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.

MP203 'Security Assurance of Device Triage Facilities'

September 2022 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Kev Duddy	SECAS
Joey Manners	SECAS
Bradley Baker	SECAS
Elizabeth Woods	SECAS
Ben Giblin	SECAS
Fiona Bond	SECAS
Rainer Lischetzki	SECAS
James Hosen	SECAS
David Walsh	DCC
Tom Rothery	DCC
Chris Thompson	DCC
Mark Pitchford	DCC
Julie Brown	British Gas
Emma Johnson	British Gas
Beth Davey	Calvin Capital
Martin Bell	EUA
Alastair Cobb	Landis+Gyr
Mark Powell	Macquarie
Ralph Baxter	Octopus Energy
Audrey Smith-Keary	OVO Energy
Mafs Rahman	Scottish Power
Michael Snowden	Secure Meters
Lorna Clarke	SMDA
Gordon Hextall	SSC Chair
Matt Alexander	SSE Networks
Shuba Khatun	SSE Networks
Robert Johnstone	Utilita
Karen Jacks	Vantage Meters
Luke Brady	Vantage Meters
Kelly Kinsman	WPD

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue identified, the Proposed Solution and the drafted legal text.

Issue

Use Case 004 (Factory Reset) has recently been approved, meaning Parties will be able to triage and refurbish Devices in line with relevant use cases. The SEC does not current reference security assurance of Triage Facilities, Triage Tools or Triage Interfaces. Initial consideration was given that Parties might be able to operate these under responsibilities as “Users”. However, upon review certain requirements were not covered under the existing clauses of Section G ‘Security’. Additionally, Meter Asset Providers (MAPs) are not required to be SEC Parties and therefore some may be unable to undertake Triage Activities on their Devices. The SSC has determined that in order for Triage Facilities to operate, they will be required to pass through an assurance process.

Proposed Solution

The Proposed Solution will require all Triage Facility Providers to be a SEC Party. They will need to comply with the existing clauses G1, G3 to G5, G7 and G8. Providers will be required to maintain an asset management system to record all Triage Activities, ensure adequate protection against misuse of the Triage Tool and Triage Interface and fit tamper-protection seals to Devices that complete the Triage Activities. They will need to pass through a Full User Security Assessment (FUSA) initially, and subsequent assessments will be proportionate to security risk and could be Verification User Security Assessment or User Security Self-Assessment which are less resource heavy and lower costs.

Working Group Discussion

SECAS (KD) provided an overview of the issue and solution. The Security Sub-Committee (SSC) Chair (GH) commented that the User CIO (Competent Independent Organisation) is undertaking to provide a Security Controls Framework document to complement the SSC Guidance for Device Security and Triage. This will explain with clarity what is required from triage Facility Providers against each of the existing clauses that apply.

SECAS (KD) noted a question for Parties within the legal text as to where restriction should be placed with regards carrying out Triage Activities. As written, if an outer tamper boundary was breached then that Device should not be triaged. However, it had been noted on occasion that Suppliers might have to breach the outer tamper boundary for legitimate reason and this should not preclude a Device from being triaged.

A Working Group member (JB) noted that they can receive tamper Alerts on some occasions when the battery fails and therefore it was not likely the outer seals were the right place to restrict from.

A Working Group member (AC) questioned whether the tamper protection boundary would be legitimately broken during removal. They noted that if broken during installation the Supplier should be re-sealing them at that time. They noted that the question for the Working Group was not clear enough to be able to answer with confidence.

A Working Group member (MP) queried whether the internal seals were the Measuring Instruments Directive (MID) seals, rather than general security seals.

Another Working Group member (MS) summarised that Device Manufacturers could have fulfilled the requirements on tamper protection boundaries in different ways and therefore may not be uniform. They suggested using the definition from the Commercial Product Assurance (CPA) Security Characteristics with this legal text.

SECAS (KD) summarised the next steps. A Working Group member (BD) voiced support for this modification being implemented in November 2022.

Next Steps

The following actions were recorded from the meeting:

- SECAS to identify CPA SC text for tamper protection boundary to address the legal text; and
- SECAS to issue the Refinement Consultation.