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_78_1303_28**
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

SMETS1 Migration Capacity

The OPSG agreed at an extraordinary OPSG meeting on 7 February 2020 to remove the daily cap of 2,000 migrations per day. This was with the caveat that the DCC provide monthly progress updates on performance for the previous month and a forward look of the intended volumes for migrations and pacing strategy, to allow the OPSG to provide views and recommendations. Since the removal of the cap, the DCC has succeeded in migrating 20,000 meters in a day with a 99.7% success rate over 21 hours. The DCC plans to attempt to migrate 28,000 meters on a day in April.

SMETS1 Live Services Criteria – MOC Morrison Data Services (MDS)

The OPSG agreed to endorse the recommendation to the Panel to add the first Middle Operating Capability (MOC) entry, Morrison Data Services (MDS) Elster Device Model Combination, to the Eligible Product Combinations List (EPCL). However, the OPSG reiterated that Live Services Criteria (LSC) 6 regarding service stability will remain at Amber status due to the volume of major incidents across the DCC service in January and February; the OPSG acknowledged that service impacting incidents have reduced in February.

The OPSG outlined that LSC8 (impact on consumer experience) is currently Amber due to the risk on consumers with Auxiliary Load circuits. The DCC will mitigate this by not migrating impacted consumers until it can introduce the fix as part of Core 1.1, scheduled for May 2020. The DCC highlighted a risk that Telefonica (S1SP) may not be fully compliant with the SEC obligations on Service Management as it does not formally employ the Information Technology Infrastructure Library (ITIL) framework but utilises processes compliant with ITIL. The OPSG has requested that the DCC confirm that Telefonica's Service Management processes are compliant with ITIL.

Meter Firmware OTAs

The DCC presented progress on remediation plans for CSP N & CSP C&S, aimed at reaching "Green" status for Performance Measure 2 regarding Over the Air (OTA) Firmware performance. The CSP C&S region has now achieved the target service level for January 2020 but will be introducing further improvements in March 2020 to solidify their performance. CSP N continues to perform under

target service level, having failed to achieve the remediation target of December 2019. The DCC presented a plan that aims to have CSP N performing above target service level by May 2020.

Spurious Alerts

The OPSG noted that the Smart Metering Design Group (SMDG) had confirmed the view that the OPSG is the appropriate body to oversee the resolution of the Spurious Alerts.

The DCC has made progress on its development of remediation plans. However, alert volumes continue to increase in all CSP regions.

The DCC provided an overview of how the major spurious alert in CSP N (8F12s) will have a detrimental impact on the lifespan of the Communications Hub (CH). A root cause has yet to be identified and the DCC outlined that it has, until recently, struggled to get support from a Supplier to attend a consumer's premises to complete further testing. An OPSG member suggested that the DCC also explore testing against the Release 2.0 CH firmware as they have seen evidence that suggests it can resolve the issue; the DCC agreed to investigate.

The CSP C&S continues to see an increase in 8F3E alerts, however, plans are progressing to introduce a CH firmware update by April 2020 that should reduce a significant portion (up to 50%) of these alerts. The OPSG raised concerns regarding the timescales and ability to support User Testing of this CH firmware due to the industry focus on Release 2.0 User Testing.

The DCC introduced additional Data Service Provider (DSP) motorway capacity to increase assurance that it will be able to handle the growing traffic on the system whilst alternative remediations are being deployed. The DCC stated that it believes SECMP0062 'Northbound Application Traffic Management – Alert Storm Protection' will drastically reduce the impact of alerts on the DSP services. The OPSG requested that the DCC present projections on how key changes will affect capacity requirements.

CH Exceptions

The DCC continues to develop and improve remediation plans for the major categories of Communication Hub (CH) exceptions and has assigned leads for each region's exceptions. However, the volume of CH exceptions continues to rise.

The OPSG reiterated to the DCC that CSP N continues to overlook incidents with users regarding CH Exceptions, preventing any substantial reduction in the exceptions, in the North. The largest exception continues to be 'No or incomplete address', however, further investigation has identified that it is primarily one Service User that is responsible for this; the OPSG requested that the DCC work with this Service User to agree a plan moving forward.

Service Performance

Code Performance Measure (CPM) 1 was below minimum Service Level. This CPM has not been met in 12 out of the last 13 months. The Service Provider Performance Measure (PM) 2, delivery of firmware payloads, has been a consistent factor in this poor performance. The DCC is presenting regular progress updates to the OPSG on the planned activities to achieve consistent target service levels on PM2.

Operational Metrics Review Project

The Operational Metrics Review Project has produced and shared the first draft report to OPSG members on 18 February 2020. Feedback has been collated and an updated report will be distributed for SEC Party review on 6 March 2020; with an introductory teleconference held for SEC Parties on 5 March 2020.

The final report will be shared with OPSG in early April 2020 with the final report to be presented to the SEC Panel for consideration at its meeting on 17 April 2020.

SEC Releases 2020: June and November

The DCC presented a proposal to move the SEC June Release date to Wednesday 6 May 2020 and align this with the deployment of the SMETS1 Core 1.1 Release. The OPSG raised concerns that bringing the dates forward would allow limited time for Users to prepare for the SEC release. The DCC believes that there would be minimal-to-no impact of this release on Users but the OPSG requested that the DCC confirm this position by asking Users. The OPSG will carry out a preliminary review of readiness at the Tuesday 7 April 2020 OPSG meeting with a final review scheduled for Monday 27 April 2020.

Performance Measurement Methodology (PMM) – SMETS1 Consultation

The DCC intends to issue the consultation to include the SMETS1 Performance Measurements to the PMM in March 2020. This will address the OPSG and SEC Panel action on the DCC (SECP74/06).

3. Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) reviewed four initial Full User Security Assessments (FUSAs) and two second or subsequent FUSAs in February 2020, setting four assurance statuses and two compliance statuses, respectively, as a result. Details can be found in confidential Appendix A.

3.2 Verification Assessments

The SSC reviewed nine Verification User Security Assessments (VUSAs) in February 2020.

3.3 Director's Letters

The SSC reviewed five Director's Letters in February 2020.

3.4 Security Self-Assessments

The SSC reviewed two Security Self-Assessments in February 2020.

3.5 SSC Highlights

Meter Triage Use Cases and Guidance

The SSC Chair sent draft guidance regarding Use Case 004 (Factory Reset) to the National Cyber Security Centre (NCSC) and BEIS for comment, and, following updates for NCSC and BEIS comments, SECAS has circulated this to industry for comment. This Use Case was originally raised by Meter Asset Providers (MAPs) but is also supported by Suppliers and manufacturers. The next SSC CPA Industry Day is scheduled to take place on Tuesday 31 March 2020.

SSC Projects

<u>Security Incident Management (SIM) Exercise</u>

A Security Incident Management (SIM) exercise took place on Thursday 27 February 2020, in which security experts ran through a number of hypothetical scenarios to check that the correct processes are in place for real-life security incidents.

User CIO Re-procurement

On Friday 28 February 2020, the Invitation to Tender (ITT) was issued to a number of potential bidders for the User CIO re-procurement exercise, for which the current contract expires in June 2020.

Annual Security Obligations

There has also been significant progress made regarding the review of the Security Architecture Document (SAD) and the 8th Iteration of the SSC End-to-End Risk Assessment.

Ofgem

Ofgem recently issued a letter to the wider industry advising of Ofgem's participation at SSC Meetings, and reminding Operators of Essential Services (OES) of their obligations under the Network Information Systems (NIS) Directive, where applicable. The alignment of SEC Section G obligations to the NIS Directive are already in the Security Controls Framework (SCF).

SMETS1 Enrolment & Adoption

The DCC presented updates regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; functional testing; SMETS1 alert storms; negative security testing; SMETS1 Certificate issues; Penetration Testing of Systems Integration Testing (SIT) A and User Interface Testing (UIT) A; and Engineering Pins. Following a detailed scrutiny of evidence, the SSC made a recommendation to the SEC Panel in respect of SMETS1 Live Services Criteria Number 10 for the MOC MDS Device Model Combination (DMC) drawing attention to a new security risk.

SECMP0007

SECAS presented an update regarding the SEC Modification SECMP0007 'Firmware updates to IHDs and PPMIDs' and sought SSC advice on a proposed solution to allow for the modification to progress smoothly. The SSC agreed that Home Area Network (HAN) Connected Auxiliary Load Control Switch (HCALCs) Devices should have the same Anomaly Detection Threshold (ADT) rules as ESME and GSME, and agreed to commission a risk assessment on the SECMP0007 proposed solution upon receipt of the revised set of requirements for the solution.

3.6 SMKI PMA Highlights

Incorrect Certificates for Network Parties – DCC investigation.

The SMKI PMA was updated on an investigation being conducted by the DCC regarding the potential for incorrect Organisation Certificates being placed on Devices by certain Network Parties due to acquisition and mergers.

SMKI PMA Good Practice Guides

The SMKI PMA considered recommendations from the SMKI PMA Chair regarding replacing the SEC references to the discontinued or changed NCSC Good Practice Guides (GPGs) 43, 45 and 46 to bespoke guidance specific to Smart Metering. Members agreed to provide comments on the draft guidance, plus further guidance being drafted to replace SEC references to GPG 13, at the March SMKI PMA meeting.

Enduring Change of Supplier (ECoS) Processing Changes

The SMKI PMA was informed of proposed changes to the processing checks applied to Change of Supplier Requests under ECoS, to be introduced in parallel with the introduction of XML Signing

Certificates for DCC Users. The SMKI PMA was generally supportive of the changes and noted that the proposed changes should not impact SMKI.

New Draft Proposals and Modification Proposals

The SMKI PMA requested further updates on the progression of DP108 'SSI Job Type Role for SRO/ARO' and DP110 'Aligning SEC Appendix D with DCC Processes' as requested by the SMKI PMA, due to the potential impacts on SMKI.

SMETS1 PKIs

CP, CPS and documentation for MOC/FOC

The SMKI PMA noted the DCC update regarding the provision of the Certificate Policy (CP), Certification Practice Statements (CPS) and other relevant documentation for the Middle Operating Capability (MOC) and Final Operating Capability (FOC) SMETS1 cohorts.

S1SP Risks to FOC PKI

The DCC provided the SMKI PMA with an update regarding the risks to the FOC PKI resulting from a potential security compromise to the S1SP. The SMKI PMA requested the DCC provide further clarification on several mitigating actions.

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

4.1 TABASC Highlights

Extending Durations of 2G Coverage / 4G-LTE Communications Hubs

The DCC provided the TABASC with the business case and update on its Network Evolution approach, which seeks to mitigate the risk of Communications Hubs potentially not reaching the end of their commercial life due to lack of supporting 2G services. The DCC also presented what it believes are the high-level requirements to meet programme A (ensuring CH resilience and mitigation of contractual uncertainties) of the network evolution project. The TABASC agreed the requirements, subject to the inclusion of revisions fed back by members. The TABASC also caveated that agreement of these requirements is dependent on only the WAN module changing as part of any new next generation CH design to limit the extent of testing required. This is linked with negating any complexity of design as well as making sure that any new iteration of the next generation hubs will be delivered Q1 2021.

DSP Sandpit for Network Evolution

The DCC provided a problem statement for assessment of future technical options to be considered when renewing the DSP contract in 2021. The sandpit will allow the DCC to explore innovative solutions that will help address concerns with performance, value for money, technology and provide more control and agility. Ultimately, the TABASC challenged the approach and lack of clarity over the requirements and success factors. The TABASC also requested that the DCC provide confirmation of whether DSP is meeting current requirements in the first instance before proving new requirements. The TABASC also noted that the need for a DSP sandpit as part of the network evolution activities should also be complemented by a strong business case and that this should be agreed before going out to RPF.

Expanded GFI GBCS Test Tools 2020

The DCC proposed to expand the GFI Test Tools to cover the overarching DCC ecosystem, including supporting DCC customers with Electric Vehicle and Proportional Load control propositions. The aim is to provide DCC users with the ability to simulate the interaction of Devices with the DCC systems in

test environments. The TABASC agreed that this was a good step, however feedback was provided to the DCC to consider the methods by which any costs can be recovered as part of the new GFI test tool rollout.

Alerts Lost during DCC Scheduled Maintenance – EUK problem statement

The TABASC is continuing to consider the EUK raised issue for minimising Alerts lost during DCC Scheduled Maintenance. The current reliability of the HAN communications and the priority of certain Alerts for Service Users was assessed to understand the impact of the potential solutions. The TABASC provided a steer on focus areas for DCC to progress.

Multiple Suppliers per MPAN project

BSC Modification P379 'Multiple Suppliers through Meter Splitting' discusses meter splitting for the purposes of settlement. The TABASC notes several challenges with the proposal and notes the possible implications on Smart Metering. The TABASC agreed to request that Panel raise these concerns with Ofgem and Elexon.

Smart Export Requirements project

SECAS held a workshop on 4 March 2020 with key stakeholders to understand the current Export business processes within the smart metering end to end solution. SECAS worked with these stakeholders to identify any gaps in the processes and propose potential solutions. The outputs and actions which have been identified will be sent to the DCC to address.

Impacting IRPs Current IRP Modifications

When discussing DP98, the TABASC discussed whether there is benefit in implementing a new GBCS v3.3 if the IRP changes do not provide material benefit. The downsides of having additional versions stems from needing to develop and test for each version, the more there are the more complex, time consuming and costly it is. The TABASC agreed with the approach to not implement GBCS v3.3 if there was no material benefit to Devices. It was agreed that the changes should be included within GBCS v4.0 which is currently in Draft for delivery by BEIS in November 2020, and also applied to the next GBCS 3.x version when all the changes result in material benefit. SECAS will confirm whether there is material benefit from the IRPs before deciding whether to implement the modification in a new GBCS v3.3 at this time.

MP080 'Managing DUIS uplifts'

The TABASC considered the Modification Proposal and expressed significant concern with the proposal to remove the Schedule 11 'Technical Specification Applicability Table' (TSAT) out of the SEC and therefore the formal SEC Modification process. The TABASC agreed with the approach to add the DUIS into the TSAT with caveats.

4.2 TAG Highlights

The Testing Advisory Group (TAG) met twice during the reporting period to discuss the following topics:

SMETS1 IOC

The TAG reviewed and approved the IOC Aclara Migration and Regression Depth and Breadth documents in relation to dormant, active and mixed installations.

The DCC highlighted that it expects this testing to happen before the SMETS1 'Core 1.1 Uplift' is implemented, and before MOC Secure and FOC SIT. The TAG requested a session on the full portfolio of DCC deliveries and releases.

SMETS1 MOC

The DCC advised that Middle Operating Capability (MOC) Secure initial testing has been slower than anticipated. However, the DCC has a plan in place to accelerate post-Migration testing in order to achieve test completion on Friday 27 March 2020.

SMETS1 FOC

The DCC highlighted that Final Operating Capability (FOC) has ongoing communication issues with the SMETS1 Service Provider (S1SP) being unable to communicate with Devices. A workaround has been implemented to allow the DCC to progress with post-Migration testing. SIT test execution remains due to complete on Saturday 30 May 2020.

June 2020 SEC Release and SMETS1 Uplift 1.1

The DCC provided an overview of options for the concurrent testing and implementation of the June 2020 Release alongside the SMETS1 Uplift 1.1 to reduce overall implementation risk within a constrained timeframe. The DCC provided the TAG with its view on the best way of doing this, based on a balance between risk mitigation, governance and deployment of the functionality.

The proposal is to take the SMETS1 Core 1.1 uplift and June 2020 Release activities into the SIT-A environment at the same time, to optimise the governance overhead and regression testing. The DCC has confirmed that the SMETS1 Uplift 1.1 and June 2020 Release are not intrinsically linked and do not need to be implemented together. This means that if one release is unable to proceed, the DCC would be able to accommodate this without undermining any testing already completed by carrying out additional regression testing. However, the current plan is to implement both releases into production at the same time.

The TAG endorsed the proposed approach and requested further detail around the associated technical and governance risks, along with the associated mitigations. Once the arrangements have been agreed in full, a recommendation will be made to the Panel if the June 2020 SEC Release Implementation Document requires updating as a result.

Faster Switching

The DCC agreed to produce a testing approach depth and breadth document, similar to those used to govern SMETS1 activities.

Discussions between Ofgem and SECAS regarding the provision of regulatory cover for the Panel/TAGs governance role in assessing test completion remain ongoing.

5. Recommendations

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

Ryder Agolli

SECAS Team

6 March 2020

Attachments:

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