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_75_1312_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 considered and supported a BEIS paper on the approval mechanism for SMETS1 migrations. The proposed process is set out in SECP_75_1312_12.

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.

The DCC held a CH Reverse Logistics workshop on 18 November to gather requirements and explore options for a bulk returns process. The bulk returns process is expected to be developed and deployed for September 2020.

Communications Hubs and Other Exceptions

The DCC has produced a detailed analysis of the CH Exceptions and confirmed that there are four main categories of exceptions. More analysis work is needed, however progress has been made by engaging with Service Users and some reduction in new exceptions has been observed.

CSP C&S continues to raise exceptions citing missing address data despite the DCC having implemented a change to enable the CSP to retrieve this data directly from the DSP.

Alerts

There has been some further progress with addressing the number of rogue alerts, but they continue at a very high level. The DCC agreed to present an overall picture of how the increased volume of Alerts affects the service in each CSP Region.

CSP N Installation failures/times

In response to an item raised by a Large Supplier at the November OPSG, CSP N presented their remediation plan. The OPSG were surprised and concerned to be told by CSP N that the current level of Alerts is already causing a degradation in service performance. This was in conflict with previous assurances from DCC to OPSG and other forums that Alerts would not cause capacity issues with the CSPs.

The OPSG requested the DCC provide a clear statement on the impact of alerts in the CSP N region. The OPSG expressed disappointment that CSP N have apparently only just begun to reconfigure and tune the network where issues were first reported by them in the PMR from May 2019 and challenged at the time by SECAS.

CSP N set out a series of tasks they are undertaking which they believe will improve the performance of Install and Commission in the Northern region by the end of December. However, they found it difficult to estimate the magnitude of the improvement; the OPSG were surprised to learn that CSP N do not have a simulation of the network to assist with network configuration and tuning and to investigate likely network behaviour.

In parallel with this exercise, as set out above, the DCC is working with Service Users to reduce the volume of rogue Alerts.

A Large Supplier noted that they had experienced a 50% failure rate of Over the Air meter firmware updates in November.

Service Performance

Code Performance Measure 1 was again below target. The DCC reported that the plan of the actions being taken by CSP N and CSP C&S to get this measure above target by December was on track. A Large Supplier expressed concern that this might not be achieved as they had seen a deterioration of performance in November.

OPSG members reported that the metrics for CSP N did not reflect the extent of 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 14 Users are submitting Certificate Signing Requests and 16 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.

BCDR

The DCC reported on the BCDR testing completed in 2019 and provided a plan for extensive BCDR testing in 2020, including additional resilience testing. The additional resilience testing will resolve an outstanding amber flag on SMETS1 migrations.

Maintenance Trial Extension

The OPSG supported the DCC proposal that the trial continue until the Modification has been implemented or rejected, subject to a quarterly review at the OPSG.

Operational Metrics Project

The Operational Metrics Project has engaged with Ofgem and issued the PID. A survey has been issued to Parties and the Quick Wins workstream has been initiated with the DCC. A workshop for OPSG members will take place on Monday 16 December to gather and evaluate requirements for both Quick Wins and the full review.

OPR Changes for SMETS1

The DCC presented the proposed Operational Performance Regime (OPR) measures in relation to SMETS1.

The OPSG noted that the proposal appeared to constitute a change to the Performance Measurement Methodology (PMM) and referring the DCC to Panel Action SECP74/06.

The DCC noted that the proposed measures for SMETS1 have been discussed with Ofgem and are currently investigating how the OPR will work for them. The OPSG noted the presentation however it was felt that the DCC had not engaged with all SEC Parties and that this presentation did not constitute consultation as required in the SEC.

3. Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

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

3.2 Verification Assessments

As part of its wider obligations, the SSC review the outcomes of Verification User Security Assessments. If the SSC believes 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 November 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 which was approved. Details can be found in confidential Appendix A.

3.4 Security Self-Assessments

Three Security Self-Assessments were reviewed by the SSC in November 2019, the outcome of which can be found in confidential Appendix A.

3.5 SSC Highlights

SECMP0007 'Firmware Updates for IHDs and PPMIDs'

The SSC provided input on SECMP0007 'Firmware Updates for IHDs and PPMIDs', which requires the DCC to clarify whether SRV11.1 can differentiate between firmware upgrades to ESME & GMSE separately from In-Home Displays (IHD) and Pre-Payment Meter Interface Devices (PPMID), Anomaly Detection Threshold (ADT) to be performed and a limit of 30 days in the future for firmware upgrades to be activated.

Use Case Proposals

The SSC held a Working Group on 6 November attended by industry representatives, National Cyber Security Centre (NCSC) and BEIS to review five Use Cases for Device refurbishment that had been proposed by industry representatives. The SSC agreed to approve the drafting of guidance for SSC, BEIS, NCSC and industry review for the following Use Cases:

- 'To identify installed SMKI Certificates' which is to include the Public Certificate number behind a menu; Industry comments on the guidance are due by 6 December 2019; and
- 'To reset the HAN' in cases where Commissioning has not completed, subject to the NCSC agreeing on the security controls that need to apply to the Triage site. A meeting with BEIS and NCSC took place on 4 December to progress proposals for the security controls.

The SSC also agreed to approve the actions to progress an impact analysis for three other Use Cases: one for, 'Factory Reset', and two for 'Replace DNO Certificates'. Impacts for the DCC's systems and processes and for confidentiality of consumption data are being progressed.

SMETS1 Enrolment & Adoption

The SSC was provided with updates from the DCC regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; functional testing; SMETS1 alert storms; the depth and breadth testing documents for Final Operating Capability (FOC); the risks of XML signing enforcement; security testing Assurance proposals; SMETS1 Certificate issues; and the Joint Industry Cyber Security Incident Management Plan (JICSIMP) Scenario Workshop feedback.

Anomaly Detection Threshold (ADT) Values

The SSC Members agreed on ADT values for the DCC November Release, after considering the operational implications of the values proposed by the DCC in October. The SSC also approved the DCC's request to change the way in which users submit ADT values.

User CIO Re-Procurement Exercise

In line with SEC G7.20(h), SSC Members provided feedback on the current User Competent Independent Organisation (CIO) service provider in light of the upcoming User CIO re-procurement exercise.

Central Switching Service (CSS) Update

The SSC was provided with an update regarding the risk assessment which has been carried out on the security architecture for the CSS. The DCC advised that the Request for Tender (RFT) for the Public Key Infrastructure (PKI) has been issued.

New SEC Modifications raised by SSC

The SSC decided to raise two problem statements to initiate SEC Modifications:

An alternative to SOC2 assurance

The SSC reviewed the assurance provided by the annual Service Organisation Control (SOC) 2 audit as required by SEC G9.2 to G9.7 which is now in its third cycle. SOC2 is a USA security audit standard and has proved to be difficult to align with SEC security obligations; it provides no calibration of findings which therefore requires a great deal of subsequent investigation and follow-up; and it does not provide SSC with an equivalent assurance of DCC security compliance as User Security Assessments provide for Users. The SSC considers that an alternate assessment methodology will provide greater value and assurance to the SSC and to Users.

Technical controls to check separation of signing keys

SEC Appendix AD Clause 3.3.1 requires a User to use a separate (different) User Role Signing Private Key for XML format Service Requests to that used for a Signed Pre-Command sent to the DCC. However, during the development of security controls for SMETS1 enrolment, it has emerged that, for SMETS2, the DCC has not developed a technical control to ensure that the SEC obligation is being met. The SSC considers that this lack of a technical security control requires remediation to ensure satisfactory application of security controls for SMETS1 and SMETS2.

3.6 SMKI PMA Highlights

SEC Appendix L

The SMKI PMA were content with the proposed updates to the SEC Appendix L (SMKI Recovery Procedure) to reflect changes that have been implemented in GBCS and IRP 555, which will now be issued to BEIS for consultation with SEC Parties, subject to a meeting with DCC, BT and CGI to ensure that the Trusted Service Provider (TSP) and Data Services Provider (DSP) are aware of the proposals and can implement them.

MP074 – 'Clarity on Obtaining SMKI Device Certificates'.

The SMKI PMA Chair (GH) provided an update on MP074 – 'Clarity on Obtaining SMKI Device Certificates' noting that this modification prevents the use of the SMKI Portal via the Internet (SPOTI) from issuing SMKI Device Certificates and is due to be implemented into the SEC as part of the November 2019 SEC Release.

Changes to SEC standards and guidelines

The SMKI PMA has undertaken an annual review of the standards and guidelines relating to the SMKI Services that are embedded into the SEC and is progressing a number of standards and guidelines that have changed or been removed with NCSC and DCC. DCC will need to consult on the impact on industry from deprecating the SHA1 standard for Secure File Transfer Protocol (SFTP).

Guidance for Network Operators

The SMKI PMA has published guidance on the SEC website for Network Operators which advises on technical solutions to enable a Network Operator to change an incorrect Network Operator SMKI Certificate that has been put onto a meter by a Supplier during the Commissioning process.

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

4.1 TABASC Highlights

SECMP0067 'Service Request Traffic Management' Update

The TABASC have expressed an interest in SECMP0067 'Service Request Traffic Management'; at the November TABASC meeting the informed the TABASC that there are two concepts as part of this modifications, the first is for system capacity and the other is for individual users having allocated capacity within it. The DCC will count the total number of requests coming into the system to see if that system's capacity has been reached. The TABASC noted that DCC expects traffic management to be active for low numbers of seconds rather than any sustained period.

The TABASC is continuing to provide feedback on the modification including requesting that the TABASC has opportunity to review the impact assessment.

Effectiveness Review Responses

The TABASC was provided with the Effectiveness Review responses and the initial analysis, from the eight responses received. The TABASC agreed the proposed actions and next steps and will update Panel in due course.

SEC Strategic Plan

The TABASC discussed the SEC Strategic Plan, which feeds into the SEC Panel Draft Budget 2020 – 2023. The TABASC confirmed support for certain activities, provided input into the budget, and refined the cost and probability of activities. TABASC will now develop a plan to manage the delivery of those project activities.

4.2 TAG Highlights

The TAG met on 27 November to discuss the following topics:

SMETS1 Testing Update

The first set of End-of-Cycle (EOC) testing is currently underway for Middle Operating Capability (MOC) MDS installations, and that the blocking defect previously highlighted has now been resolved. The DCC intends to complete testing on 10 December.

Pre-Integration Testing (PIT) continues for MOC Secure installations. The DCC was not satisfied that the scope of PIT testing which Secure had completed was sufficient, and therefore requested that the SMSO undertake additional testing.

Systems Integration Testing (SIT) for the Final Operating Capability (FOC) is scheduled to start on 6 January 2020.

Management of changes to the User Testing Services environments

The DCC provided the TAG with an overview of its proposed approach to conducting Impact Assessments of changes to the User Testing Services (UTS) environment, which is a requirement of the User Testing Services Approach Document (UTSAD).

The DCC will assess the impact of each change on testing activities of Testing Participants (TPs) which are still undertaking Eligibility Testing (ET), along with TPs that have completed ET. The DCC will issue a testing notice to TPs specifying the change and impact.

The Impact Assessment process will be formed of two stages:

1. DCC will confirm if the change has an interface impact or not, if there is no impact then no retesting will be required and that is the end of the assessment.
2. If a change results in an impact to the interface, the DCC will confirm the low-level impact on the ET test scope and identify any required retests.

The TAG's role in managing any disputes which arise if additional testing is deemed necessary is clearly defined in the UTSAD and the TAG was comfortable that DCC's proposals accurately reflect this.

SMETS1 DMCT Standard Test Pack

The TAG is required to review and approve any new or amended Standard Test Packs. DCC presented its proposals for the SMETS1 Device Model Combination Testing (DMCT) Standard Test Pack for approval at this meeting.

The TAG was broadly comfortable with the proposals but highlighted that some Negative Testing should be considered around the generation of spurious Device Alerts and requested that DCC undertake work to ascertain to what extent Alerts can be monitored during testing, along with confirming the parameters it currently uses during testing. Approval was deferred until this work is complete.

SMETS1 MOC MDS testing approach

The TAG approved the Depth and Breadth approach document for MOC MDS SIT and Migration test approach documents.

SMETS1 FOC testing approach

The DCC presented three test approach Depth and Breadth documents relating to migration, solution and regression testing. The DCC was seeking feedback to support the development of final versions of each document for approval at the next TAG meeting on 16 December. The TAG was unable to provide sufficiently detailed feedback during the meeting and agreed to provide written feedback to the DCC by 4 December instead.

5. Recommendations

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

Rebecca Jones

SECAS Team

6 December 2019

Attachments:

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