Security Sub-Committee (SSC) 84_2808

28 August 2019 10:00 – 16:00

Gemserv Office, 8 Fenchurch Place, London, EC3M 4AJ

SSC_84_2808 – Meeting Headlines

Matters Arising

Updates were noted on the following Matters Arising:

- The SSC **NOTED** an update regarding a proposal relating to SEC obligations G3.17 to G3.20 which offers a solution for those Suppliers struggling to obtain a fully signed Meter Asset Provider (MAP) contract due to commercial negotiations. (**GREEN**)

- The SSC **NOTED** an update on questions relating to SEC obligation G5.27 which requires Users who employ Shared Resource Providers to notify the SSC every six months of the number of Smart Metering Systems that can send Critical Service Requests.(**GREEN**)

- The SSC **NOTED** questions posed by Users to the SSC regarding scheduling User Assessments and the volumes of enrolled SMETS1 Devices. Two scenarios were reviewed, and a decision will be made at a future SSC meeting. (**RED**)

- The SSC **NOTED** a signed MAP contract from Small Supplier 'BO'. (**RED**)

- The SSC **NOTED** an update from a previous Large Supplier Representative who has since left, questioning whether support is available in User Systems for the partitioning of SMKI XML Signing Certificates for SMETS1. (**RED**)

- The SSC **NOTED** Confidential Minutes from the SSC meeting held on Wednesday 27 February 2019 which were circulated for re-approval based on an unminuted action that required clarification at a Supplier of Last Resort (SoLR) Workshop. SSC members were requested to review the post-meeting note and provide comments to the Secretariat by Wednesday 4 September 2019. (**GREEN**)

Gemserv

This document has a Classification of **White**

Items for Decision/Discussion

1.   Previous Meeting Minutes and Actions Outstanding

The SSC noted no comments were received for the Draft Minutes and Confidential Draft Minutes from the SSC meeting held on Wednesday 14 August 2019, and the SSC **APPROVED** the Draft Minutes and Confidential Draft Minutes as written.

All outstanding actions were marked as complete or on target for completion, with several updates provided under separate meeting agenda items.

2.   Full User Security Assessment – Small Supplier 'CH' (RED)

The SSC considered Small Supplier 'CH's Full User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** to defer the decision on setting an Assurance Status for Small Supplier 'CH'.

3.   Director's Letter – Small Supplier 'C' (RED)

The SSC considered Small Supplier 'C's Director's Letter. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** Small Supplier 'C's Director's Letter.

4.   Director's Letter – Small Supplier 'AK' (RED)

The SSC considered Small Supplier 'AK's Director's Letter. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** Small Supplier 'AK's Director's Letter.

5.   Remediation Plans (RED)

The SSC **NOTED** the following Remediation Plans submitted:

- Small Supplier 'AX';
- Small Supplier 'P';
- Small Supplier 'AB'; and
- Small Supplier 'AC'.

The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

This document has a Classification of
White

6. Security Self-Assessment – Shared Resource Provider 'A' (RED)

This Agenda Item has been deferred until the Security Self-Assessment has been reviewed by the User CIO and SECAS.

7. NIS/CAF Alignment with the SEC/SCF (AMBER)

The SSC Chair provided an update following the SSC meeting on Wednesday 22 May 2019 at which the SSC considered that the SEC and guidance in the Security Controls Framework (SCF) could be equivalent to the Network Information Security (NIS) / Cyber Assessment Framework (CAF) requirements in order to provide an economical approach to assurance for Operators of Essential Services (OES). The SSC **NOTED** the recommendations and proposed amendments to SCF Part 2 and Agreed Interpretations v1.9.

The SSC **NOTED** the update and **APPROVED** SECAS to amend the Security Controls Framework and approved the publication of Agreed Interpretations v1.9. The Agenda Item was marked as AMBER and therefore recorded in the Confidential Minutes.

8. CPA Monitoring (AMBER)

Communications Hub CPA Conditions

The SSC **NOTED** the update in relation to a Communications Hub with Commercial Product Assurance (CPA) Conditional Certification and an update on a Communications Hub firmware upgrade status.

The Agenda Item was marked as AMBER and therefore recorded in the Confidential Minutes.

Withdrawn Certificates Decision

The SSC **NOTED** the update in relation to Withdrawn and soon to be Withdrawn CPA Certification Certificates.

The Agenda Item was marked as AMBER and therefore recorded in the Confidential Minutes.

Early Expiry of Smart Meter Certificates

The SSC **NOTED** an update in relation to a notification from NCSC of a notice provided to a Device manufacturer that the existing CPA Certificate will expire early on Friday 28 February 2020 arising from an Optical Port within the Device that is non-compliant with the CPA Security Characteristics. The SSC **AGREED** to notify Parties to allow six months' notice for planning purposes In line with SEC Section F2.7.

The Agenda Item was marked as **AMBER** and therefore recorded in the Confidential Minutes.

9. **SMETS1 Update (RED)**

Remediation Plan

An update was provided on the updated Remediation Plan submitted by the DCC, noting which actions are still outstanding on the Initial Operating Capability (IOC) SMETS1 Service Provider (S1SP).

The SSC **NOTED** the update. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

CIO Report

It was advised that the DCC are still awaiting CIO review comments of the Management Response from their Communications Service Provider (CSP) before issuing the full final report and comments to the SSC.

The SSC **NOTED** the update. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

New PKI for MOC

The SSC was informed of issues being addressed for Middle Operating Capability (MOC) due to ongoing engagement with specialist manufacturers of Devices for MOC and work being undertaken to bring a Public Key Infrastructure (PKI) into SEC governance.

The SSC **NOTED** the update. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

New PKI for FOC

The SSC was informed that a Final Operating Capability (FOC) PKI Option paper had been updated to clarify the DCC's risk position and to clarify work being undertaken to bring a Public Key Infrastructure (PKI) into SEC governance.

The SSC **NOTED** the update. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

JICSIMP Updated Actions

Following the last SSC meeting at which a high-level scenario for the Joint Industry Cyber Security Incident Management Plan (JICSIMP) was discussed, the DCC will be in a position to bring details of proposed testing to a future SSC meeting.

The SSC **NOTED** the update. The Agenda Item has been marked as **RED** and therefore recorded in the Confidential Minutes.

10.   Enduring CH Firmware Release (AMBER)

The DCC provided an update on the ongoing work which will allow the DCC to proactively monitor Comms Hubs firmware upgrades. The DCC provided the approach and scope of the Security Risk Assessment before providing examples of the proposed security controls and mitigated risks.

The SSC **NOTED** the update. The Agenda Item has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

11.   Post Commissioning Report (RED)

The SSC was provided with an update in relation to the monthly Post Commissioning Report which provides information on the number of relevant SMETS2 Devices where the Responsible Supplier or DCC has failed to complete its Post-Commissioning obligations in accordance with Section 5 of Appendix AC of the SEC.

The Agenda Item has been marked as **RED** and therefore recorded in the Confidential Minutes.

12.   Risks from TCoS (AMBER)

The SSC were presented with an overview of the current and projected risks associated with the Transitional Change of Supplier (TCoS) activity whilst noting potential controls to address any residual risks.

The SSC **NOTED** the update which has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

13.   TABASC Effectiveness Review Survey

The SSC was provided with an update regarding the TABASC Effectiveness Review survey which will be sent to operational DCC Users or those SEC Parties undergoing the User Entry Process. The survey will be issued in September 2019 and Parties will have one month to respond to help identify areas in the current technical and business architecture where attention may be required.

14.   New Draft Proposals and Modification Proposals

SECAS provided updates to the SSC regarding several Draft and Modification Proposals and noted which ones the SSC were interested in receiving further updates on:

- DP080 'Ensuring a managed move to DUIS version 3.0' - the SSC confirmed it was interested in a further update;
- DP081 'Alignment of DUIS and CHISM to reflect current DCC Processing' – noted the update;
- DP082 'Alt HAN Channel Selection' - the SSC noted the update;
- MP077 'DCC Service Flagging' - the SSC noted the update;
- MP078 'Incorporation of multiple Issue Resolution Proposals into the SEC - Part 2' - the SSC confirmed it was interested in a further update; and
- MP075 'Third party metering service providers' - it was confirmed the proposer decided to withdraw this Modification on Wednesday 14 August 2019.

The SSC **NOTED** the updates and was invited to provide any views and comments on the proposals.

15. SECMP0067 Business Case

The SSC was provided with an update regarding SECMP0067 'Service Request Traffic Management' noting the DCC System has a finite capacity. The Proposed Solution is to define a maximum system capacity, operating threshold and appropriate Service User allocations, which has been assessed by the DCC and considered by the Working Group and has now been issued for Refinement Consultation to seek wider industry views.

The SSC **NOTED** the update and was invited to provide any views and comments on the proposals.

16. Standing Agenda Items (RED)

The SSC were provided with updates on the following standing agenda items:

- Anomaly Detection Update (**RED**);
- Shared Resource Notifications (**AMBER**); and
- Security Incidents and Vulnerabilities. (**RED**).

17. Any Other Business (AOB)

Four additional items of business were raised which were classified as **RED** and therefore recorded in the Confidential Minutes. No further items of business were raised, and the SSC Chair closed the meeting.

Next Meeting: Wednesday 11 September 2019

SSC_84_2808 – SSC Meeting Headlines

Managed by

Gemserv

Page 6 of 6

This document has a Classification of
White