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).

Meeting SECPMA_30_1312, 13th December 2016

10:00 – 13:00

Gemserv, 8 Fenchurch Place, London, EC3M 4AJ

SMKI PMA Final Minutes

Attendees:

Category	SMKI PMA Members
SMKI PMA Chair	Gordon Hextall
Large Suppliers	Geoff Huckerby
	Fabien Cavenne
Small Supplier	Victoria Patrick
Networks	Sara Neal (Part)
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
SMKI Specialist	Darren Calam (Part)
SMKI PMA Secretary (SECAS)	Joe Davenport

Apologies:

Category	Attendees
SECPMA_30_1312 - Typings.docx	Marc Avery (but was available by telephone)
The Authority (Ofgem)	Gwen Cruise

Introductions

The SMKI Chair welcomed Victoria Patrick as a new SMKI PMA member representing Small Supplier Parties and introduced the other members of the SMKI PMA.

1. Minutes of SMKI PMA Meeting 29_0811

There were no comments received, and the minutes were **APPROVED** as an accurate representation and record of the November 2016 SMKI PMA 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 discussion points of **ONGOING** actions held during the December 2016 meeting, specifically:

Action Reference	Update
SECPMA 25/01	**The DCC have confirmed the cost of running 'Method 1' for a single Recovery Event, however, costing information from the Data Services Provider (DSP) to determine the costs associated with running Recovery Events for 'Methods 2 and 3' are still to be received.** The DCC advised that cost assumptions would be provided in advance of the SMKI Recovery Desktop Exercise workshop (to be held early 2017). The action was marked as **ONGOING**.
SECPMA 26/06	**The Trusted Service Provider (TSP) will investigate reducing the proposed maximum 24-month window and the associated costs and overheads for necessary downtime.** The Department for Business, Energy and Industry Strategy (BEIS) confirmed a meeting was being held on Thursday, 15th December 2016 to consider the DCC responses to questions posed by the National Cyber Security Centre (NCSC). The SMKI PMA Chair advised that the invite will be sent to the DCC and TSP. The action was marked as **ONGOING**.
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.** SECAS uploaded the flow diagram to Egress and made this available to SMKI PMA members. This action is now **CLOSED**.
SECPMA 27/13	**The SMKI PMA advised that action and corrective plan papers will be required in order to have an audit trail for how the DCC/TSP wish to progress and resolve the issue relating to the Apex Contingency Key in UIT. The DCC agreed to provide information on this to the SMKI PMA as the corrective actions develop.**

Action Reference	Update
	The DCC advised that the Release 1.3 (R1.3) approach would mean the current Certificate Authority (CA) is rolled over and no longer present. Further details will be explored and provided in advance of the desktop exercise (early 2017). The action was marked as **ONGOING**.
SECPMA 27/15	**The DCC Security Team will hold additional conversations with their internal test team to see whether they can facilitate an additional test to include the transition over an additional Certificate Authority (CA) hierarchy.** The DCC advised that use cases above and beyond the standard recovery were currently being developed and this would be rolled out across a number of test cases. The SMKI PMA questioned the additional testing being constructed and whether it was being applied to the transition of the new CA hierarchy. The DCC advised that this is being undertaken as part of CR101 (DSP environment to Support SMKI Recovery Procedure) testing by the DCC. It was also noted that there was no reliability on Parities to conduct this testing. This action is now **CLOSED**.
SECPMA 27/17	**The DCC will review how SMKI Users are currently being notified of their obligation to inform the DCC when an ARO, or SRO, leaves a company. The DCC will also investigate enhancing its ARO and SRO forms to remind SMKI Users of their roles and obligations in these roles.** The DCC confirmed that a quarterly report is available to Suppliers in their 'SMKI Live' section of the DCC SharePoint site. SMKI PMA members made a number of comments in relation to the reliability of the information, and the DCC advised they will confirm how often this is updated and whether it fulfils the requirements previously requested by the SMKI PMA. The action was marked as **ONGOING**.
SECPMA 28/03	**In relation to liability in the event of a Recovery Event involving Communication Hubs, the DCC agreed to discuss this further with their internal legal team to understand cases and instances where the CSP do and do not pay.** The DCC advised this action was still pending whilst they wait for legal confirmation. The DCCs internal legal team are not clear where liability rests unless blame is apportioned and legal attribution is associated. The DCC determined and informed the SMKI PMA that it is likely to spread this cost across industry. SMKI PMA Members noted their concern at this standpoint, and questioned why industry was responsible for meeting the costs, noting this view would be seen as unjustifiable to wider User audiences outside of the SMKI PMA. The DCC advised that they would seek further information from their legal team. The SMKI PMA Chair advised there is a risk that this query is not resolved prior to full live services where this situation could potentially occur and noted that the SMKI PMA could take its own legal advice but the cost of this ought not to be necessary in such a clear cut scenario. The action was marked as **ONGOING.**

Action Reference	Update
SECPMA 28/04	**Minutes, actions and any other relevant documentation from the 3rd October 2016 workshop will be circulated to SMKI PMA Members in order to close actions from SECPMA 26/03 to SECPMA 26/07.** Materials had been made available to SMKI PMA members prior to the meeting. It was advised that this no longer closes the associated actions due to developments of the actions themselves. This action is now **CLOSED**.
SECPMA 28/05	**In relation to the 3rd October 2016 workshop; SECAS will approach CESG to determine if the outcomes of the meeting are appropriate, and fit within the original scope for delivery of the SMKI Service with particular respect to the Device Certificate Authorities (DCA).** As previously noted, a meeting was scheduled for Thursday, 15th December 2016. Information will be fed back to the SMKI PMA at their next meeting. The action was marked as **ONGOING.**
SECPMA 28/09	**The DCC will publish the Stage 1 Assurance Report and Stage 2 Assurance Report on the SMKI Repository and DCC SharePoint site.** These reports have now been made available on the DCC Operational SharePoint site. SECAS also requested the latest versions for publication on the SEC Website. This action is now **CLOSED**.
SECPMA 28/11	**SECAS will include a Process Flow Diagram to the Confidential supporting document prior to the November 2016 meeting.** As per previous updates, this action will be concluded after the SMKI Recovery Desktop Exercise Workshop (to be held early 2017). The action as marked as **ONGOING**.
SECPMA 28/14	**SMKI PMA Members are requested to raise any other escalation points and suggest any other factors they wish to have included within the SMKI Recovery Key Guidance supporting confidential document.** As per previous updates, this action will be concluded after the SMKI Recovery Desktop Exercise Workshop (to be held early 2017). The action as marked as **ONGOING**.
SECPMA 29/02	**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.** The TSP has confirmed to the DCC that they are looking at a UK mainland location. The location under consideration has the correct level of controls and removes the requirement of a flight to collect the Hardware Security Module (HSM). The DCC requested that the SMKI PMA confirm their support for the Change Request (CR) required to relocate the HSM. The SMKI PMA confirmed that there was initially a risk with the location of the backup HSM being so close to the original HSM. The SMKI PMA confirmed that relocating the HSM would, as a result, reduce the associated risk. An additional

Action Reference	Update
	third HSM should then be created prior to the Key Ceremony scheduled for February 2017. The SMKI PMA provided their support for this change, but noted that they are not approving the cost of this exercise (and only the DCC proposal to reduce the risk). The SMKI PMA position is that the DCC proposal is a sensible risk mitigation. Any updates will be provided to the SMKI PMA at future meetings. This action is now **CLOSED**.
SECPMA 29/04	**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 long-term solution prior to either a Modification Proposal or Section 88 change being made to DUIS.** It was advised that there was no appetite between Energy Network Association (ENA) Members to introduce a naming convention at this time. The SMKI PMA were informed that ENA Members were confident in their current bilateral agreements in place with Suppliers. As a result, no identifiers were being utilised within the Certificates. SMKI PMA Members noted their concern that there was no appetite from Network Operators to mitigate this issue. It was noted that this will not evolve into a solution, and will instead develop into a growing issue as the SMKI Repository continues to grow through normal Business as Usual (BAU) processes. As a result, the SMKI PMA noted that this may have to be enforced in future as the programme increases in size and smart meters are rolled out. It was advised that naming conventions should be implemented as this is good practice. In relation to the proposed change to be made to the DCC User Interface Specification (DUIS), the BEIS representative noted they are reluctant to make this change via Section 88 powers. It was noted that a SEC Section X5 change would not be suitable for this, and advised raising a SEC modification to amend DUIS. BEIS advised the SMKI PMA that DUIS is correctly worded and was there to provide good crypto practice however, there is currently no good guidance for using the correct Certificate which could therefore result in industry using the wrong Certificate. In order to rectify this, DNOs would need to use their certificates for the wrong purpose thereby putting them in breach of the SEC. In relation to the proposed change to be made to the DCC User Interface Specification (DUIS), the BEIS representative noted they a Section X5 change would be required rather than Section 88 powers. BEIS therefore advised that the party that initiated this query should raise a SEC modification to amend DUIS. ~~BEIS advised the SMKI PMA that DUIS is not necessarily wrong, but there is currently no good guidance for using the correct Certificate and this may be interpreted in a variety of ways, therefore, resulting in industry using the wrong Certificate.~~ This action is now ~~**CLOSED**~~**ONGOING**.

Action Reference	Update
SECPMA 29/08	**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.** This documentation had now been made available to SMKI PMA Members. The SMKI PMA Chair questioned the reference to DX/0535 within the documentation. The DCC confirmed that all the procedural documents begin with this reference statement. SMKI PMA queried the 'DCCKI III' CA. The DCC confirmed that this was the Internal Infrastructure Issuing Certificate Authority (III CA), and does not fall under the DCCKI Certificate Policy (CP). The DCCKI III CA has its own CP that is based off of the DCCKI CP. This action is now **CLOSED**.

ACTION SECPMA 30/01: As a result of the closure of action *SECPMA_27/15*, the DCC will provide feedback to the SMKI PMA on the testing being undertaken for CR101.

ACTION SECPMA 30/02: SECAS to raise the risk of a Recovery Event involving Communication Hubs on the SMKI PMA Risk Register.

ACTION SECPMA 30/03: The DCC to provide the latest versions of the Assurance scheme documentation to be published on the SEC Website.

ACTION SECPMA 30/04: The SMKI PMA will respond to the DNOs via the ENA to raise the reasons behind establishing a naming convention and why this is in their best interest.

ACTION SECPMA 30/05: The DCC to produce a guidance note and distribute this through the DCCs Design Release Forum. This will be investigated together with the TABASC representative.

ACTION SECPMA 30/06: The SMKI PMA will go back to the originator, via the ENA, about the issue to inform them of the ongoing developments. It is likely that a change to the DUIS will require a modification being raised.

ACTION SECPMA 30/07: The DCC to provide an action update a week prior to each meeting of the SMKI PMA forthwith**.**

3. SMKI Recovery Desktop Exercise – Draft Use Cases

The SMKI PMA Chair advised that he had distributed the Terms of Reference (ToR) for the SMKI Recovery Desktop Exercise prior to the meeting.

The DCC presented outline slides on the draft use cases as an approach to the SMKI Recovery Desktop Exercise workshop and listed actions to be considered by the SMKI PMA. The slides listed recovery scenarios that summarised those listed in the ToR.

The SMKI PMA Chair noted the deliverables in the ToR and advised of the updates that the DCC would need to provide in a typical recovery event. The DCC advised that 'real time' factors are not fed back to the DCC. The SMKI PMA Chair advised that these updates would need to be fed back to the SMKI PMA and questioned the importance of understanding what the DCC would be asking the SMKI PMA during a recovery event.

It was advised that a real time update of where the Recovery Key fails would be useful to see and where the DCC would have to use the Apex Contingency Key. The DCC advised this would only be utilised where the SMKI Root itself had been Compromised. The SMKI PMA reiterated the importance

of being able to witness, and be privy to, the processes surrounding these possible recovery scenarios.

The SMKI PMA advised that they would require information on how long it would take to implement recovery and this information should be fed back to the SMKI PMA. The DCC advised that they would be able to gauge this kind of information from CR101 testing. The DCC advised that for each recovery event, the SMKI PMA would have to define what the expectation of the updates would be (for example, on a daily or weekly basis) and the DCC would respond to that request.

Questions were raised over Transitional Change of Supply (TCOS) process and whether recovery would be undertaken if TCOS was in place. It was advised there is currently no scenario where TCOS is being used and recovery is invoked, for example, if there was an issue with the Certificates being used.

The DCC noted that the design of the system should be able to cope with the throughput of recovery and assurance would be provided through test events being undertaken as a part of CR101. However, the DCC advised that load testing had not yet occurred. The DCC advised that the SMKI PMA needs to be aware that the packets needing to be sent as part of recovery are large. Because of this, the actual Devices themselves can take a long time to recover (it was noted some Devices can take over two minutes to change a single Certificate).

The DCC queried whether any recovery event would run in parallel with a Major Security Incident. SMKI PMA Members were advised that, whilst there will need to be some collaboration and consultation between the SSC and the SMKI PMA (in relation to a SMKI Recovery Event being reported as a Major Security Incident), it is the SMKI PMA rather than the SSC that has responsibility for decision-making. The DCC raised the point that an attack during a SMKI Recovery Event may be a time at which someone tries to compromise the DCC Total System. The SMKI PMA advised that this would be handled by collaboration between the two sub-committees.

The DCC highlighted that if the wrong Devices were being recovered, then there must be a method for notifying a governance body (such as the SMKI PMA) that these meters are being recovered erroneously. The DCC raised this as a ‘false alarm’ scenario. The DCC noted that this would be dependent at what stage it is realised that a ‘false alarm’ has been raised, if this is during the initial stages then the scenario would end with SMKI PMA ‘rejects recovery’.

The DCC advised that where multiple users are involved, there would be multiple determining factors, such as timescales and resolution factors (recovered proportion). The DCC noted that an HSM impact may affect all users of a service. In a situation where there is a Shared Service Provider (SSP), it may be necessary to engage recovery for all those on the shared services. The DCC and the SMKI PMA were reminded that they would need to assess the overall impact of this scenario. In this situation, it would likely be the SSP that reports the Compromise to the DCC rather than the Small Supplier they manage.

For the SMKI Recovery Desktop Exercise, the DCC advised they would be considering the Apex Contingency Key scenario last. The SMKI PMA advised there are a lot of scenarios within the Apex Contingency Key scenario itself which should be considered. The DCC advised they would investigate up to three of these scenarios for the workshop. SMKI PMA Members recommended that a large amount of focus and effort be put into these types of scenarios due to the urgency and importance of an event of this nature.

Discussions were held around what happens internally at the DCC where a customer calls in to inform them of a Compromise (or suspected Compromise). The SMKI PMA noted that the DCC would follow the processes associated with a Major Incident prior to initiating the SMKI Recovery Procedure processes. The SMKI PMA questioned whether guidance was being utilised to see whether the DCC

believe that recovery should be used before taking it to the SMKI PMA for decision. SMKI PMA Members noted that if the SMKI PMA were not getting the correct information, then making appropriate decisions may be difficult (as the SMKI PMA will need to be made aware of why a Major Incident requires a SMKI Recovery Event).

SMKI PMA advised that their current expectation is for the DCC to be asking the Supplier why an associated recovery method has not been requested, what the Supplier has done to resolve the situation and no longer be Compromised (or suspected of being Compromised), and try to gather as much evidence and information as possible to understand if processes and changes may subsequently be required to the SEC. It was noted that it might not necessary be for the SMKI PMA to review all of this information, and that the DCC may suggest amendments to the SEC within their remit of suggesting SEC modifications (where appropriate). SMKI PMA Members suggested this should all be defined within a process script in order to gather the same information every time (which the SMKI PMA may want to see to support decision-making).

The SMKI PMA reiterated they wish to know what the DCC will bring to the SMKI Recovery Desktop Exercise and whether it will work in an actual recovery situation in order for the SMKI PMA to discharge its obligations in relation to using the SMKI Recovery Key Guidance.

The SMKI PMA **NOTED** the SMKI Recovery Desktop Exercise – Draft Use Cases update.

ACTION SECPMA 30/08: The DCC are to review the ToR, SMKI Recovery Key Guidance, and any other related internal documentation in order to bring a fully developed plan and examples to the SMKI Recovery Desktop Exercise workshop.

ACTION SECPMA 30/09: The DCC will confirm to SECAS the dates for the Recovery Workshop and whether this needs to be pushed back from the original planned date of 10th January 2017.

4. SMKI Recovery – DCC R1.3 Approach

The SMKI PMA Chair had requested further information from the DCC on their approach to the delivery of the SMKI recovery environment for R1.3 now that the consultation has closed. The DCC provided further detail on how this would be tested within Systems Integration Testing (SIT) and within the User Interface Testing (UIT) environment.

The DCC advised that testing will be focussing on recovery in SIT where there are two SMKI hierarchies, and that multiple SIT cases will be undertaken first. The SMKI PMA were informed that the Apex Contingency Key scenario would be tested last due to its destructive impact, with all other recovery scenarios being undertaken before this. The SMKI PMA were informed that the last Apex Contingency Key use-case is classified as complete when the Organisation Certificate Authority (OCA) 3 rolls over to OCA 4.

BEIS questioned why this was not tested in UIT before going live. The DCC informed SMKI PMA Members that this will act as an actual Apex Recovery Key event on OCA 3, and will cause issues with SIT functionality if tested in the UIT environment.

The DCC advised the SMKI PMA that the SMKI recovery environment does not go live at the same time R1.3 goes live and is instead delivered the month after R1.3. The DCC confirmed that if the contingency is used for R1.3, then this will have an effect on the delivery of the SMKI recovery environment.

As with previous SMKI milestones, the SMKI PMA expect the SEC Panel to ask for their advice in respect of the SMKI Recovery testing progress and associated governance requirements. This will include the development and approval of the updated SMKI and Repository Testing Approach (SRT) Document, which will include SRT Part 3 (as described in the latest SRT Approach Document

approved on 8 March 2016) and regular testing updates. DCC acknowledged that an updated SRT Approach Document would need to be provided to the SMKI PMA.

The SMKI PMA **NOTED** the DCC's SMKI Recovery – DCC R1.3 approach.

ACTION SECPMA 30/10: The DCC to provide the SMKI PMA with an updated SRTA.

5. SMKI Operational Update

The DCC presented slides to the SMKI PMA that related to operations during November 2016. The DCC advised that the monthly reports are still being provided to the SEC Panel for Certificate Signing Request (CSR) Forecasts, the issuance of Certificates, and any raised tickets.

The SMKI PMA Chair required that these reports are also shared with the SMKI PMA as well as the SEC Panel to enable the SMKI PMA to meet its obligations under SEC L1.10 (n).

SECAS noted that these would have to come from the DCC directly due to the Panel Information Policy (PIP) markings on the papers restricting these from being copied from the SEC Panel papers.

The SMKI PMA **NOTED** the SMKI Operational update provided by the DCC.

ACTION SECPMA 30/11: The DCC to ensure that any reports relating to SMKI Operations are distributed to SMKI PMA members as well as the SEC Panel.

6. DCC Update

The DCC provided the SMKI PMA with an update on the issues that affected the first batch of Communication Hubs. The DCC informed the group that during the manufacturing cycle, the SMKI Certificate files had become truncated and therefore could not be authenticated. The SMKI PMA were informed that these had now all been recalled to the manufacturer. The DCC advised that they were now implementing 'Production Proving' to ensure this issue is not repeated, and that this issue would be assessed and discussed by the SSC.

BEIS questioned whether this affects the assurance of the Communication Hubs. BEIS further noted that SEC Parties will have no proof that the Recovery Keys will work where they are manually injected into Devices. The DCC noted that CR109[1] testing proves the cryptographic material is sound and is therefore not in question, and that the issue is during the manufacturing process and whether the Certificate is still valid after production and injection. The DCC informed the group that during 'Production Proving' this will be validated against the SMKI production chain once the Device is enrolled

The DCC noted this is a locked down Device, and therefore the only way to test it is to send it a live Critical Command. The DCC informed the SMKI PMA that they will test Commissioned Devices to ensure the Certificates have been correctly injected onto the Devices once they are enrolled. It was noted that this is the only method possible to assess whether the Certificates have been truncated at this stage.

The SMKI PMA highlighted that this is an issue with the way in which Secret Key Material has been managed, and should be an area of discussion at a future SMKI PMA meeting surrounding assurance and obligations.

The SMKI PMA **NOTED** the DCC update for November 2016.

[1] CR109 – SMKI keys for RDP file signing

ACTION SECPMA 30/12: The SMKI PMA will hold discussions on the management of SMKI Key Material as a result of the Communications Hub issue at a future SMKI PMA meeting.

7. Emergency Suspension of SMKI Services – Update

An update was provided on the SSC's considerations regarding the suspension of SMKI Services following the SMKI PMA request for their views.

The SSC considered that the emergency suspension of SMKI Services should be included within the scope of the Joint Industry Cyber Security Incident Management Plan (JICSIMP), and may be a future security incident that will be factored and considered by the Smart Metering Issue Response Team (SMIRT).

The SMKI PMA **NOTED** the Emergency Suspension of SMKI Services update.

8. 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. An additional risk had also been added to the register as a result of the work being undertaken by the BEIS Smart Metering Issue Resolution Forum (SMIRF) and would continue to be monitored.

The SMKI PMA **NOTED** the Risk Register Update for December 2016.

9. SMKI PMA Activity Planner

SECAS provided the SMKI PMA with an updated activity planner outlining the activities expected over the next three months. SECAS advised that the traceability of the updated SRT Approach document had been added to Appendix A.

The SMKI PMA **NOTED** the Activity Planner for December 2016.

10. Modifications Status Report

SECAS informed the SMKI PMA that the modification for increasing the voting SMKI PMA Members and removing the restrictions on Alternates from the same company had now been approved and would take effect from Wednesday, 14th December 2016. SECAS would undertake the necessary election processes following this modification being implemented.

The SMKI PMA **NOTED** the Modifications Status update for December 2016.

ACTION SECPMA 30/13: SECAS to begin the election process for the new roles created by the acceptance and implementation of the SMKI PMA membership modification.

ACTION SECPMA 30/14: SECAS to circulate the alternate notification forms to SMKI PMA members as a result of the acceptance and implementation of the SMKI PMA membership modification.

11. DCCKI PMA Functions Update

The DCC advised that the DCCKI PMA minutes have now been circulated to SMKI PMA members. The SMKI PMA were informed that the next meeting of the DCCKI PMA Function will be focused on the audit activity.

The SMKI PMA **NOTED** the DCCKI PMA Functions update for December 2016.

12. BEIS Update

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

The SMKI PMA **NOTED** the BEIS update for December 2016.

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

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

Next Meeting

The SMKI Recovery Desktop Exercise workshop on **Tuesday, 10th January 2017** has been **POSTPONED** and a new date will be confirmed as soon as possible.

The next meeting of the SMKI PMA will be held on **Tuesday, 17th January 2017**.