an agenda item at said meeting].**

The group noted it would be beneficial for the DCC to continuously update the steps of SRT testing as they complete, to allow the compilation of the final document to be expedited and presented to the necessary governance bodies within the current timescales.

The SMKI PMA **NOTED** the upcoming requirement to review an SRT completion report, prior to the DCC submitting the aforementioned final report to the SEC Panel for approval.

**ACTION SECPMA 20/07:** DCC to clarify the timelines for SRT completion, in order for ex-committee meetings being organised prior to the final SRT completion report being submitted to the SEC Panel for approval.

## 8. SECPMA\_20\_0902\_08 – SMKI RAPP and SMKI Recovery Procedure

SECAS informed the SMKI PMA that in accordance with SEC Section L1.17(d), the SMKI PMA would be required to review a number of designated SMKI SEC Subsidiary Documents, and if required, submit one or Modification Proposals as soon as reasonably practicable.

The SMKI PMA Chair and DCC advised the group that, as both the SMKI Registration Authority Policies and Procedures (SMKI RAPP) and SMKI Recovery Procedure had been through extensive consultation and review periods prior to designation, it may be beneficial to defer the review of both documents until a later date. The DCC further noted it may be of benefit to review the effectiveness of SMKI SEC Subsidiary Documents once further SEC Parties had completed SMKI and Repository Entry Processing Testing (SREPT), and where the DCC can provide information in relation to the SMKI PMA on the effectiveness of SMKI SEC Subsidiary Documents. SECAS agreed to produce a paper for the March 2016 SMKI PMA meeting, which sets out the various SMKI SEC Subsidiary Documents that the group has governance over.

**ACTION SECPMA 20/08:** SECAS to produce a timetable for the review of SMKI Subsidiary Documentation as per the SEC Obligation.

## 9. SECPMA\_20\_0902\_09 – SMKI Recovery Procedure Workflows

The DCC presented the group with the current workflows in relation to the Recovery Event processes. These showed the methods by which the DCC would inform the SMKI PMA of when the group would be contacted in the event of a Compromise and as part of the Recovery Event.

The group queried flow 4.8 of the presentation, which shall involve dialogue between the DCC, the SMKI PMA and any affected User(s). It was noted that discussions had been held previously, where it was noted that the initialisation of the recovery environment would involve the DCC, the Security Sub-Committee (SSC), affected SEC Parties and any other persons deemed necessary to provide evidence and details to facilitate the SMKI PMA to make a decision.

Members were also advised that the estimated cost for establishing the recovery environment was not excessive and would be manageable, and that updated figures would be provided to the SMKI PMA at a future meeting.

SECAS noted it would be beneficial to work alongside the DCC in order to develop wider SMKI-related guidance, which captures the ways in which the SMKI PMA are involved with the recovery process (and/or future Recovery Events), and various elements of SMKI Services from a DCC User perspective.

**ACTION SECPMA 20/09:** SECAS to finalise the draft SMKI Recovery Key Guidance document and accompanying confidential processes document for the next meeting.

**ACTION SECPMA 20/10:** SECAS and the DCC to discuss the development of wider SMKI Service guidance.

## 10. SECPMA\_20\_0902\_10 – SEC Modification Process

SECAS presented an outline of the SEC Modification Process, and the levels of involvement the SMKI PMA may have, and can have, in regards to Modification Proposals being raised and progressed.

DECC informed the group that it would be possible to raise Modifications for SEC Subsidiary Documents that had not yet been designated by the Secretary of State. Ofgem noted that due to the Smart Metering Implementation Programme (SMIP) still being delivered in stages, DECC (for a period of time following DCC Release 1.3) would act as the 'Authority' in relation to the Modifications Process.

The SMKI PMA requested that a new standing agenda item be added to each future SMKI PMA meeting, whereby SECAS would provide an update in relation to all Modifications Proposals raised by industry that may require SMKI PMA involvement, or equally, where the SMKI PMA may be able to assist with the Modification Process.

**ACTION SECPMA 20/11:** SECAS to add a new standing agenda item to each future SMKI PMA meeting which provides the group with a Modifications Update.

## 11. SECPMA\_20\_0902\_11 – SMKI PMA Activity Planner

The SMKI PMA **NOTED** there had been no changes to the SMKI PMA Activity Planner since the last meeting.

## 12. SECPMA\_20\_0902\_12 – DCC Update

The SMKI PMA **NOTED** there was no further updates from the DCC for February 2016.

## 13. SECPMA\_20\_0902\_13 – DCCKI PMA Update

The DCC informed the group that the first meeting of the DCCKI PMA Function had been held.

The SMKI PMA **NOTED** the update and **REQUESTED** minutes from the first DCCKI PMA Function meeting be provided to the SMKI PMA.

**ACTION SECPMA 20/12:** DCC to circulate the minutes from the first DCCKI PMA Function meeting to SMKI PMA prior to a future meeting.

## 14. SECPMA\_20\_0902\_14 – DECC Update

The SMKI PMA **NOTED** there was no further updates from DECC for February 2016.

## 15. Any Other Business

The DCC sought approval from the SMKI PMA for three Service Policy Disclosure Statements (SPSD) to be published within the SMKI Repository as a compliance requirement of tScheme Stage 1. These documents were the Device Certificate Authority (DCA) SPD, IKI SPD and Organisation Certificate Authority (OCA) SPD.

The SMKI PMA **AGREED** that the DCC link the above documents within the SMKI Repository.

The SMKI PMA also discussed the possibility of having a risk register for the Sub-Committee similar to those published for the SEC Panel.

**ACTION SECPMA 20/13:** SECAS to investigate and produce a Residual Risk Register for the SMKI PMA group at a future meeting.

## 16. Next Meeting

The next meeting will be held on 8<sup>th</sup> March 2016.