This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Paper Reference:	**SECP_74_1511_26**
Action:	**For Information**

SEC Panel Sub-Committee Report

1. Purpose

This paper provides the Panel with an update on recent activities from the Panel Sub-Committees. It highlights the key issues discussed and details specific points the Sub-Committees would like to bring to the Panel's attention. The Panel is requested to note the updates.

2. Operations Group

2.1 Operations Group Meeting Highlights

The Operations Group (OPSG) has now scheduled an additional meeting each month at which the SEC Panel reports delegated to OPSG by Panel are discussed. Both meetings are reported in this section.

Release Governance

OPSG has considered the DCC's statements of readiness for the next step in SMETS1 migration and the November 2019 Release. The recommendations to Panel for these Releases are set out in SECP_74_1511_06 and SECP_74_1511_22 respectively.

Communications Hubs Returns

In response to a request from OPSG, at the July meeting the Panel requested that the DCC:

1. urgently host a workshop with its Customers to identify immediate improvements.
2. urgently develop a Communications Hub (CH) bulk returns process.

Following the CH Order Management System workshop in October, a further workshop has been scheduled for 18 November to gather requirements and explore options for a bulk returns process.

Communications Hubs and Other Exceptions

Following a meeting with SECAS in October, the DCC has produced an analysis of the CH Exceptions and confirmed that there are four main categories of exceptions. The next phase of the work is to engage with Service Users to explore what is happening during the installation process when these exceptions are generated. The DCC requested OPSG to encourage Users to support this work. A more detailed update is scheduled for the December meeting.

Alerts

There has been some progress with addressing the number of rogue alerts, but they continue at a very high level. The OPSG agreed to support the DCC by encouraging Service Users to take all

reasonable steps to reduce the number of Device Alerts being generated. The DCC agreed to produce guidance on how to avoid the production of superfluous Alerts. It was agreed that the Device Alerts issue would be added to the OPSG Risk Register.

Service Performance

The OPSG continues to be concerned by the reliability of the DCC Services. The OPSG noted in particular that recent incidents had impacted Install and Commission.

The OPSG acknowledged the strenuous efforts being made to improve reliability but noted that these have not yet achieved the desired outcome.

The August Performance Measurement Report (PMR) includes SMETS1 metrics; the addition of these will need to be aligned with SEC requirements for adding metrics to the PMR.

Code Performance Measure 1 was again below target. The DCC presented a plan of the actions being taken by CSP N and CSP C&S to get this measure above target by December.

OPSG members reported that the metrics for CSP N did not reflect the issues being experienced in the region, with around 1 in 6 installations failing and a significantly longer installation time than in CSP C&S. The DCC will investigate and report back to the December meeting.

Service Request Forecasting

The DCC reported that 15 Users are submitting Certificate Signing Requests and 14 Users are submitting Service Requests without having submitted the relevant forecasts. The same Large Supplier appears in both of these categories. OPSG members continue to raise questions as to whether the administrative process for dealing with these forecasts is correct, and SECAS is addressing this with DCC.

SSI Improvements

The OPSG approved the package of Service Improvement Proposals (SIPs), noting that some of these may be relevant to DP083: 'Change Coordination'. The OPSG asked both SECAS and DCC (as the modification Proposer) to communicate this work on requirements to the Modification Working Group, the aim being to avoid duplication.

Operational Metrics Project

The Operational Metrics Project is now fully staffed. The key contact has been nominated by the DCC who has now joined the team. Communication to Stakeholders has commenced and a survey will be issued to Users during November.

3. Security Sub-Committee and SMKI PMA

Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) set no Assurance statuses in October 2019.

3.2 Verification Assessments

As part of its wider obligations, the SSC review the outcomes of Verification User Security Assessments. If the SSC believe that a User is non-compliant, or potentially non-compliant, with obligations contained in SEC Sections G3-G6, then it will notify the Panel.

During October 2019, the SSC reviewed two Verification User Security Assessments (VUSAs) in which Compliance Statuses were agreed. Details of the VUSAs can be found in confidential Appendix A.

3.3 Director's Letters

The SSC reviewed one Full User Security Assessment (FUSA) Director's Letter and two VUSA Director's Letter in October 2019, all of which were approved, and details can be found in confidential Appendix A.

3.4 Security Self-Assessments

One Security Self-Assessment was reviewed by the SSC in October 2019, the outcome of which can be found in confidential Appendix A.

3.5 SSC Highlights

DP091 'Updating Security Assurance Status'

The SSC Chair raised a Problem Statement for DP091 'Updating Security Assurance Status' which identifies that the wording of the Security Assessment assurance status terminology set out in SEC Sections G8.36 – G8.37 does not reflect the substantial remediation that is required for 'Provisionally approved' and 'Deferred'. It is proposed that the terminology is amended to 'Deferred' and 'Rejected' respectively. It has now been raised as a Draft Modification and was discussed at the Change Sub-Committee on 29 October 2019, with a recommendation to be presented at the November Panel meeting for conversion to a full Modification Proposal.

Use Case Proposal for Factory Reset

The SSC agreed to take the Commercial Product Assurance (CPA) Use Case for Factory Reset to the SSC CPA Working Group on 6 November 2019. The Use Case was raised by Jeff Studholme on behalf of the Community of Meter Asset Providers (CMAP) as a potential solution to allow Meter Asset Providers (MAPs) to perform a factory reset on SMETS2 meters. The solution proposes the affected meter connects via an external port to a software solution which would securely connect to the meter manufacturer site, and the latest firmware and appropriate security keys would then be applied to the meter, which can then be re-issued for installation as though it were a new meter.

Central Switching Service (CSS)

The SSC reviewed proposals from the DCC for security controls associated with CSS, and subsequently provided advice on setting Anomaly Detection Thresholds to ensure the integrity of Registration Data.

SMETS1 Enrolment & Adoption

The SSC has monitored DCC progress in remediating outstanding actions from the first Eligible Products Combination List (EPCL) in July 2019 and in preparing to make a recommendation to the Panel on the Live Service Criteria for the next Device Model Combination.

Anomaly Detection Values

The DCC sought SSC approval for changes to a range of Anomaly Detection Values which are no longer realistic. SSC members are considering the operational implications of the proposals before giving approval, as required by the SEC.

3.6 SMKI PMA Highlights

SECMP0063 'Ensuring correct Network Operator Certificates are place on Electricity Smart Meters'

The SMKI PMA agreed that the current proposed solution to SECMP0063 'Ensuring correct Network Operator Certificates are place on Electricity Smart Meters' does not present a viable business case and agreed an alternative solution should be investigated.

The SMKI PMA also agreed to consider guidance to the Distribution Network Operators (DNOs) on configuring their gateways to replace incorrect Network Certificates.

SECPMA Standards and Guidance Review

The SMKI PMA noted the changes to Standards and Guidance quoted in the SEC, relating to the SMKI Service and the SMKI Document Set, following the annual review.

The SMKI PMA has since reviewed the changes, and the updated Standards and Guidance was published by SECAS on 1 November 2019.

SEC Appendix L

The SMKI PMA is collaborating with BEIS to prepare amendments to SEC Appendix L Section 6, to reflect changes that have been implemented in GBCS and IRP 555.

SMKI Recovery

The SMKI PMA reviewed a 'Lessons Learned' report from a SMKI Recovery Exercise that was conducted in the summer, to consider whether any changes are required to the SEC or to the SMKI Recovery Guidance Document.

PKI Proposals for SMETS1 and CSS

The SMKI PMA has reviewed proposals from the DCC and provided advice on proposals for the use of new Public Key Infrastructures (PKI) for SMETS1 Middle Operating Capability (MOC), SMETS1 Final Operating Capability (FOC), and CSS.

4. Technical Architecture and Business Architecture Sub-Committee (TABASC) and Testing Advisory Group (TAG)

4.1 TABASC Highlights

CSS Interface Code of Connection

The DCC provided an update to the TABASC regarding the CSS Code of Connection, highlighting that there are three network access options (internet, Private Network, or a Switching Adaptor solution) available for connecting Users and the DCC to a Central Switching Solution, which will enable faster switching.

DCC Change Co-ordination pilot project

The DCC provided an update on the DCC Change Co-ordination pilot project, highlighting how the risk assessment works and the factors influencing the heatmap risk status. A scoring system is proposed, which is based on whether it is core service or customer affecting, as well as taking into consideration the complexity and the downtime required. The scores are used to calculate a risk score, which reflects a Red Amber Green (RAG) status in the heatmap.

The TABASC raised some concerns with the classification of some changes which may have an unnecessarily detrimental effect on change progression and requested that the DCC provide specific examples in November for further discussion.

SECMP0062 'Northbound Application Traffic Management – Alert Storm Protection' Update

The DCC provided an overview of the Modification Proposal, noting that the proposed solution is to provide Alert Storm protection using a mechanism that consolidates excess Alerts from any Device if threshold volumes are exceeded for a period of time.

The TABASC are continuing to provide feedback on the modification including suggesting additional notification during times of traffic management and also for DCC to further consider implementing the modification as a single stage to minimise the effect on Users. The TABASC requested formalised details of the technical solution and the process of its operation be provided. Similarly, the DCC will provide an update on SECMP0067 'Service Request Traffic Management' in November for the TABASC to consider and provide feedback on.

Non GBCS Non-Mandated Alerts (NGNM) register

The TABASC were provided with an overview of the process for the management of Non-GBCS-Non-Mandated Alerts. The TABASC agreed the process for adding Alerts to the 'Non GBCS Non-Mandated Alerts Register'.

4.2 TAG Highlights

The TAG has met three times during this reporting period. The additional meetings have been necessary to address issues relating to the forthcoming decisions relating to the November 2019 SEC Release and the next SMETS1 Device Model Combinations (DMCs) to be added to the EPCL. A brief overview of each meeting and its outcome is provided below.

TAG 59X – 10 October

This was an extraordinary meeting convened with the intention of approving three testing approach breadth and depth documents:

- The SMETS1 IOC Honeywell Elster SRVT Depth and Breadth document was not approved, pending clarification of some details, including whether the User Role of Export Supplier would be included in the scope of testing.
- The SMETS1 MOC MDS Regression Depth and Breadth Elster Dormant Active Mixed was not approved pending the inclusion of additional scenarios in the document.
- The SMETS1 IOC Regression Depth and Breadth Elster Dormant Active Mixed and Itron Active Mixed was not approved pending minor changes.

Additionally, the DCC provided the TAG with an update on Change Request CR1066, which relates to the unapproved Modification Proposal SECMP0062 'Northbound Application Traffic Management – Alert Storm Protection', whereby CR1066 had been 'switched on' throughout testing and needed to be tested. DCC confirmed that CR1066 will be 'switched off' in production for November 19. The TAG requested further information and agreed to convene TAG 59XX to discuss the issue in more detail.

TAG 59XX – 18 October

An issue with the proposed testing of the November 2019 SEC Release was raised under Any Other Business (AOB) at the TAG meeting on 10 October 2019. This issue relates to a specific DCC Change Request, CR1066, which the DCC intends to use to implement some of the functionality associated with SECMP0062, if that Modification Proposal is approved.

The issue arose because the DCC assumed that SECMP0062 would be approved in time to be included in the November 2019 SEC Release, and began to implement and test CR1066 as part of that release prior to approval. The SEC does not prohibit this but the DCC would have been in breach if it had proceeded to deploy the change into the production environment before approval is granted. The Change Board elected to return SECMP0062 to the Working Group during its August 2019 meeting for further clarification and analysis on the proposed solution in order to address comments and concerns that had been raised in the Modification Report Consultation. This means that SECMP0062 will not be included in the November 2019 SEC Release.

The TAG approved a revised testing approach which will result in additional testing being completed to provide sufficient assurance. IOC will test in Systems Integration Testing (SIT) A with all of November 19 code switched off, and when November 19 is released, it will go into SITA with most of the November 19 code switched on, but CR1066 will be switched off. There will also be an additional cycle of regression testing.

TAG 60 – 30 October

The TAG approved the following documents during this regular monthly meeting:

- The SMETS1 IOC Regression Depth and Breadth document;
- The SMETS 1 IOC SRV Testing Depth and Breadth Elster Dormant/Active/Mixed document was approved on the condition that changes were made to introduce testing of the Export Supplier User Role;
- The SMETS1 MOC MDS SIT Depth and Breadth Elster Dormant/Active/Mixed document;
- The SMETS1 MOC MDS Regression Depth and Breadth Elster Dormant/Active/Mixed document was approved on the condition that changes are made to reflect that an additional functional regression test in SITA will be executed prior to deployment.

The TAG will convene again on 8 November to review the test completion reports relating to the November 2019 SEC Release and the next SMETS1 DMCs to be added to the EPCL. A joint paper (SECP_74_1511_06) will be provided to the Panel making a recommendation from the Operations Group, Testing Advisory Group and Security Sub-Committee.

5. Recommendations

The Panel is requested to **NOTE** the content of this paper.

Rebecca Jones

SECAS Team

8 November 2019

Attachments:

- **Appendix A:** User Security Assessments – Identified Non-Compliances (**RED**)