This document is classified as **Green.** Information can be shared with other SEC Parties and SMIP stakeholders at large, but not published (including publication online).

Security Sub-Committee (SSC) Meeting

SSC_75_1004, 10 April 2019

10:00 – 16:00

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

Final Minutes

Attendees:

Party Category / Representing	Name
SSC Chair	Gordon Hextall (GH)
SECAS	Nick Blake (NB)
SECAS (Meeting Secretary)	Holly Burton (HB)
SECAS	Connie Muir (CM)
SECAS Security Expert	Kwadwo Anim-Appiah (KAA)
TABASC Representative	Julian Hughes (JH)
BEIS Representative	Daryl Flack (DF)
User CIO	Alistair Grange (AG) (part) teleconference
User CIO	Mark Richardson (MR) (part) teleconference
DCC	Alex Brown (AB) (part)
DCC	Frederick Wamala (FW) (part)
DCC	Tim Dunning (TD) (part)
Actica	Jonathan Watson (JW) (part)
Gemserv	Andy Green (AG) (part)
Gemserv	Adam Harrison (AH) (part)

Voting Members Present:

Party Category / Representing	Name
Large Supplier	Graham Eida (GE)

Party Category / Representing	Name
Large Supplier	Fabien Cavenne (FC)
Large Supplier	Gordon Millar (GM)
Large Supplier	Manoj Odedra (MO)
Large Supplier	Martin Christie (MC)
Large Supplier	Crispin Brocks (CB)
Shared Resource Provider	Simon Crouch (SC)
Other User	Michael Snowden (MS)
DCC	Ian Speller (IS)

Apologies:

Party Category / Representing	Name
DCC	Russell Kent-Smith (RK-S)
Gas Networks	Alastair McMurtrie (AM)

Introductions and Matters Arising

The SSC Chair (GH) welcomed all attendees to the meeting held on 10 April 2019, and advised attendees of the running order, timings of each agenda item and noted apologies.

Matters Arising:

- The SSC were informed that two papers were drafted and circulated to Panel members on Friday 5 April 2019 in relation to User Security Assessments highlighting any non-compliances during the Verification User Security Assessment stage. It was confirmed that no Events of Default had been recommended, excluding one which was currently under review at the SSC. A second paper was also circulated to Panel members highlighting the SSC process for CPA Security Characteristics (SC) Modifications.

- The SSC **NOTED** the update in relation to a Smart Metering Information Exchange (SMIE) meeting and a subsequent proposal for Chairmanship of the meetings. (**GREEN**)

- The SSC were provided with an update in relation to mitigating Security risks from internet-connected devices on which the Gemserv team had previously presented to the SSC. The SSC Chair confirmed a research paper was being drafted and would seek to focus on the core vulnerabilities and mitigating risks as agreed during a teleconference with Gemserv Representatives. (**GREEN**)

- SSC Members reviewed the forward plan for scheduled Security Assessments.

1. Minutes and Actions Outstanding

The SSC noted that no comments were received on the Draft Minutes, however one set of comments was received from a Large Supplier Representative for the Confidential Minutes from the SSC meeting held on Wednesday, 27 March 2019. The SSC **APPROVED** the Draft Minutes and Confidential Minutes as modified.

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

Action ID	Action	Owner
SSC 74/01	SECAS to develop a guidance document to support SEC Parties in applying ISO 29147, Standards to help satisfy the requirements of Duty to Notify and Be Notified.	SECAS
SSC members were informed that an update would be provided at a future meeting due to ISO 29147 not yet being released. The SSC agreed to leave the action open. Action: **Open**		
SSC 74/02	SECAS to develop a guidance document to support SEC Parties in applying ISO 30111 Standards to help satisfy the requirements on the Duty to Notify and Be Notified.	SECAS
SSC members were informed that an update would be provided at a future meeting noting that a draft version of ISO 30111 has been identified which can be used to support the development of a guidance document in the interim. The SSC agreed to leave the action open. Action: **Open**		
SSC 74/03	The TABASC Representative (JH) to write up the use cases arising from SECMP0013 Meter Triage in detail in order to share with SSC members.	TABASC Representative (JH)

Action ID	Action	Owner
SSC members were informed that a strawman use case has been written and is currently under review by the National Cyber Security Centre (NCSC). Once this has been reviewed by NCSC, it will be presented to TSIRS for further review and brought back to SSC with any comments. The SSC agreed to leave the action open until the written use case has been agreed by NCSC and manufacturers. Action: **Open.**		
SSC 74/04	The DCC to confirm that the proposed processes for firmware upgrades and clearing Devices can be achieved without any system changes.	DCC
SSC members were informed that the DCC Representative (IS) would present an update at the next SSC meeting currently scheduled for Wednesday 24 April 2019. SSC members agreed to leave the action open until an update has been received. Action: **Open.**		

3. Verification User Security Assessment – Small Supplier 'Z' (RED)

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

The SSC **AGREED** the Compliance Status for Small Supplier 'Z'.

4. Verification User Security Assessment – Small Supplier 'AN' (RED)

The SSC considered Small Supplier 'AN's Verification User Security Assessment. The agenda item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Compliance Status for Small Supplier 'AN'.

5. Verification User Security Assessment – Small Supplier 'AM' (RED)

The SSC considered Small Supplier 'AM's Verification User Security Assessment. The agenda item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Compliance Status for Small Supplier 'AM'.

6. Directors Letter – Small Supplier 'BP' (RED)

The SSC considered Small Supplier 'BP's Directors Letter. The Agenda item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** the Director's Letter for Small Supplier 'BP'.

7. Director's Letter – Large Supplier 'J' (RED)

The SSC considered Large Supplier 'J's Directors Letter. The Agenda item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** the Director's Letter for Large Supplier 'J'.

8. Outstanding Actica Work (RED)

CPA Gap Analysis SEC VS CPA Assurance and Release 2 Risk Assessment

The SSC were provided with an update in relation to the additional work commissioned from Actica in May 2018. Actica previously conducted a partial risk analysis of DCC Release 2, however, the SSC had since requested that the work should include Dual Band Comms Hubs. Actica also provided a Gap Analysis to compare security assurance in the SEC versus assurance provided via the Commercial Product Assurance (CPA) Scheme in order to identify whether additional CPA or SEC requirements are needed.

The SSC **NOTED** the contents regarding the security matters relating to Dual Band Comms Hubs and the CPA Analysis which had provided a Gap Analysis and identification and calibration of Residual Risks.

The SSC **NOTED** the update and **AGREED** several recommendations which have been marked as **RED** and therefore recorded in the Confidential Minutes.

9. Security Controls Framework

An update was provided to the SSC specifically, proposed changes to the guidance for:

- what constitutes a SMETS1 'Appropriate Standard' for inclusion in the Agreed Interpretations (AIs);
- additional steps to take place as part of the DCC On-Boarding Process; and

- the Assessment type and frequency for Non-Domestic Supplier Parties and Other Users.

The SSC Chair (GH) confirmed the new section added to Section 4.5 of the Security Controls Framework (SCF) Part 2 v1.16 which noted '*The SSC has published guidance on achieving an 'Appropriate Standard' in the Agreed Interpretations* and *Appendix B of the SCF Part 2 will shortly be amended to explain what the User CIO will look for when assessing an 'Appropriate Standard' for an enrolled SMETS1 SMS'.*

The SSC Chair (GH) informed SSC members that a new section (11) had been added to the Agreed Interpretations V1.7 which noted the scope of the Supplier's responsibility for ensuring an 'Appropriate Standard' had been applied to their SMETS1 Device assurance and what to expect from future User Security Assessments

The SSC were also informed of the new addition to the SCF Part 2 Appendix E - To facilitate a smoother and more efficient process, steps have now been agreed between the SSC and the DCC to allow DCC User Onboarding steps to be completed in parallel before final sign off of Director's Letters.
It was confirmed that to commence the PP1 Live connectivity test with the DCC, Users will need an assurance status of 'Approved' or 'Approved Subject to;' with a Director's Letter, explicitly approved by the SSC before live operations can start.

The SSC Chair (GH) highlighted the amendments to the Security Controls Framework Part 1, Section 4.3. It was confirmed that the User Security Assessment frequency table had been adjusted as per SECMP0059 to include Supplier Parties who supply Non-Domestic premises in the User Assessment Cycle, and also amended the Year Two Assessment Type for Other Users.

The SSC **NOTED** the update and **AGREED** the amendments made to the SCF and AIs.

10. Timing of Third and Subsequent User Assessments (GREEN)

The SECAS Representative (NB) provided an update relating to an updated paper which was circulated to members in Egress on Wednesday 3 March 2019. The SSC noted the current process whereby the second-year assessment must be scheduled within 12 months from the date that the original Assurance Status was set by the SSC. The Assessment must then be completed within a further 12 weeks. However, the period between completing the Assessment and setting a Compliance Status for Verification User Security Assessments is variable, depending on time taken to finish the User Management Response validation for SSC review and, if necessary, subsequent completion of a remediation plan.

The SSC was assured that the process for scheduling a second-year Assessment would remain the same, however, the User would now be required to schedule their third-year and subsequent Assessments within 12 months from the Fieldwork close date of their Second Year Assessment. This means the time between second and third-year Assessments would be consistent for all Users, ensuring the process is fair and equitable. For example, if a User's second-year Fieldwork closed on 12 March 2019, the new Assessment period can be scheduled no later than 11 March 2020. The User CIO informed SSC members that this was an advanced Operating Model to avoid two potentially confusing processes for scheduling User Assessments. Instead, SECAS would proactively look to approach and engage with Suppliers in advance of Assessment dates needing to be scheduled.

Large Supplier Representative noted it would be feasible to adjust the SCF in the short term however, proposed that a SEC Modification should be considered in order to adjust wording of User Assessments in the SEC long term.

The SSC **NOTED** the amendments proposed to be made to the SCF which added '*In Line with G8.40, the SSC expects the third-year assessment to be booked and completed within 12 months of the second-year fieldwork being completed. The cycle will then continue on a 12month rolling basis from this point forwards.'* It was confirmed 'booked and completed within 12 months' should be amended to 'scheduled within 12 months' and no reference made to 'being completed'. All subsequent assessments will then begin a year from when the second-year Fieldwork period ended.

The SSC **NOTED** the Suppliers who could be impacted based on when this operating model would come into effect based on their Fieldwork end dates from 2018.

The SSC;

- **NOTED** the update;
- **CONSIDERED** the amendments to the timing of third and subsequent security assessments;
- **AGREED** a grace/transition period for the implementation of these amendments to apply all assessments scheduled from 1 August 2019 (allowing a three-month transition period from end April); and
- **AGREED** the amendments to the Security Controls Framework Part 1, Section 4.5 (with a separate explanation of the agreed transition period to be provided).

11. SECMP0013 Meter Triage (GREEN)

The SSC were provided with an update in relation to the Business Requirements previously discussed for SECMP0013 'Smart meter device diagnostics and triage'. The TABASC Chair confirmed that a use case has been developed which has been sent to the National Cyber Security

Centre (NCSC) for review. This will in turn be forwarded to the Technical Specification Issue Resolution Sub-Group (TSIRS) to confirm the viability from a technical point of view before coming back to the SSC.

The SSC **NOTED** the update.

12. Network & Information Systems Directive (NISD) (RED)

Gemserv Representatives provided an overview of the NISD and the degree of alignment between the SEC security obligations and the Cyber Assessment Framework (CAF), specifically focusing on the approach, findings and recommendations for the SSC. The five considerations detailed within the comparative analysis were in addition to the methodology of the Cyber Assessment Framework (CAF) and how this compared to the guidance in the SCF.

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

The SSC **NOTED** the update.

13. SOC2 Final Report (RED)

The DCC confirmed the SOC2 Final Report had now been received and was currently being reviewed in order to specifically map and break down the findings and management responses before bringing to the SSC on 24 April 2019.

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

14. SMETS1 Update (RED)

The SSC were provided with an update in relation to the SMETS1 Security Architecture V1.4 and XML Certificate Recovery. It was confirmed that the SSC comments on the SMETS1 Security Architecture V1.4 had been provided to the DCC.

The SSC also **NOTED** the update regarding SMKI XML Certificate Recovery whereby the SSC previously requested that the DCC explain the applicability of SEC Appendix L SMKI Recovery Procedures to SMETS1. It was confirmed this update would also be presented to the SMKI PMA on 16 April 2019.

Post meeting note: The DCC have now shared an AMBER version of the SMETS1 Security Architecture v1.4 document for SEC Parties. It can be found on the SEC website here.

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

15. DCC Post Commissioning Report (RED)

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

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

16. CPA Matters

Security Characteristics Timing of Implementation

The SSC **NOTED** the update in relation to the Security Characteristics document V1.3 which is being finalised by NCSC following comments from industry. The SSC consulted with the relevant trade bodies on an implementation date for V1.3 of the Security Characteristics and is awaiting a response.

CPA Conditions relating to a Communication Hub

The SSC **NOTED** the update in relation to a Communications Hub with CPA Conditional Certification. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

ESME Optical Report

The SSC **NOTED** the update in relation to the ESME Optical Report. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

CPA Qualification

The SSC **NOTED** the update regarding the extension of a Device Manufacturer’s CPA Certification. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

17. Rogue Devices being Joined/Un-Joined (AMBER)

Due to time constraints, this agenda item was deferred to the next SSC meeting scheduled for Wednesday 24 April 2019.

18. Standing Agenda Items (RED)

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

- Reporting on 'Conditional' CPA certificates **(RED)**;
- Anomaly Detection Update **(RED)**;
  - A DCC request was presented by the SSC Chair (GH) who stated the DCC have requested changes to the existing ADT thresholds.
    This agenda item was marked as '**RED'** and therefore recorded in the Confidential Minutes. The SSC **APPROVED** the DCC request.
- Shared Resource Notifications
  - SECAS provided the SSC with an update which noted, in line with SEC Section G 5.26, Small Supplier 'N' notified SECAS that they are changing their Shared Resource Provider.
- Security Incident and Vulnerabilities (**RED**).

The SSC **NOTED** the updates.

19. Any Other Business (AOB) (RED)

No additional items of business were raised, and the Chair closed the meeting.

Next Meeting: 24 April 2019