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

# SMKI PMA Meeting 52

# SECPMA_52_2011, 20 November 2018

### 10:00 – 13:00, Gemserv Office, 8 Fenchurch Place, London, EC3M 4AJ

# Final Minutes

## Attendees:

| Category | SMKI PMA Members |
|---|---|
| SMKI PMA Chair | Gordon Hextall |
| Technical Architecture and Business Architecture Sub-Committee (TABASC) Representative | Julian Hughes |
| SMKI Specialist | Darren Calam |
| Large Suppliers | Graham Eida |
| Large Suppliers | Fabien Cavenne |
| Electricity Networks | Paul Fitzgerald |
| Gas Networks | Earl Richards |

## Non-Voting Members:

| Category | Attendees |
|---|---|
| DCC | Frederick Wamala |
| BEIS | Daryl Flack |
| SECAS | Hollie McGovern (Meeting Secretary) |
| | Nick Blake |

## Apologies:

| Category | SMKI PMA Members |
|---|---|
| DCC | Paul Wilson |

## 1. Introductions & Matters Arising

The SMKI PMA Chair welcomed the attendees to the November 2018 meeting, noting the running order of the agenda. The Chair welcomed newly elected SMKI PMA Member Earl Richards, who has replaced Sara Neal as the Gas Networks representative.

The following items were discussed under Matters Arising:

**SECMP0042 Update**

The group were provided an update on SECMP0042 'Amendment to SMKI Services to provide DCC Users and/or SMKI Participants with Authorised Responsible Officer (ARO) Statistics and Information', following the SMKI PMA's request at the October 2018 meeting, for DCC to consider a cheaper solution.

It was noted that the DCC have advised that the solution proposed was the best, and only option to be provided by the Service Providers. It was noted that the DCC have requested the post-Pre-Integration Testing (PIT) costs from their Service Providers and have suggested waiting for the costs to be returned before considering the business case. The SMKI PMA Member who raised the modification believed that it would still be worth proceeding with the modification in some capacity, even if it is to request the ARO reports on an ad-hoc basis. The group agreed to wait to receive the post-PIT costs from DCC, and agreed, that if the costs were still too high and the group decide not to pursue the modification, to inform the DCC that it is due to unreasonable costs.

**Network Operator Certificates**

A confidential update was provided on Network Operator Certificates which was discussed at **AMBER**, and therefore recorded in the confidential minutes.

## 2. Draft Minutes of SMKI PMA Meeting 51_1610

The Draft Minutes and Confidential Draft Minutes from the October 2018 SMKI PMA meeting were **AGREED** as written.

## 3. Actions Outstanding

SECAS, the SMKI PMA Chair and DCC provided the Sub-Committee with an update on several actions outstanding from previous SMKI PMA meetings. The following table sets out key items of discussion held during the October 2018 SMKI PMA meeting, specifically:

| Action Reference | Update |
|---|---|
| **SECPMA 51/01** | **SMKI Specialist to undertake a risk assessment to understand the security risks associated with making Device Certificates available to parties that are not regulated under the SEC.**<br>*An update was provided under agenda item 5.*<br>The action was marked as CLOSED**.** |

## 4. SMKI Recovery Scenarios Approval

In June 2018, the SMKI PMA carried out a SMKI PMA Recovery Scenario Exercise, and it was suggested that the exercise be carried out by volunteer Suppliers, who are not as familiar with SMKI,

in order to gain feedback from a more realistic scenario. Following this, the Operations Group were asked to nominate a volunteer, however the SMKI PMA recognised that it would be a non-trivial time commitment for a Supplier representative to attend a SMKI PMA meeting that may last 1/1.5 hours as an agenda item and requested to see some Supplier-specific Recovery scenarios in order to assess the value of Supplier attendance.

At the November 2018 meeting, the SMKI PMA Chair presented the group with the following set of original Supplier related SMKI Recovery Scenarios and the relevant objectives and SEC References, noting that SEC Appendix L provides detailed guidance on the different potential scenarios that could arise:

| | Use Case Description | Objective and SEC References |
|---|---|---|
| 1 | A single User suspects the compromise of their SMKI Organisation Private Key and notifies the DCC but indicates that they will try to use Method 1 to replace their SMKI Organisation Certificates using their own SMKI Private Key and they subsequently manage to successfully replace their SMKI Organisation Certificates. | To test the information flows and processes as in Scenario 2a when the DCC notifies the SMKI PMA as in SEC Appendix L, section 4.2.1.3 and to test the SMKI PMA processes to reach a decision as in SEC Appendix L section 4.2.1.7 and using the SMKI Recovery Key Guidance document. This should provide valuable experience similar to that in Scenario 2a but also about the SMKI PMA decision-making process when authorisation of recovery is refused as in SEC Appendix L section 4.2.2.1 et seq |
| 2 | A single User reports the compromise of their SMKI Organisation Private Key to the DCC and requests the DCC to suspend Devices and invoke recovery. The DCC revokes the affected Organisation Certificates and sets the status to 'Recovery' and seeks confirmation from the SMKI PMA of next steps. The User subsequently finds that there was no actual compromise and reports a 'false alarm' to the DCC requesting connectivity to its Devices to be restored. | To test the information flows and processes arising from Method 2 when the DCC notifies the SMKI PMA as in SEC Appendix L, section 4.2.1.3 and to test the SMKI PMA processes to start to reach a decision as in SEC Appendix L section 4.2.1.7 which is then aborted as a 'false alarm'. This should provide valuable experience similar to that in Scenario 1 but also about the User, DCC and SMKI PMA interaction in the case of a 'false alarm' and where reconnection is carried out as in SEC Appendix L section 4.2.2.1 et seq. |
| 3 | As for Scenario 2 where a single User reports a compromise and asks the DCC to suspend Devices and to invoke recovery and the DCC seeks confirmation from the SMKI PMA of next steps. After due consideration and application of the SMKI Recovery Key Guidance, the SMKI PMA decides not to authorise recovery. | To test the information flows and processes as in Scenario 2a when the DCC notifies the SMKI PMA as in SEC Appendix L, section 4.2.1.3 and to test the SMKI PMA processes to reach a decision as in SEC Appendix L section 4.2.1.7 and using the SMKI Recovery Key Guidance document. This should provide valuable experience similar to that in Scenario 2a but also about the SMKI PMA decision-making process when authorisation of recovery is refused as in SEC Appendix L section 4.2.2.1 et seq |
| 4 | As for Scenario 2 where a single User reports a compromise and asks the DCC to suspend Devices and to invoke recovery and the DCC seeks confirmation from the SMKI PMA of next steps. After due consideration and application of the SMKI Recovery Key Guidance, the SMKI PMA decides that the DCC should invoke recovery. | As for scenario 2a and 2b but to learn from the experience of invoking recovery and implementing the processes in SEC Appendix L sections 4.2.2.2 and 4.2.3.2. |

| | | |
|---|---|---|
| 5 | A Shared Resource Provider and / or multiple Users who are using the same Shared Resource Provider notify the DCC of a suspected compromise of their SMKI Organisation Private Keys which were all stored in the same HSM. Some Users have opted to try Method 1 to recover their Devices but other Users have asked the DCC to suspend Devices and invoke recovery. The DCC reports the incident to the SMKI PMA and seeks confirmation from the SMKI PMA of next steps for those Devices for which recovery has been requested. | To test the information flows and processes arising from Method 1 and 2 when these occur simultaneously and the DCC notifies the SMKI PMA as in SEC Appendix L, section 4.2.1.3 and to test the SMKI PMA processes to reach a decision as in SEC Appendix L section 4.2.1.7. This should provide valuable experience of the potential range of scenarios that might occur with a Shared Resource Provider. |
| 6 | Ofgem inform the DCC (and / or the SMKI PMA) that a Supplier has ceased trading in an unmanaged manner and the SMKI Organisation Private Key (in a HSM in a Third Party datacentre) has been retained by the Third Party to whom debts are owed. Ofgem will shortly appoint a Supplier of Last Resort (SoLR). | Not documented in SEC but would be similar to Scenario 4. |

A Member requested an additional scenario to be included which covers the loss of the whole of the Hardware Security Modules (HSM) and all of the keys.

The group discussed the best way to undertake the scenarios with volunteers; it was noted that it was not practical to invite volunteers to a SMKI PMA meeting for only an hour, and it was suggested that a separate session should take place on 15 January 2019 to run through the scenarios. It was agreed that Operations Group Members would be invited to attend, and that the scenarios would be sent to attendees in advance of the session.

The group also discussed whether it would recover a Pre-Payment Meter Interface Device (PPMID), since it has a recovery certificate.

The SMKI PMA considered a table set out in SEC Appendix L (section 1.2) which shows the Public Key Certificates/Kays covered by the SMKI Recovery Procedure. It was noted that the recovery of a PPMID would therefore be appropriate in the event of a Compromise to:

- Root Organisation Certificate Access (OCA) Key;
- Recovery Key;
- AccessControlBroker (ACB) Key (Digital Signature); and
- ACB Key (Key Agreement Key).

It was therefore noted that Recovery would only be requested by the DCC, and not a Supplier.

A Member queried why the above certificates are put onto PPMIDs; it was confirmed that this is to establish the relationship with the other Devices on the HAN. It was noted that if the meter were to fail, the meter would need to be swapped and a rejoin would need to be undertaken; a Root OCA Key would be required to validate the Device and the DCC would then trigger the recovery.

The SMKI PMA queried whether a PPMID has a commissioned status; it was confirmed that In Home Devices (IHD) and Consumer Access Devices (CAD) are not commissioned but PPMIDs are. The SMKI PMA requested the DCC to confirm whether testing has been undertaken/will be undertaken to show whether a PPMID can be recovered.

The SMKI PMA:

- **NOTED** the SMKI Recovery Scenarios;
- **AGREED** that a separate session would be required to undertake the scenarios with volunteer Suppliers; and
- **AGREED** that it is appropriate to recover a PPMID Device as part of a wider SMKI Recovery Event involving ESME and GSME Devices (SEC Appendix L Section 1.2 relates).

**SECPMA 52/01:** The SSC Chair to invite Operations Group Members to attend a SMKI Recovery Scenarios workshop and to send the scenarios in advance to the attendees.
**SECPMA 52/02:** DCC to confirm whether testing has been undertaken/will be undertaken to show whether a PPMID can be recovered.

## 5. Device Certificates Risk Assessment (RED)

Following on from an issue that was raised at the September 2018 Panel meeting, which relates to obtaining Device Certificates via the SMKI Portal via the Internet (SPOTI), the SMKI PMA considered the security risks associated with making Device Certificates available to parties that are not regulated under the SEC. The agenda item was marked as **RED** and therefore recorded in the confidential minutes.

The SMKI PMA **AGREED** to advise the DCC on its use of SPOTI.

## 6. Dual use of SPOTI and DCC Gateway by a single Party

The SMKI PMA considered whether a User should be able to access both SPOTI and the DCC gateway, and whether to restrict Users to the DCC gateway as a more secure means of obtaining SMKI Certificates. The discussion was classified as **RED** and therefore recorded in the confidential minutes.

The SMKI PMA AGREED that the same advice regarding SPOTI would apply to dual use of SPOTI and DCC Gateway by a single party.

The SMKI PMA **NOTED** the update.

## 7. 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:

### 7.1 SMKI Operational Update

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

### 7.2 DCC Update

The SMKI PMA **NOTED** there was no DCC update.

### 7.3 DCCKI PMA Functions Update

The SMKI PMA **NOTED** there was no update relating to the DCCKI PMA.

### 7.4 BEIS Update

A Member queried the addition of two role party codes in relation to the BEIS consultation on regulatory changes relating to the provision of a DCC SMETS1 Service, which was issued on 5 November 2018. It was noted that Section 7.11 of the consultation proposes minor amendments to SEC Section L to include new Remote Party Role Codes for the Commissioning Party, Requesting Party and S1SP (SMETS1 Service Providers) in relation to the migration of SMETS1 meters into the DCC under the process set out in Transition and Migration Approach Document (TMAD). It was noted that this had previously been presented to the SMKI PMA by the DCC.

## Any Other Business (AOB)

A SMKI PMA Member asked about arrangements for proving SMKI Recovery in the Live Environment. The discussion was classified as **RED** and therefore recorded in the confidential minutes.

The SMKI PMA **AGREED** to defer the December SMKI PMA meeting to 15 January 2019 noting that there were not enough agenda items to make a December meeting feasible.

There were no other items of AOB and the Chair closed the meeting.

**Next Meeting: 15 January 2018**