

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP239 ‘Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue’

February 2024 Working Group – meeting summary

Attendees

Attendee	Organisation
Rachel Black (RBI)	SECAS
Kev Duddy (KD)	SECAS
Ali Beard (AB)	SECAS
Elizabeth Woods (EW)	SECAS
Simon Grimwood (SG)	SECAS
Mo Sumro (MS)	SECAS
Rainer Lischetzki (RL)	SECAS
Tim Newton (TN)	SECAS
Bradley Baker (BB)	DCC
Chun Chen (CC)	DCC
Robin Seaby (RS)	DCC
David Walsh (DW)	DCC
Gary Stuart (GS)	DCC
Nick Rogers (NR)	DCC
Jamie Flaherty (JF)	Ofgem
Patricia Massey (PM)	BEAMA
Julie Brown (JB)	British Gas
Emma Johnson (EJ)	British Gas
Rochelle Harrison (RH)	British Gas
Beth Tatton (BT)	Calvin Capital
Sharon Armitage (SA)	E.ON
Ian Turner (IT)	E.ON
Graham Wiles (GW)	E.ON
Alex Hurcombe (AH)	EDF
Daniel Davies (DD)	ESG Global
Kelly Kinsman (KK)	National Grid Electricity Distribution
Ralph Baxter (RB)	Octopus Energy
Emslie Law (EL)	OVO
Eric Fowler (EF)	Power Data Consultants

Attendee	Organisation
Mahfuzar Rahman (MR)	Scottish Power
Jeff Studholme (JS)	Smart Meter Assets
Shuba Khatun (SK)	SSEN
Kevin Clark (KC)	Utilita

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue, impact, business requirements, DCC Preliminary Assessment and feedback gained to date.

Issue

- Suppliers and Wide Area Network (WAN) Providers are expected to update the Device certificate within seven days following installation, via Service Request (SR).
- Sometimes the success response is not processed or not received by the Data Service Provider (DSP), resulting in a certificate misalignment between the Device and the DSP.
- Parties are unable to communicate with any Device that has a certificate that is misaligned with the DSP Master Key Store.
- Manual correction has high associated costs and is prone to errors.

Proposed Solution

- Amend the Certificate Confirmation Scheme (CCS) cycle (a scheme to iterate over different Access Control Broker (ACB) certificate when the MAC verification using first ACB certificate did not work) to consider iterating through all possible ACB KA Key and KA Device Certificate as well.
- This will help in identifying the correct Device Certificate – the root cause of this modification.
- Allow triggering the CCS in response to:
 - timeout of SRV 6.15.2;
 - Install and Commission process; or
 - via the SSI/SSMI.
- This will help to identify and record the correct Device Certificate in early stage of Install & Commissioning (I&C) process, post-I&C Certificate Update process and via SSI/SSMI during in-life operation.
- Amend SSI/SSMI to allow an authorised user to initiate CCS using:
 - SSI – for a single Device; and
 - SSMI – for a set of Devices.
- This requires additional role on SSI/SSMI and additional Device Certificate update capability on SSMI.

- Amend SSML to allow an authorised user to set the current certificate(s) for a Device.
- Add information to Service Audit Trail (SAT) logs for CCS timeout to indicate which cycle and the stage of the current cycle.
- Provide required information to DCC's DS&A team to allow to produce required reports on Device and certificate misalignment.
 - DS&A Team will ensure required data is shared with the DCC to generate desired reports.
 - The impact on the analytics system will be assessed as part of the Impact Assessment.
- Security Impacts:
 - This modification requires an amendment to check certificates and update where necessary, this will have a minimal security impact. New roles created will require security oversight, validation and any required documentation changes.
 - The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.
 - A more detailed security impact will be carried out as part of the DCC Full Impact Assessment.

DCC Preliminary Assessment Summary

- Cost - £161,000 - £360,000
- Full Impact Assessment cost – £20,684
- DSP and DCC Data Science and Analytics (DS&A) team impacted

Working Group Discussion

SECAS (EW) provided an overview of the issue, impact, business requirements, DCC Preliminary Assessment and feedback gained to date.

Scale of the issue

A Large Supplier member (KC) queried the number of Devices impacted. The DCC (CC) noted the initial report from March 2023 stated 120,000 Devices have certificate misalignment. They added that this number went down to 44,000 Devices in September 2023 due to manual corrections and further reporting refinements. The DCC (CC) stated the latest reported number is 42,000 Devices. The DCC (DW) added the cost associated with manual corrections for the DCC and SEC Parties is very significant. They also added that they are aware of a large number of correction requests pending submission from Suppliers.

A Large Supplier member (JB) stated that although the updated reporting has shown the number of impacted Devices to be currently less than previous, the number is likely to steadily increase as the rollout continues. They added that it is difficult to determine accurate figures due to ongoing resolutions. Two Large Supplier members (SA & JB) acknowledged that this is an enduring issue

which needs to be resolved. They also queried if there would be any reporting of certificate misalignment. The DCC (CC) stated there would be reporting as stated in Business Requirement 5. The Proposer (IT) emphasized that the current process to manually correct the misalignment via the ticketing system is very expensive, difficult and problematic. A Large Supplier member (JB) added that the solution would resolve misalignment immediately and noted that frontline staff are possibly replacing meters without realising the issue. A Working Group member (JS) stated they are supportive from a MAP perspective and anything that can reduce unnecessary Device removal is desired.

Root cause of the issue

The Proposer (IT) pointed out that for installing Suppliers, using SRV6.24.2 is the usual resolution route. However, they noted that this is not possible where Devices are inherited after a Change of Supply (CoS) and they have misaligned certificates. They added that there are a couple of Device Manufacturers who incorrectly apply the Message Authentication Code (MAC) validation check for CS02e. SECAS (RL) asked if it was possible to obtain the number of Devices which does a MAC check incorrectly. The DCC (CC) noted that it would be the current 42,000 figure, however noted that there is a possibility to tell by what Firmware Version the Device accepts. They added that a large portion of the issue is occurring at CoS gain, where the Device is doing the MAC validation correctly. SECAS (RL) noted that the flow chart will need to capture when it's not working from a CoS gain perspective as well, as this would have slightly different prerequisites and will ensure this scenario is resolved as part of the solution. The DCC (CC) noted they could add an additional flow chart to capture this scenario.

The DCC (CC) advised the whole scope of the modification is for situations where SRV6.24.2 isn't working. The Proposer (IT) added that even if you are the installer for those Devices, you cannot get them to realign without manual intervention. A Large Supplier member (JB) stated that this presents to Suppliers when they send SR6.23 and there is no response, and noted the gaining Supplier cannot see the history of the Device from the losing Supplier. A Large Supplier member (EL) added that it is impossible for gaining Supplier perspective to know what has historically happened to the Device.

SECAS (RL) noted that the root causes needed to be documented in the modification report. Working Group Chair (KD) confirmed this can be added to the modification report, but asked the DCC if the Proposed Solution would fix both the issues discussed today. The DCC (CC) confirmed it would and noted the scenarios are stated in Business Requirement 2.

Next Steps

The following actions were recorded from the meeting:

- DCC to provide additional process flow chart.
- SECAS to draft legal text and update modification report.
- SECAS to issue Refinement Consultation.