

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.

<b>Paper Reference:</b>	<b>SECP_79_1704_20</b>
<b>Action:</b>	<b>For Information</b>

## 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

##### Coronavirus Update

The OPSG has included a regular agenda item to cover the current status, risks and impact to the day to day operations brought on by the COVID-19 Pandemic. The DCC provided an overview of the Pandemic response plan to ensure staffing and procedures are in place to protect critical services. The DCC are meeting regularly with Service Users and their Service Providers to monitor the situation for any change. The DCC confirmed that at present both its own operations and those of the Service Providers are carrying on without problems ("green" status).

The OPSG endorsed the DCC decision to defer some DR testing as part of their strategy for minimising risk in the current circumstances. The DCC are currently assessing how to re-plan the DR testing that has been postponed. The OPSG asked that DCC present a revised plan as soon as it was practicable to do so.

The scheduled Business Continuity Disaster Recovery testing for Telefonica, Arqiva, SIE and DCO has been postponed due to the pandemic. There is a risk that the Secure Disaster Recovery testing, that forms part of the Live Service Criteria assessment, may not be able to go ahead if the situation continues up to June. The DCC is currently assessing the ability to re-plan the DR testing that has been postponed.

##### SMETS1 Live Services Criteria – Aclara

The OPSG agreed to endorse the recommendation to the Panel to add the last Initial Operating Capability (IOC) entry, Aclara Device Model Combination, to the Eligible Product Combinations List (EPCL). The OPSG made a general statement that this decision is being made under exceptional circumstances due to the pandemic, and noted the close monitoring described by the DCC to ensure early identification of any problems. The DCC is currently operating under Business Continuity protocol, with further information on mitigations and assurance under LSC9.

The OPSG acknowledged the improvement in the number of incidents over the last two months under Live Services Criteria (LSC) 6 regarding service stability. The OPSG highlighted that due to the

current reduction in installations, the DCC systems are not experiencing the usage that would be expected in business as usual.

The OPSG outlined that LSC8 (impact on consumer experience) was 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 OPSG requested that the DCC consider the energy consumer impact when planning the pacing strategy for Auxiliary Load circuits, and with this qualification agreed that this LSC should be assessed as Green.

## 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 and February 2020. CSP N continues to perform under target service level for February 2020, significant fixes were deployed throughout March: it is anticipated that these will result in performance improvements in April.

## Spurious Alerts

The OPSG noted that the SEC Panel endorsed the view that the OPSG is the appropriate body to oversee the resolution of the Spurious Alerts.

The total number of alerts has decreased slightly in CSP Central and South Regions and increased slightly in CSP North region. The DCC has made progress on its development and deployment of remediation plans.

The DCC provided an overview of how the dominant spurious alert in CSP N (8F12s) will have a detrimental impact on the lifespan of the Communications Hub (CH). The DCC are in the process of generating individual Service User reporting on predicated “life-expired” dates for Communications Hubs based on the 8F12 volumes. The DCC has identified what it believes to be the principal root cause of superfluous 8F12 alerts. The DCC will be raising this at TSIRs and with the relevant manufacturers to confirm. The DCC noted that there were some indications that the upgrade to Release 2.0 CH firmware might ameliorate 8F12 alerts, the DCC stated that out of 14 alerting devices, 13 had stopped alerting after the upgrade. However, due to the nature of the sporadic alert behaviour, the DCC stated that it was too early to confirm definitively whether the R2.0 CH Firmware has resolved or improved the 8F12 volumes.

The 8F3E alerts have recently plateaued in growth, however this may be correlated to the reduction in installations. Plans are progressing to introduce a CH firmware update by April 2020 that should reduce a significant portion (up to 50%) of 8F3E alerts in the Central and South Regions. The DCC noted that Operational Acceptance for the CH firmware is due on 8 April 2020. The DCC has worked with Service Users to identify candidates for the pilot and will monitor any change in alert behaviour throughout the Pilot.

The DCC and OPSG are monitoring emerging new alert types for any behaviour that might warrant further investigation.

The DCC provided an overview of the Data Service Provider (DSP) motorway capacity and how this might change based on upcoming changes and fixes such as [SECMPO062 ‘Northbound Application Traffic Management – Alert Storm Protection’](#) and the CH Firmware deployments stated above.

## Excluded Alerts – SECMOD62

The OPSG reviewed a DCC proposal to alter the parameters and alerts excluded as part of [SECMPO062 ‘Northbound Application Traffic Management – Alert Storm Protection’](#). The OPSG

questioned the governance on changing an approved mod that has yet to be put into operation: this would need to be consulted upon by the DCC and approved by the Panel, as outlined in the legal text of the modification. The OPSG requested that unless there is a significant urgency, then the proposal should follow the proper governance.

## Service Performance

Code Performance Measure (CPM) 1 was below minimum Service Level. This CPM has not been met in 13 out of the last 14 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 produced and shared the final report to OPSG members on 3 April 2020. The OPSG reviewed and endorsed the recommendations of the final report, except for the recommendation on number of Incidents: this recommendation will be adjusted in the final report.

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

## SEC Releases 2020: June Preliminary Review

The DCC presented a preliminary overview of readiness for the SEC June 2020 Release ahead of the final OPSG decision on 27 April 2020.

The OPSG raised concerns regarding the governance of the SSI changes within [SECMP0062 'Northbound Application Traffic Management – Alert Storm Protection'](#), as neither the working group or the OPSG has considered these changes yet.

## 3. Security Sub-Committee and SMKI PMA

### 3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) set the assurance statuses for one initial Full User Security Assessment (FUSA) and one FUSA that had been subject to a Follow-Up Assessment. The SSC also set the compliance statuses for two second or subsequent FUSAs. Details can be found in confidential Appendix A.

### 3.2 Verification Assessments

The SSC reviewed three Verification User Security Assessments (VUSAs) in March 2020.

### 3.3 Director's Letters

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

### 3.4 Security Self-Assessments

The SSC reviewed six Security Self-Assessments in March 2020.

### 3.5 SSC Highlights

## SSC CPA Industry Day

The SSC hosted another well attended CPA Industry Day on 31 March 2020. Presentations from the SSC Chair, BEIS and NCSC generated useful debate and feedback from industry representatives in attendance. A range of topics were covered including updating the Security Characteristics Threat

Maps, CPA Build Standards, Use Case Guidance (Factory Reset), Lessons Learned and BEIS Strategic Developments.

## COVID-19

The SSC Chair discussed Business Continuity arrangements with SSC Members in the event of travel restrictions due to COVID-19.

### Assessments

The User Competent Independent Organisation (CIO) advised Members that a communication had been issued to SEC Parties detailing the Business Continuity arrangements for carrying out fieldwork assessments due to COVID-19 travel restrictions, adding that the response from SEC Parties has been positive and that remote assessments could be offered to SEC Parties going forward.

### Central Products List

The SSC Chair informed SSC Members of a decision on behalf of the SSC to approve nine SECAS personnel to have the technology - the File Signing Utility - downloaded to their laptops, and provided with tokens, along with instructions relating to their security requirements, safe-keeping and the need to notify any suspected compromise. This decision was taken to allow SECAS to make updates to the Central Products List (CPL) remotely in order to support business continuity in the event of unavailability or illness. SSC Members endorsed the decision made ex-Committee by the SSC Chair to protect CPL Business Continuity arrangements.

### CPA Monitoring

The SSC Chair advised Members that some Suppliers are reporting that, in accordance with government advice with regards to social distancing and self-isolation, they have taken the decision to only carry out essential work, impacting smart metering installations. Therefore, the SSC agreed that the removal of Landis & Gyr (L&G) and EDM I entries from the CPL on 8 April 2020, as previously agreed by the SSC, would be deferred until further notice.

## Proposals for Enhanced Separation between ECoS and DSP

The SSC noted an update from BEIS on Proposals for Enhanced Separation between the Enduring Change of Supplier (ECoS) role and the DCC's Data Service Provider (DSP).

## SMETS1 Enrolment and Adoption

The SSC noted the updates presented by the DCC regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; Security Functional Testing update; negative testing; engineering pins; Middle Operating Capability (MOC) including the SMETS1 CSP CIO Report; Single Use Authorisation (SUA) Reset; future 'Parent' and 'Child' approvals; Internet Protocol Security (IPSec) Links; and SSC assurance required from the DCC for the next Live Services Criteria assessment to be considered by SSC on 8 April 2020.

## Anomaly Detection

The SSC reviewed the management information relating to Anomaly Detection Threshold breaches over the past six months as presented by the DCC.

## Post-Commissioning Report

The SSC reviewed the latest DCC Post Commissioning Report for February's data and considered information regarding Service Request Volumes (SRV's), providing feedback for further development improvements needed to the report for presentation at the end of April SSC meeting.

## **SOC2 Progress Update**

The SSC continued to apply pressure on the DCC with regards to resolution of the outstanding SOC2 2018 Report; the SSC review of which has not been possible to conclude due to delays from the DCC in completing their Remediation Plan. The DCC advised that following presentation of the SOC2 2019 report, which is now also due, the outstanding SOC2 2018 validation could be finalised. The DCC is intending to present the SOC2 2019 Report for SSC consideration in April 2020.

## **Proposed Amendments to SCF Appendix Part 2 (BS7858 Updates)**

The SSC agreed the amendments to the Security Controls Framework (SCF) Part 2, Appendix B, to align guidance with the new version of the BS7858:2019 standard.

## **SSC Quarterly Work Package Q1 2020-21**

The SSC recommended the Quarterly Work Package for Q1 2020-21 (Apr-Jun) to the SECCo Board for approval.

## **Quarterly Standards Review**

The SSC noted the SECAS Security Expert's overview of the changes to the security Standards set out in the SEC over the most recent quarter, and agreed for the information to be uploaded to the SEC Website for SEC Parties.

## **SSC Risk Register Review**

The SSC noted an update from SECAS on the SSC Risk Register and re-assessed the impact levels for the most recently added risks.

## **Modifications**

The SSC Chair informed SSC Members of an update to the progress of SEC Modification [MP104 'Security Improvements'](#), which is now undergoing legal drafting. The suggested SEC drafting was made available to SSC Members and will be shared with BEIS to ensure a consistent approach with the BEIS proposals for using the XML Signing Key as part of ECoS processes.

## **Annual Security Obligations**

The SSC Chair provided an update on progress made on current SSC projects, including the Security Architecture Document (SAD) review, SSC Risk Assessment, Security Incident Management (SIM) exercise, and a review of CPA Security Characteristics (SCs) threat mapping.

## **3.6 SMKI PMA Highlights**

### **SMKI PMA Guidance**

The SMKI PMA considered recommendations from the SMKI PMA Chair regarding replacing the SEC references to the discontinued or changed National Cyber Security Centre (NCSC) Good Practice Guide (GPG) 13, to bespoke guidance specific to Smart Metering. Members were invited to provide comments on the new guidance to be discussed at the April SMKI PMA meeting.

### **BEIS Consultation (Changes to SMKI Organisation Certificates)**

The SMKI PMA noted a BEIS consultation on changes to SEC obligations regarding SMKI Organisation Certificates.

### **SMKI Certificate Testing Plans**

The SMKI PMA was updated by the DCC on the current status of the SMKI Certificate testing plans.

## **PKI for SMETS1 FOC**

### CP and CPS

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.

## **SMKI PMA Quarterly Work Package Q1 2020-21**

The SMKI PMA recommended the SMKI PMA Quarterly Work Package for SECCo Board approval.

## **SMKI PMA Risk Register Review**

The SMKI PMA reviewed the SMKI Risk Register, amended the risks where appropriate and agreed the new amendments.

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

### **4.1 TABASC Highlights**

The TABASC met twice in March and covered the following topics:

#### **DCC Network Evolution – DSP Sandpit**

The DCC provided the TABASC with an update on its Network Evolution approach for the development of a Sandpit environment. Its aim is to allow DCC to objectively prove design options and recommendations on changes to the Smart Metering Infrastructure during the re-procurement of DSP. The TABASC asked the DCC to further clarify the problems being sought to be addressed, critical success factors, and provide more information regarding projected timescales and costs.

#### **DCC Network Evolution - Test Automation**

The TABASC is providing feedback to the DCC with regards to the Test Automation proposal, as part of the wider Network Evolution programme. This is in response to current lengthy SMETS2 Regression Testing timescales and cost for the delivery of programmes and releases. The Request For Proposal for build and test is still in progress, however, the DCC demonstrated the automation framework and the key Components of the solution. The TABASC continue to request that the DCC prepare an outline business case to show the benefits of its delivery, including how much time it will reduce the Regression Testing based on the June and November release schedule.

#### **SECMP0062 - Alert Exclusion**

The TABASC discussed and provided views on the parameters and configurations which have been proposed by the DCC as part of the Alert management mechanism associated with [SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection'](#). The TABASC provided a recommendation to the Operations Group (OPSG) particularly focussing on Alert code specific counting. The recommendation was for consideration of Parameter B (Alert code Specific Threshold – Alert Storm protection) for each specific Alert code and that it should be invoked upon 1000 specific Alerts being generated in 24 hours rather than 20 previously stated (a rate of circa 41 per hour). This



would provide Service Users with enough headway to capture normal Alerts generated, as well as protect the DSP system from excessive traffic. The DCC confirmed its support for TABASC's position, however suggested that it would implement the measurement over a 1-hour period so there isn't an extended period where high volumes of Alerts can be sent. To do this, the Alert Code specific parameters would be configured as Parameter B 'Alert Code Specific Threshold' at 41, and Parameter R 'Alert Code Specific Rolling Window' at 60 minutes.

The TABASC also agreed with the DCC proposal to include Alert 8F12 in the exclusion list, in addition to those present in the modification report. This was on the basis that 8F12 Alert is considered critical to the Install and Commission process, and to consolidate it may have a detrimental effect on that process.

### **DCC Network Evolution - Extending Duration of 2G Coverage/LTE Communications Hubs**

The DCC continue to address the TABASC feedback 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 mobile services. The TABASC is awaiting the outline business case from the DCC and once provided, will consider the DCC recommendation.

### **Expanded GFI Test Tools "DCC in a Box"**

The expanded GFI Test Tools, to be known as "DCC in a Box" is to support wider Device testing in support of the November 2020 and later Releases. The DCC provided clarity regarding the TABASC's previous feedback on the provision including its plans to engage with the DCC Finance Forum. Further details on functional specification to provide an understanding of the capability of the product at launch, are required by the DCC.

### **Alerts Lost During DCC Scheduled Maintenance - EUK Problem Statement**

The TABASC is continuing to consider the issue raised by EUK for minimising Alerts lost during DCC Scheduled Maintenance and during failure scenarios. Feedback was provided on the User and Data Service Provider (DSP) buffer as well as considerations towards preventing AD1 alert loss.

### **Design Positions - Market-Wide Half Hourly Settlement Update**

The TABASC provided its views on the three viable options for implementation associated with the Market-Wide Half Hourly Settlements and its current design positions. Generally, the TABASC prefers solutions which would involve Suppliers collecting the data and that would minimise Device change and traffic impacts to the current architecture.

## **4.2 TAG Highlights**

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

### **SMETS1 and SEC Release concurrent testing**

The TAG reviewed DCC's proposal to conduct concurrent testing of the SMETS1 Uplift 1.1 release alongside the June 2020 SEC Release, including a review of technical and governance risks. The group agreed that the proposed approach reduces overall implementation risks across the two releases, and that any risks which arise must be considered and mitigated in the approach taken in the Testing Approach Document (TAD) for each release. The agreed approach requires that each release must be able to proceed if there are delays to the other, with this requirement reflected in both the SMETS1 Uplift 1.1 TAD and the June 2020 SEC Release TAD.

### SMETS1 testing documents

The TAG reviewed and approved the following SMETS1 testing approach documents for the following installations:

- SMETS1 Uplift 1.1 release TAD: This has been developed alongside the June 2020 SEC Release TAD to reflect the concurrent testing of the two releases and ensure that any risks arising as a result of concurrent testing are managed across the two releases. The agreed SMETS1 Uplift 1.1 TAD will not take effect until the governance arrangements set out in the SEC Variation Testing Approach Document (SVTAD) have been updated.
- June 2020 SEC Release TAD: As with the SMETS1 Uplift 1.1 TAD, the agreed approach requires that any delay to one release should not result in a delay to the other. However, one of the potential risk mitigations discussed is that if a delay to either release is likely to impact the other, the TAG may recommend to the Panel that the June 2020 SEC Release is delayed until November 2020 or later.
- MOC Secure migration Depth and Breadth of testing: This was agreed with no significant issues raised.
- Skeleton test completion reports: IOC Aclara (migration and System Integration Testing) and MOC Secure (migration only).

### Portfolio-level view of testing environment usage

The TAG reviewed testing environment usage across the DCC's entire programme portfolio. This information is intended to help the TAG assess testing and implementation risks which can be mitigated by carrying out appropriate testing, and to assist the development of future testing approaches.

The TAG agreed that the information provided is helpful, and that adding text to describe the key risks identified by the DCC (e.g. Testing of any release impacted by other releases in the environment), along with the associated mitigations, would support more targeted conversations.

### Faster Switching

The TAG agreed the exit criteria which will apply to testing of the interface between the Centralised Switching service (CSS) and existing DCC Systems.

The structure of the testing depth and breadth document has been agreed and the DCC will present a draft of the document during the TAG meeting scheduled for 29 April.

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

## 5. Recommendations

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

**Holly Burton, SECAS Team, 9 April 2020**

### Attachments:

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