

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_76_1701_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

Communications Hubs Returns

In response to a request from the Operations Group (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 is proceeding with development of the new Order Management System (OMS). The first phase, giving a consolidated ordering and returns system, is expected to be ready in the spring and the bulk returns process is expected to be developed and deployed for September 2020. The OPSG has requested the DCC to provide the consolidated set of requirements for the new OMS.

Communications Hubs and Other Exceptions

Whilst the DCC has continued to work on CH Exceptions, no update was given to OPSG on the December position.

Communication Service Provider Central & South (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 Data Service Provider (DSP). As this data is now available to the CSPs, the OPSG Chair stated that the report is likely to be rejected if these exceptions continue to appear.

Alerts

There has been further progress with addressing the number of rogue alerts, with no new instances of alerts from one type of single fuel installation. However, alerts generally continue at a very high level and represent around 80% of the traffic through the DCC systems. Overall, the total volume of alerts continues to increase. Of particular concern is that the root causes of a significant proportion of these alerts has not yet been reliably identified. The OPSG recognised that although the root cause of many of the alerts is not within the DCC systems, the DCC has been very active in using its tools to monitor

the alerts and facilitate the investigations. The OPSG reiterated the request for the DCC to provide a comprehensive plan for determining the root causes and coordinating remediation for each alert type.

Capacity Forecast

The DCC presented the first of what are planned to be regular briefings on service capacity. The DCC highlighted its assessment of the impact of the increasing volumes of Alerts: the DCC said the consequence of this would be the requirement for the deployment of further hardware infrastructure earlier than would otherwise be the case.

CSP N Installation failures/times and Service Stability

A Common Issues Forum has been established to monitor progress on CSP North (CSP N) issues.

The DCC has implemented some short-term fixes and is preparing a detailed plan for addressing the CSP N issues highlighted in December. The DCC reported that the CSP N performance in December had stabilised at the 'normal' level observed earlier in 2019.

Following feedback at the December OPSG meeting, CSP N has modified the approach to be taken for the audit/technical review due to complete in March 2020.

There was a Major Incident in CSP N during December caused by human error in the application of a change. As the failure was overnight there was no impact on Users. CSP N have changed their processes to ensure further checking of such changes.

Service Performance

Code Performance Measure 1 was again below target for the tenth month in succession. The DCC reported that whilst the situation was improving, the planned remedial actions being taken by CSP N and CSP C&S to get this measure above target by December 2019 had not been completed successfully and the DCC has been asked to give a revised completion date.

SMETS1 Migration

The OPSG noted that an issue has been identified with the master keys on one meter type, and concerns were raised regarding the exact number of Devices with this issue that are being migrated. The DCC noted that migrations had been suspended whilst the master key issue was under investigation. It intends to resume migrations early in January 2020, subject to agreement by the Responsible Suppliers. The DCC noted that it will be requesting OPSG approval to increase the migration rate under the governance arrangements agreed in December 2019.

Service Request Forecasting

The OPSG supported a plan by DCC to submit a modification to change the approach to Service Request (SR) Forecasting (SECP_76_1701_25 – Service Request Forecasting Problem Statement). The proposal involves the DCC using its historic usage patterns together with User business inputs to estimate future SR traffic. The DCC propose to trial the revised approach.

The OPSG asked that the DCC raise a Modification to consider the change, and that the Trial be included as part of the Modification Refinement stage. It is hoped that the trial could start in February. The OPSG also asked that the modification include consideration of the required accuracy of forecasts, which is currently set at 10%.

Should the trial be successful, and the modification approved, Users will no longer need to submit SR forecasts.

The OPSG welcomed this initiative by DCC, noting that it responded to concerns about the current process which have frequently been expressed by OPSG members.

Maintenance Trial Extension

At the December OPSG meeting, OPSG supported the DCC proposal that the maintenance trial continue until [MP092 'New Planned Maintenance methodology'](#) has been implemented or rejected, subject to a quarterly review at the OPSG. SECP_76_1701_10 sets out a proposal from the DCC to extend the trial.

Operational Metrics Review Project

The Operational Metrics Review Project evaluated the survey responses and held a User workshop to review User experience and existing metrics. Quick wins were identified and prioritised and one quick win trial report has been published. The Performance Measurement Report (PMR) issues log has been reviewed and updated. The scope has been confirmed as focusing on industry level metrics.

Process for addressing Party differences

The OPSG noted that the Panel has asked the OPSG to implement this process. Work is underway to prepare procedures and rules of engagement.

3. Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) reviewed one Full User Security Assessment (FUSA) and set one assurance status for a Shared Resource Provider in December 2019, details can be found in confidential Appendix A.

3.2 Verification Assessments

The SSC reviewed no Verification User Security Assessments (VUSAs) in December 2019.

3.3 Director's Letters

The SSC reviewed no Director's Letters in December 2019.

3.4 Security Self-Assessments

The SSC reviewed no Security Self-Assessments in December 2019.

3.5 SSC Highlights

Meter Triage Use Cases

The SSC discussed the outcome of a meeting held on 4 December 2019 between the SSC Chair (GH), BEIS and the National Cyber Security Centre (NCSC), where the Meter Triage Use Cases were discussed with regards to defining the security controls required at triage facilities and options to achieve a Factory Reset:

- For a Factory Reset, it was noted NCSC has concerns about any solution that would not adhere to GBCS security controls. NCSC did agree to consider an alternative approach to the one discussed at the Working Group on 6 November and this now needs to be documented for consideration by NCSC seniors.

- It was noted NCSC had no security objections to the Home Area Network (HAN) Reset Use Case and draft guidance was issued for review and comment to meter manufacturers, Meter Asset Providers (MAPs), SSC, BEIS and NCSC on 18 December 2019 with comments requested by 10 January 2020.

Security Self-Assessment Questions

The User Competent Independent Organisation (User CIO) presented new draft Security Self-Assessment (SSA) questions to the SSC, with the intention of asking more granular questions and adding questions relating to SMETS1 as part of the SSA. The new SSA questions agreed by SSC were included in the latest update of the Security Controls Framework (v1.19), which was published on 16 December 2019.

Interpretation of SEC G4.2

The User CIO raised a query on the interpretation of SEC G4.2 (b), specifically, who can compromise and affect, either directly or indirectly, the supply of energy. The User CIO sought the views of the SSC on three options on how this issue can be addressed without compromising security.

Potential risk of third-party Providers

The SSC discussed a paper submitted by BEIS which raised potential risks posed by third party Service Providers operating in the Smart Metering ecosystem and agreed that this issue requires further consideration.

SECMP0007 - Firmware updates to IHDs and PPMIDs

The SSC agreed to provide advice to the SEC Working Group regarding [SECMP0007 'Firmware updates to IHDs, PPMIDs and HCACLS'](#), noting that it does not wish to introduce any delay to the existing approach but suggesting that the Working Group consider whether the proposed solution will enable Device refurbishment.

CPA Remediation Plans

The SSC requested Remediation Plans from Suppliers by 20 January 2020 to upgrade EDM1 Devices to the latest firmware version since the Commercial Product Assurance (CPA) Certificates of existing EDM1 Devices are due to expire on 28 February 2020.

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; security testing; SMETS1 Certificate issues and Joint Industry Cyber Security Incident Management Plan (JICSIMP) scenarios.

3.6 SMKI PMA Highlights

Progressing enforced XML Signing

The SMKI PMA was updated on the proposals regarding use of an XML Signing Key for SMETS2 to ensure separation of the XML Signing Key for DUIS Commands from the use of a SMKI digital Signing Key for Pre-Commands. The SSC has initiated a SEC Modification for the DCC to introduce a technical control to validate that different Signing Keys have been used. BEIS is to consult in January 2020 on an XML Signing role to be included in SEC Section L3.18.

SEC Amendments

SEC Appendix L – Section 6

The SMKI PMA discussed the outcome of a meeting held on 2 December 2019 between DCC, BT, CGI, BEIS, the SMKI Specialist and SMKI PMA Chair, to discuss the ability of DCC, BT and CGI to operate the proposed changes to SEC Appendix L, Section 6. As a result, the SMKI PMA approved the draft of SEC Appendix L (SMKI Recovery Procedure) for BEIS consultation.

SEC Appendix D – SMKI Registration Authority Policies and Procedures (RAPP)

The DCC highlighted the proposed updates to SEC Appendix D following the Scheme audit finding that there are discrepancies between the DCC Work Instructions and the SMKI Registration Authority Policies and Procedures (RAPP). The SMKI PMA approved the proposed amendments to SEC Appendix D and agreed to raise a SEC Modification to align SEC Appendix D to the DCC's actual working practices.

Replacing SMKI Organisation Certificates

A Large Supplier presented the SMKI PMA with lessons learned from an experience regarding replacing SMKI Organisation Certificates.

SMKI Standards and Guidance Review

The SMKI PMA considered adopting an internal standard based on the Good Practice Guidelines (GPG) for GPG13, GPG43 and GPG45, as previously set out by NCSC but which have since been discontinued or changed.

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

4.1 TABASC Highlights

Market-Wide Half Hourly Settlements

ELEXON and Ofgem provided the TABASC with an update on Market-Wide Half Hourly Settlements explaining that the Target Operating Model introduces the use of Settlement Period level data for every meter. The Meter Data Retrieval (MDR) Service will retrieve Smart Meter data via the DCC with the Processing Service validating and estimating (where necessary) meter data and providing the data for each Meter Point Administration Number (MPAN) to the BSC Central Settlement Services.

The TABASC noted that there could be a significant impact on smart metering if the MDR is not the Supplier, potentially including the creation of a new SEC User Role and changes required to the security model. The TABASC strongly recommended that the MDR is implemented through Suppliers only and requested they review any proposed solutions to minimise any adverse consequences on the smart metering technical and business architecture.

DCC Change Coordination

The TABASC supported the simplified approach to the DCC Change Coordination for gaining information from Users. The complexity and significance of a change will also be considered by the DCC as part of the programme.

Alerts Lost during DCC outages – EUK problem statement

SECAS provided the TABASC with a problem statement and high-level assessment of options for minimising Alerts lost during DCC outages, where the TABASC recognised that multiple options would be necessary to deal with the majority of issues and even then, could not guarantee 100% delivery of Alerts. Further work to develop the options and their effectiveness in addressing the issues will be provided to the TABASC in February for consideration.

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

The DCC provided an update on options to extend the duration of 2G service and the provision of 4G/LTE Communications Hubs solution. The TABASC continue to request clarity on the business requirements to be used in the procurement process and have also provided feedback specifically on the timelines and need for further customer engagement.

Upcoming TABASC Projects

The TABASC supported the following Project Initiation Documents in December for:

- supporting the Market-Wide Half-Hourly Settlement project whereby the TABASC agreed participation in the Architecture Working Group until completion of the functional requirements for interfaces and data transfer, subject to confirming funding arrangements.
- supporting Market Structure Impacts (changes to other Codes that could impact the SEC and smart metering) specifically focusing on [BSC Modification P379 'Multiple Suppliers through Meter Splitting'](#). The TABASC agreed that the overall participation in industry changes and the proposed activities set out specifically for BSC Modification P379 engagement.

TABASC Principles for Assessing Modification Proposals

SECAS proposed an updated set of TABASC principles for assessing Modification Proposals and the TABASC agreed the approach for using the principles in the future, subject to applying minor amendments to enhance the existing principles.

4.2 TAG Highlights

The Testing Advisory Group (TAG) met on 16 December to discuss the following topics:

SMETS1 DMCT Standard Test Pack

The DCC has made several changes to the Device Model Combination Testing (DMCT) Test Pack based on the recommendations from TAG, including adding monitoring the number and frequency of Alerts generated, to allow visibility and management of excessive or spurious Alerts. The DCC also noted that the Test Pack will include some elements of security testing. The TAG suggested that any additional testing should be incorporated in the Test Pack and the TAG be consulted prior to the revised pack being made available to Testing Participants.

SMETS1 FOC

The DCC provided an overview of the comments received from TAG members on the Migration, Systems Integration Testing (SIT) and Regression Testing Approach Documents, along with the resulting changes made to those documents. The TAG confirmed that all of the points raised had been satisfactorily addressed, and approved all three documents.

The TAG raised concerns that there is a significant risk of environmental constraints arising as testing activities relating to the Final Operating Capability (FOC) for SMETS1 and the June 2020 SEC Release for SMETS2 will take place within a short period of time. The main concern was that if these

releases are linked to each other, testing timescales could be compressed if one or more of them are delayed.

The TAG noted that the current means of assessing whether one release could have an impact on another, for example if they share a common code-base, does not appear to be fit for purpose because the DCC previously informed TAG that there would be no impact on IOC testing activities due to the November 2019 SEC Release being implemented alongside it, which turned out to be incorrect. The TAG questioned how the DCC would manage this going forward and a detailed response is expected during January 2020.

SMETS1 IOC Aclara Items

The DCC presented an updated version of the Migration Depth & Breadth document and noted that the security testing section in the document is under review by the SSC. The DCC stated that if amendments are made to the document after the SSC's review, it will return to TAG for approval.

The DCC presented an overview of the Service Request Variant Testing (SRVT) Depth document. This provided an overview of the comparisons between the new Aclara document and the Elster document which was approved at previous meetings. No further comments were raised by the TAG.

SMETS1 MOC MDS Migration

During discussions of the SMETS1 Middle Operating Capability (MOC) MDS Migration document, the TAG stated that it does not want active meters to be migrated before the dormant and mixed Devices, and therefore the DCC should provide a statement of assurance that it will not migrate active Devices before dormant and mixed Devices. An alternative approach would be to split the document into two, with one covering active installations and the other containing dormant and mixed installations.

The TAG decided not to pursue this option at this time and requested that DCC provides a statement of assurance. It was highlighted that the Live Services Criteria review may be used to prevent active Devices from being migrated ahead of dormant and active ones.

5. Recommendations

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

Rebecca Jones

SECAS Team

10 January 2020

Attachments:

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