

SEC Modification Problem Statement

**Notify DCC which Access Control Broker
Certificate is on a Device Before Install and
Commission**

Version:

0.61

Date

5th December, 2022

Author

Classification:

DCC Public

About this document

This document is a problem statement. It sets out the background, issue or problem identified, the impacts this is having, and the context of this issue within the Smart Energy Code (SEC).

Contact

This proposal has been raised by Chun Chen from DCC.

If you have any questions on this modification, please contact: Chun Chen from DCC
(chun.chen@smartdcc.co.uk)

Summary

A small number of production meters and Communication Hubs (Comms Hubs) are failing the Install and Commission (I&C) process on-site. The root cause analysis of the failures indicates that the following conditions contribute to the problem:

- The DSP does not know which Access Control Broker (ACB) certificate was put on the Device during manufacture
- The DSP process to establish the correct ACB certificates on the device is only completed after the Installing Supplier submits their first Service Request (SR) to the Comms Hub
- The Device failed Message Authentication Code (MAC) validation and rejected the SR from the Installing Supplier because the DSP used the wrong ACB certificate to authenticate the command

A solution is required to notify DCC which ACB certificate is installed in the Device before the I&C process begins.

What is the Issue?

Installing energy suppliers have noted there are a number of Comms Hubs that fail the first SR8.11 which adds a meter, leading to Install and Commission process failure on-site. The cause of this failure is that the DSP using the wrong ACB certificate to MAC the first service request because DSP does not know which ACB certificate is in the Device.

During the I&C process, the DSP will query which certificates are present in all trust anchor slots on devices using SR206.24.1. This is known as the certificate confirmation process. This process needs to complete before the first SR message is sent to the devices. Otherwise, the I&C process is likely to fail.

For the Comms Hub, the certificate confirmation needs to complete soon after powering up, ideally within three minutes. For ESME, GSME and HCALCS, the certificate confirmation needs to complete soon after 8F12 alert, preferred within 3 minutes.

The duration required to complete the certificate confirmation process is dependent on how many valid ACB certificates could be installed within a Device. Each valid certificate will take up to three minutes to confirm whether it is the correct one installed in the Device or not.

- Currently there is only one manufacturing ACB certificate available in production, so the issue is rare and can only happen to a refurbished CH.
- A 2nd manufacturing ACB certificate will be introduced at end of 2022 to allow Device manufacturers to start manufacture with new ACB certificates at least 24 months before the current ACB certificates expire. In the worst-case scenario, 50% of the I&C process may fail.
- Moving forward, it is proposed to introduce new ACB certificate more often (e.g., a new certificate each year), the I&C failure rate will increase in line with number of valid ACB certificates in production. The more certificates introduced, the higher possibility of the I&C failure. For example, if there are four valid ACB certificates that could be installed on the Device, the possible I&C failure rate could be as high as 75%)

What is the Current Design for the Certificate Confirmation Process?

DSP carries out the certificate confirmation process via SR206.24.1 to ensure it uses the correct ACB certificate to MAC the command. For the Comms Hubs Communications Hub Function (CHF) and Gas Proxy Function (GPF), this is carried out following the birthing¹ of the Comms Hub. For other devices (ESME, GSME, PPMID, or HCALCS), the DSP will do this after SR8.11(add) and the second 8F12 alert is sent.

The process follows these steps:

- The DSP will use default manufacturing certificates to MAC SR206.24.1, as listed in the most appropriate mapping table published by the DCC to industry. Currently DCC only publish one version of the mapping table to start this process.
- If the default manufacturing certificate fails, then the DSP will work its way through the list of all the manufacturing certificates previously published by DCC in a specified order, as defined at the point of the pre-notification SR12.2. The order is based on the timing of the publication of the mapping table.
- If all the manufacture certificates fail, then the DSP will work its way through the list of all valid ACB certificates.

The timeout of SR206.24.1 is 180 seconds with three short retries 40 seconds apart. As a result, the certificate confirmation process will take more than three (3) minutes to complete if the ACB certificate on the Device is not the first attempted certificate.

DCC is investigating a separate design change to reduce the delay caused by the certificate confirmation process. However this will not resolve the root cause of the DSP not being able to identify which ACB certificate is on the devices. The separate DCC design change will help reduce the failure rate but will not be able to resolve the issue completely, thus an enduring solution is required to fix the root cause.

What is the Impact?

A delayed certificate confirmation process will result in a higher I&C failure rate on site, or where a retry is required an extended I&C process.

A consumer may not have a smooth experience if multiple site visits, or a longer on-site installation, results due to a higher failure rate of first attempt.

Currently only about 100 refurbished CSP North Comms Hubs are impacted by this problem. However as new device certificates are released by manufacturers at the end of a year, or with a new device, the potential retry time will increase by three minutes for each certificate retry.

New device certificates are required for 2023 but the rollout of the new Devices and certificates may take some time. A target date for implementing this Modification would be June 2024.

¹ the successful join of the device to the Wide Area Network

Potential Solutions

The root cause of this issue is that the certificate on the Device is not known before I&C, and the proposed enduring solution is to require the Device manufacturer (via Supplier or MAP) to notify DCC/DSP on what certificates were put into Device. This notification could be:

- Process based; for example, a file is loaded via the Self Service Interface (SSI)
- SR12.2 based; a new attribute is introduced in a newer version of DUIS to allow a DCC User to pre-notify a new Device and inform DCC which certificates (or the version of the mapping table) was put on a Device
- Device Alert based; as soon as Device is able, generate an Alert which contains the certificate information and send it to ACB. This will require GBCS change

The solution will be developed as part of the Modification development process.