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_83_1408_20**	Corporate member of Plain English Campaign Committed to clearer communication 592
Action:	**For Information**	

SEC Panel Sub-Committee Report

1. Purpose and highlights

This paper provides the Panel with an update on recent activities from the Panel Sub-Committees, including 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.

Highlights for the Panel's attention include:

2. Technical Operations

2.1 TABASC Highlights

The TABASC met twice since the last update was provided. The meetings covered the following topics:

SECMP0007 'Firmware Updates to IHDs and PPMIDs'

The TABASC have provided input into the proposed solution ahead of the Panel decision, including the associated firmware distribution process for PPMIDs and HCALCs.

Alert Issues During DCC Scheduled Maintenance

The DCC presented the TABASC with its investigative findings of various aspects of HAN stability. The TABASC agreed that continued investigations are required but that it should be managed by the Technical Specification Issues Resolution Subgroup (TSIRS). The TABASC Chair will liaise with TSIRS Chair to confirm TABASC's monitoring role until TSIRS have concluded its activities.

Network Evolution: Summary of Analysys Mason Assessment of 2G/3G Networks Lifespan & Impacts on Smart Meters

The TABASC noted a DCC presentation on the summary of Analysys Mason's findings and recommendations surrounding the likely lifespan of 2G/3G networks and the associated impacts on the smart metering communications network.

Network Evolution: Communications Hub Minimum Viable Product (MVP) Technical Specifications

The TABASC supported the DCC's latest position of Cat1/2G for the RFP process, however, requested DCC provide plans that consider a switch to Cat1/M once the viability of Cat1/M has been confirmed.

Network Evolution: DSP Re-Procurement Update

The DCC presented an update on the DSP re-procurement programme and the TABASC requested that the DCC returns to a future meeting with a revised Problem Statement to clearly articulate the areas the DCC is aiming to solve.

Network Evolution: Managing Backward Compatibility across Communications Hubs

The DCC provided an update on the options for current operating models for CH maintenance to enable coexistence with future 4G CH. The TABASC noted the update and next step is for the DCC to provide the principle proposal of an approach.

Market-Wide Half Hourly Settlements Consultation Response

SECAS provided the TABASC with an update on the main challenges introduced by Market-Wide Half Hourly Settlements (MWHHS) including the capability for a Supplier to retrieve HH data and capacity constraints which will be placed on the smart metering network. The TABASC agreed to option 2 in the paper, which includes the need for a New User Role and MWHHS specific Service Requests with extended Target Response Times. This position will feed into the TABASC response to the associated Ofgem consultation.

SECMP0067 'Service Request Traffic Management'

The TABASC noted SECAS update on SECMP0067 'Service Request Traffic Management', following the ad-hoc Working Group on Thursday, 9 July, and the Second Refinement Consultation which closed on Monday, 3 August. The TABASC agreed an implementation model whereby the capability is included in the SEC at the earliest opportunity, however the DUIS changes are implemented in the November release alongside a number of the other DUIS changes.

DCC Power Outage Alert Programme

The DCC informed the TABASC of its Power Outage Alert Programme, which is designed to improve the performance of Alerts in terms of timing, volume and quality. The TABASC requested that the DCC returns to a future meeting with more information about its proposed requirements and technical solutions.

Phase 2 of the DSP Northbound Message Cache Issues

The DCC provided an update on the Phase 2 of the DSP Northbound Message Cache Issues, including its intent to increase the size of the cache to provide a longer period of continued operation should Service Users experience Service Outage. The TABASC provided feedback including its preferred option for the proposed enduring solution and noted the need for good governance associated with the change.

CSP North Performance

The DCC presented the TABASC with a view of CSP North Performance and the TABASC requested that the DCC returns to a future meeting to discuss other performance parameters and a view on scalability options. The TABASC will monitor this area going forward.

New Draft Proposals and Existing Modifications Proposals Updates

Updates were given on new Draft Proposals including:

- DP136 'Enduring ICHIS Compliance Related to RF'

- DP137 ‘Sharing information on Defects and Issues’, in which the TABASC expressed its interest and request to be involved in the process.
- DP138 ‘DCC Service Testing in ETAD’

The TABASC also noted updates on multiple Draft and Modification Proposals for which it had previously requested due to the potential impacts on technical and/or business architecture, including

- SECMP0024 ‘Enduring Approach to Communication Hub Firmware Management’
- MP125 ‘Correcting the ESME variant’
- MP131 ‘Default maximum demand configuration conflict’
- MP134 ‘Use of SMKI Certificates relating to a SoLR event’

2.2 TAG Highlights

The Testing Advisory Group (TAG) met twice in July to discuss the following topics:

SMETS1 MOC Secure SIT-A test completion

Systems Integration Testing (SIT) was split across two testing environments for MOC Secure. Most of the testing was conducted in the SIT-B environment, with some deferred and additional testing carried-out in SIT-A. During this reporting period the TAG reviewed SIT completion for the testing carried-out in the SIT-A environment.

One Severity four Testing Issue was discovered during regression testing, which requires a 100% pass rate. The associated defect does not impact Users and does not have a detrimental impact on DCC’s operational performance, so the TAG agreed that this Testing Issue should be recorded as an exception.

The TAG approved MOC Secure SIT-A test completion.

SMETS1 uplift 1.2 Test Approach Document

The DCC provided the TAG with the Testing Approach Document (TAD) for the SMETS1 Core Uplift 1.2. The scope of Uplift 1.2 has been reduced and will now comprise only two changes, with the other four being removed as they do not result in or require amendments to the SEC. The changes which have been removed from scope will be included in the Appendix of the TAD to ensure visibility of the changes.

The TAG discussed whether the agreed defect tolerances should be reduced proportionally to the reduction in scope. It was concluded that the agreed tolerances should remain the same and that any defects relating to the de-scoped changes will be measured against the threshold if they have a material impact on the changes which remain in-scope.

The TAG requested that the DCC makes several changes to the document and will review it again once these are complete.

November 2020 SEC Release testing update

The DCC presented the November 2020 Testing Update and highlighted that the emulators that will be used to conduct testing will not be Zigbee certified when a test completion decision is sought. From the TAG. The DCC advised that it will be running comparable testing, and that the emulator stack is based on a previously Zigbee certified stack, with all the changes that were made being limited to the messaging layer, which represents a low risk.

The TAG agreed with the DCC's assessment of the level of risk.

Faster Switching Scope of DSP Changes

The TAG is overseeing governance of the elements of testing within Ofgem's Faster Switching programme which relate to the interface between the forthcoming Central switching Service (CSS) and the existing DCC Systems. The DCC requested the TAG's approval of the document that defines the scope of the testing which the TAG will oversee, along with the criteria that must be met to allow the successful completion of testing.

The TAG approved the Switching Scope of DSP Changes document.

Network Evolution – Early TAG Engagement

The DCC provided the TAG with a Network Evolution Update in response to some requests for clarification which the TAG had made during previous presentations.

The DCC confirmed that it will ensure that regression testing will validate backwards compatibility of Network Evolution Communications Hub. However, due to the scale of Device Model Combinations (DMCs) currently deployed in the production environment the DCC will be unable to regression test all combinations of Devices. To mitigate this, the DCC will identify the most representative Meter installations in production, along with those DMCs which are known to be problematic, and will use these to conduct regression testing. Users will be consulted regarding the Devices which the DCC identifies for use in regression testing.

The DCC confirmed that because the Network Evolution programme will focus on making changes to the Wide Area Network (WAN), it is not expecting to use emulators during testing and will use real Devices. However, some test conditions cannot be easily triggered using real Devices, particularly during negative testing where unusual events need to be simulated. Because of this, Emulators will form some part of the testing strategy in these limited circumstances.

2.3 Operations Group Highlights

Pandemic Response Update

The DCC provided an overview of the operational status of DCC critical services and staff. The DCC confirmed that at present both its own operations and those of the Service Providers are operating without impact ("green" status), although it was noted that constraints on site working have impacted CSP activities.

The DCC noted that installations continue to follow an upward trend with daily figures now averaging around 65% of pre-Pandemic volumes.

Major Incident review

The OPSG reviewed the Major Incident Report for INC000000599486. The Incident occurred on 17 June 2020 and the time taken to restore the service was 3 hours and 4 minutes. This incident led to all SMETS1 Service Requests failing. SMETS1 Migrations and the SMETS2 Service were not impacted. The DCC has implemented additional monitoring to mitigate the recurrence of this issue. Further remediations will be introduced as part of the DCO stability plan uplift.

The OPSG reviewed the Incident timeline and highlighted concerns with the initial engagement between the DCC's Major Incident Management (MIM) and the DCO service desk. The OPSG also questioned the categorisation of the incident, and, in particular the time taken to recognise the severity of the event. The DCC acknowledged the concerns raised and noted that they are working

with the DCO on lessons learnt regarding rules of engagement and escalation paths. The DCC agreed to amend the report to reflect the concerns raised, and OPSG will provide any further comments within five days of the report being recirculated.

SMETS1: Secure MOC Readiness Major Incident Summary

Earlier in the month, the OPSG carried out several assessments of the status of the Live Services Criteria related to Secure MOC. The OPSG recommendation from these was that concerns remained related to the stability of the existing services, but that it would be acceptable to proceed with an initial low volume of migrations.

Subsequent to the OPSG recommendation being made, information on further defects came to light, and there were a further two Category 2 incidents. Consequently, the DCC decided that service stability had not been achieved. BEIS also took the decision to postpone the addition of SMETS1 MOC Secure to the Eligible Product Combination List (EPCL) due to the SMETS1 service stability and defects detected in User Testing.

At the last OPSG meeting, the DCC provided a summary of the SMETS1 Incidents affecting the service since 27 May 2020 and the mitigations and remediations that are being implemented. There have been 14 High impact (category 1 and 2) incidents regarding the SMETS1 Service in the period from 27 May 2020 to 27 July 2020. The DCC have encountered three SMETS1 incidents following the deployment of the Network Database (NDB) on 14 July 2020. A further fix has been scheduled for the NDB code on 4 August 2020 that the DCC are confident will introduce stability to the service.

The DCC postponed the deployment of the SMETS1 MOC Secure code due to poor stability of the DCO SMETS1 Service over the last two months. The DCC are proposing to progress with the code deployment on the weekend of 15 August 2020 subject to DCC Operational Acceptance. The OPSG raised concerns about the timescales available to demonstrate the stability of the service before the first EPCL entry for Secure is considered by BEIS. The DCC have set the Go Live criteria as a minimum of 5 days without incident. However, OPSG members noted that they had previously indicated they did not consider this to be adequate in the current circumstances, in particular given the recent history of category 1 and 2 incidents.

. It is understood that BEIS have agreed Go Live criteria with DCC and are aiming to reconsider the EPCL addition following DCC's Operational Acceptance on 14 August 2020. The current plan is to commence the first SMETS1 MOC Secure migrations on 24 August 2020.

Spurious Alerts

The OSPG noted the continued reduction of the 8F3E Spurious alerts in CSP C&S, due to the mass rollout of WNC CH Firmware. There are now under 8million 8F3E alerts being generated daily (reduced from 50million 8F3E alerts a day at the end of June). The DCC are working with Suppliers and Manufacturers to investigate and resolve the devices that continue to alert.

The DCC noted that the 8F12 alerts in CSP N have started to increase in line with installation activity. The fix will be implemented as part of the Release 2.0 CH Firmware, which has been on hold since March. A micro pilot commenced on 27 July 2020 for v2.02.6 of the firmware, with a target date of 22 September 2020 to begin mass rollout.

Aged Incidents and CH Exceptions

The DCC reported a slight increase (approx. 4%) in Aged Incidents since the previous report.

The DCC presented an outline proposal regarding the management of Incorrect CH variant Incidents. The intention is that the DCC will only raise new Incidents where the coverage recommendation is

defined as a “Gateway” hub and an incorrect CH variant has been installed. The OPSG requested that the DCC confirm this proposal would not contradict any SEC requirements regarding incidents on CH variants, and asked that DCC provide a detailed description of the proposal and its benefits and implications.

The DCC noted that the figures reported for CH exceptions are being reviewed, with changes expected. The OPSG raised concerns that the figures indicated that over 250k CHs in CSP N appear to be subject to the exception “No Incident for Outage”. The DCC are engaging with CSP N to investigate this and identify whether there are any gaps in the management of these exceptions.

SEC Release – November 2020

The DCC presented a 3-month checkpoint review of progress for the SEC Release November 2020. The OPSG noted that the approved Go-Live date is now 29 November 2020. The DCC reported that there were currently no issues and that all activities were on track.

The OPSG requested that the DCC confirm the intended target date for the consultation on the SSI proposals.

The OPSG will have a 2-month review of progress at the September meeting (OPSG_36)

Service Performance

Code Performance Measure (CPM) 1 was below Target Service Level. CPM1 has not been above Target Service Level in the previous 12 months, with only 3 reporting periods above Minimum Service Level. The Service Provider Performance Measure (PM) 2, percentage of firmware payloads delivered within Target Response Time (TRT), has been a consistent factor in this poor performance.

The DCC provided an update at the OPSG Reporting Meeting (OPSG_34xxx), indicating that they aim to achieve a service level of 92% for PM2 by October 2020, which is below the minimum service level. The DCC and CSP N noted that they are investigating how to achieve the SLA requirements and will be able to provide, by October 2020 at the latest, a plan showing how they will achieve the SLA requirements.

The DCC reported that the reporting tool error has now been fixed, but they have yet to establish exactly when the error was introduced. CSP N has now regenerated the reports for the previous regulatory year (2019/20) and are in the process of producing the remaining reports. They have confirmed the error was introduced prior to April 2018 and that they will now investigate further back to January 2018. DCC will need to restate and resubmit the affected PMR reports.

Engagement with DCC on Network Evolution Proposals

The OPSG is looking forward to engaging with the DCC on this topic and has been awaiting information presenting the operational perspective and impacts of the proposals. It is expected that it will be possible to start structured engagement at the end of August.

3. Security Sub-Committee and SMKI PMA

3.1 Assurance and Compliance Status Decisions

The Security Sub-Committee (SSC) set the assurance status for three initial Full User Security Assessments (FUSAs) and two Follow-Up Security Assessments (FSAs) in July 2020.

The SSC set the compliance status for two Verification User Security Assessments (VUSAs) and one second or subsequent FUSA. Details can be found in confidential Appendix A.

3.2 Security Self-Assessments

The SSC reviewed three Security Self-Assessments in July 2020.

3.3 Director's Letters

The SSC reviewed one Director's Letter following a Verification User Security Assessment (VUSA).

3.4 SSC Highlights

SMETS1 Enrolment and Adoption

The SSC noted DCC updates regarding the different aspects of SMETS1 enrolment including the DCC's Active and Monthly Dormant Migration Process, CIO report updates, Home Area Network (HAN) Control Assurance, Middle Operating Capability (MOC) Morrison Data Services (MDS) Cohort, Device Model Combination Testing (DMCT) Tranches; the HAN Control Testing Document, and the MOC Secure Live Service Criteria.

DCC Interoperability Tracker

The SSC noted an update from the DCC on proposals relating to the Interoperability Checker service and confirmed that no security issues have been identified that would prevent the DCC 'back end' element of the service from proceeding to testing with the Citizens Advice Bureau 'front end'. Going forward the SSC will receive ongoing updates related to the Interoperability Tracker as a complete service and have an opportunity to advise on the security matters prior to the live service commencing in October 2020.

Anomaly Detection

The SSC noted DCC updates on the management information relating to Anomaly Detection Threshold breaches in June 2020, whilst requesting granularity on critical Service Request Variants (SRVs) regarding information displaying ADTs separated by Users and Service Requests.

SOC2 Update

The SECAS Security Experts recently validated the two outstanding observations from the SOC2 2018 Report;

- Monitoring of Relevant Patch Updates
- Security Clearance Checks

SECAS and the SSC were satisfied with the response for both observations, allowing remediation of actions to address the findings of the SOC2 2018 Report to be closed and reported to the SEC Panel as required by SEC Section 7.19(g).

The SSC also approved the scope of the 2020 SOC2 Report under delegated authority from the SEC Panel as required by SEC Section 9.3(c).

Factory Reset Guidance

The SSC Chair presented proposals for the Factory Reset Use Case Guidance (004) that had been approved by BEIS and NCSC which was subsequently approved by SSC and published to the SEC website alongside the associated sequence diagrams. Members have since noted that the guidance was well received by the Community of Meter Asset Providers (CMAP).

Quarterly Standards Review

The SECAS Security Expert presented the latest Quarterly Standards Review which was subsequently approved by Members and published to the SEC website.

SSC Risk Register Review

The SSC noted an update from SECAS on the SSC Risk Register and assessed the impact and likelihood levels for all open SSC risks, including the addition of a new risk.

Supplier of Last Resort

The SSC Chair and TABASC Representative presented an alternative solution to SEC Modification MP134 'Use of SMKI Certificates relating to a SoLR event' in order to protect prepayment consumers when a failed Supplier leaves the market in a disorderly fashion. SSC Members agreed to support the alternative solution as it is more secure than the existing proposed solution.

New Draft Proposals and Modifications Proposals Updates

Updates were given on new Draft Proposals and Modification Proposals including:

- DP136 'Enduring ICHIS Compliance Related to RF'
- MP135 'Correcting equivalence in Security Standards'

The SSC also noted updates on multiple Draft and Modification Proposals for which it had previously requested due to the potential impacts on security.

3.5 SMKI PMA Highlights

SMKI Testing

The SMKI PMA was updated on SMKI testing by the DCC, considered the proposed scope and approach for Phase 2 of testing, and provided feedback to the DCC.

SMETS1 Symmetric Keys

The DCC provided the SMKI PMA with an update on the use of Symmetric Keys in SMETS1 environments and the SMKI PMA agreed to set up a Working Group (WG) between interested Members and the DCC to discuss the approach to meeting the SEC obligations in Section L14.7.

SMKI PMA Guidance for GPG13 (MP115)

In support of SEC Modification MP115, the SMKI Specialist provided the SMKI PMA with the draft SMKI Guidance to replace outdated National Cyber Security Centre (NCSC) Good Practice Guide (GPG) 13, relating to protective monitoring, and the SMKI PMA was content to recommend the SMKI Guidance to the SSC for approval.

MD5 Audit Identification of Environments

The DCC provided the SMKI PMA with an update on the outcome of a recent DCC audit regarding the use of a deprecated hash algorithm MD5 in DCC environments and Members requested further information from the DCC to be considered at the August meeting.

DP128 'Gas Network Operations SMKI Requirements'

The SMKI PMA approved multiple recommendations regarding a potential solution for DP128 'Gas Network Operations SMKI Requirements', subject to further analysis by the DCC, and provided feedback on an ongoing issue related to the Modification.

DP134 'Use of SMKI Certificates in a SoLR Event'

The SMKI PMA considered an alternative solution for DP134 'Use of SMKI Certificates in a SoLR Event' and agreed that the more secure option should be considered for implementation, subject to the outcome of an impact assessment.

New Draft Proposals and Modification Proposals

The SMKI PMA noted updates on Draft Proposal 135 – Draft Proposal 136 and agreed there are no potential impacts on SMKI.

4. Recommendations

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

Cecily Bain

SECAS Team

7 August 2020

Attachments:

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