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.

MP183 'Post Commissioning Obligations Reporting'

March 2022 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
David Kemp	SECAS
Elizabeth Woods	SECAS
Joey Manners	SECAS
Bradley Baker	SECAS
Joe Hehir	SECAS
Kev Duddy	SECAS
Mike Fenn	SECAS
Tim Newton	SECAS
Rainer Lischetzki	SECAS
Anik Abdullah	SECAS
Tom Mudryk	SECAS
David Walsh	DCC
Tim Dunning	DCC
Eleanor Taylor	BEIS
Emma Johnson	British Gas
Lynne Hargrave	Calvin Capital
Alex Hurcombe	EDF Energy
Daniel Davis	ESG Global
Julie Geary	EON
Terry Jefferson	EUA
Martin Bell	EUA
Carmen Strickland	Horizon
Peter Hoare	Kaifa Metering
Ralph Baxter	Octopus Energy
Gordon Hextall	Security Sub-Committee (SSC)
Elias Hanna	Smart ADSL
Audrey Smith-Keary	SSE - OVO
Emslie Law	SSE - OVO
Matthew Alexander	SSEN
Robert Johnstone	Utilita

Attendee	Organisation
Luke Brady	Vantage Meters
Karen Jacks	Vantage Meters
Gemma Slaney	WPD

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue identified, the draft business requirements and the Proposed Solution.

Issue

The Smart Energy Code (SEC) currently requires the Data Communications Company (DCC) to report on failures in the Post Commissioning process for Smart Metering Equipment Technical Specification (SMETS) 2+ Devices. The DCC is required to provide reporting to the Panel, the Security Sub-Committee (SSC), its Service Users and the Communications Service Provider (CSP).

Because the Post Commissioning Obligations require Suppliers to successfully execute several Service Request Variants (SRVs) related to updating the Security Credentials, one of the criteria for Devices to 'pass' Post Commissioning is that the right number of relevant SRVs have been sent and subsequent 'successful' Responses received.

Devices can therefore be identified as 'failing' Post Commissioning if there is a breakdown in the process pathway even though the correct Certificates have been placed on the Device and it is communicating successfully.

The DCC is required to raise an incident for every failing Communications Hub Function (CHF), which the CSP then has to investigate. DCC Users also waste time and resource investigating Devices which have actually completed Post Commissioning.

Ultimately the issue leads to inaccuracy of reporting and reputational damage to the industry.

Business Requirements

SECAS presented the following draft business requirements:

1) Devices which have not sent Responses indicating the successful execution of Commands associated with Service Requests issuing/updating Security Credentials will no longer be reported as having failed Post Commissioning.
2) The DCC will report on the Certificate status for all Commissioned Devices throughout their lifespan.

Proposed Solution

The Proposed Solution is to remove Appendix AC 'Inventory, Enrolment and Decommissioning Procedures' section 5.7(c), which states that the failure to successfully execute Service Requests issuing/updating Security Credentials results in a 'failure' of Post Commissioning. SECAS advised that once the legal text has been drafted there will likely be consequential amendments required to clauses in Appendix AC which reference section 5.7(c).

The DCC will still report on the successful execution of Certificate-related SRVs, but this will no longer be a criterion for pass/fail of Post Commissioning.

As part of the solution, the DCC will update its current reporting suite to show the 'in-life' Certificate health of all Commissioned Devices. The updated reports will include the status of all 11 Certificate slots, as well as counts of relevant SRVs sent and subsequent Responses received.

Working Group Discussion

A Working Group member (JG) queried how the DCC would know if Device-specific Certificates were correct. The member noted that the current reporting doesn't distinguish between SRV 6.15.2 'Update Security Credentials (Device)' messages for 'keyAgreement' and 'digitalSignature'. SECAS and the DCC (TD) agreed to investigate the inclusion of this detail in the reporting criteria, with the member's input, before this modification returned to the Working Group.

Another member (GS) asked if Suppliers would have a view of SRVs that are sent to their Devices by different Parties. The DCC (TD) advised that during solution development the reporting methodology can be amended based on Party preference. SECAS (MF) agreed this functionality will be investigated and can be included if Parties decide it would be beneficial. SECAS agreed to bring this question back to the Working Group prior to Refinement Consultation.

The Working Group agreed that the Proposed Solution doesn't undermine the Post Commissioning Obligations, and that the Proposed Solution would meet the business requirements once the discussed amendments had been considered for inclusion.

Next Steps

The following actions were recorded from the meeting:

- SECAS and the Proposer to further develop the solution and the legal text, with input from JG, before presenting this back to a subsequent Working Group meeting.