

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.



DP232 'ACB certs on I&C'

Modification Report

Version 0.3

11 April 2023

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary.....	3
2. Issue.....	3
3. Assessment of the proposal	5
Appendix 1: Progression timetable	5
Appendix 2: Glossary	6

Contact

If you have any questions on this modification, please contact:

Mohammedanwar Sumro

020 3934 4506

mohammedanwar.sumro@gemserv.com

1. Summary

This proposal has been raised by Chun Chen from the Data Communications Company (DCC).

The DCC is introducing new manufacturing Access Control Broker (ACB) Certificates which may impact the Install & Commission (I&C) process. A small number of production meters and Communication Hubs are failing the I&C process on-site. This is due to the length of time the Data Service Provider (DSP) takes to Message Authenticate Code (MAC) if the ACB Certificate is not the one on the Device. The DSP therefore must try all known ACB Certificates to progress, which leads to an increased risk of the system timing out and preventing successful I&C. Having the correct ACB Certificate initially will reduce the amount of time an engineer is at a premise and reduce the risk of the I&C process timing out and the Devices not being commissioned.

2. Issue

What are the current arrangements?

What is an ACB Certificate?

An ACB Certificate is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimises risk to a business organisation. An ACB Certificate is placed on the Device by the Manufacturer but is known to the Supplier. The Method used to put the ACB Certificate onto a Device is by the device manufacturer. The DCC will check the ACB Certificate on the Device via Service Request 6.24.1.

All certificates originate from the DCC for all Devices. This is via a manufacturing pack. The DCC makes available all the codes required in these packs. To date, there has only been one ACB Certificate that has been in circulation.

Authenticating the device

The ACB Certificate allows access to a Device for the DSP. The DSP will use default manufacturing certificates to Message Authentication Code (MAC) by retrieving Device security credentials. When new ACB Certificates are released and the default manufacturing certificate fails, the DSP will work its way through the list of all manufacturing certificates previously published by the DCC in a specified order. If all the manufacture certificates fail, then the DSP will work its way through the list of all valid ACB Certificates. The current process has no mechanism for the DCC to find out and record which certificates are installed on the Device by the Manufacturer.

What is the issue?

Introduction to new ACB Certificates

The current manufacturing ACB Certificate will expire in 2026, and a new manufacturer pack containing a new ACB Certificate will be introduced by the DCC in 2023. However, as an increased security measure there has been a proposal to introduce new ACB Certificates every four years moving forward. New Device certificates are expected for the end of 2023, but the rollout of the new Devices and certificates will enter the into the Supply Chain June 2024.

Introducing new ACB Certificates will increase the DSP's certificate reading time, potentially leading to an increase in the number of retries required during I&C. The DCC has noted there are several refurbished Communication Hubs that fail the first Service Request which adds a meter; this leads to I&C process failure on-site. The issue is yet to present itself in new Devices. However, when the new ACB Certificates are in existence there is a possibility that the DSP may use the incorrect ACB Certificate to MAC the first Service Request because the DSP will not know which ACB Certificate is in the Device.

Issues for DSP

The timeout of the ACB Certificate Request (SR 6.24.1) is 180 seconds with three short retries of 40 seconds. The certificate confirmation process will take more than three minutes to complete if the ACB Certificate on the Device is not the first attempted certificate, leading to a timeout. This results in a higher I&C failure rate on site, or where a retry is attempted this leads to an extended I&C process.

At the time of receiving the problem statement an estimated 100 refurbished Communications Hubs have already been impacted by this problem. Each new ACB Certificate would also increase the potential retry time by three minutes for each certificate retry.

Design Enhancement

The DCC has confirmed a design enhancement is being delivered to minimise impact to I&C with the delivery date expected before June 2024. The aim of the DCC design enhancement is to have no service deterioration resulting from the new manufacturer pack, with a total of 6 attempts. It will achieve this by parallel certificate reading via DSP building a batch of certificate read commands using all possible ACB KA Certificates and send to the Device 10 seconds apart. However, the DCC believes that the residual risk following this enhancement is that approximately 1% of all installs will be affected by this issue and fail I&C.

What is the impact this is having?

The DCC System timing out and requiring User retry due to an incorrect ACB Certificate results in valuable time being lost for the engineer on site. Repeated failure can mean the Device is not able to be Commissioned and is therefore left in a decommissioned state.

With the introduction of new ACB Certificates comes a risk for 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%.

The DCCs design enhancement will minimise this risk of I&C failing. The DCC believes that the residual risk will be less than one in one hundred installs will fail I&C. However, the enhancements will not resolve the root cause of the DSP not being able to identify which ACB Certificate is on the Device.

Impact on consumers

Having I&C fail on site will impact consumers negatively. Should I&C fail on site consumers are left having a engineer at the premises for an extended period of time whilst attempting multiple retries. There is also the increased risk that Devices are not able to be commissioned at all.

3. Assessment of the proposal

Areas for assessment

How can DCC obtain ACB Certificates before I&C?

The enduring solution is to require the Device Manufacturer to notify the DCC on what certificates were put into the Device before pre-notification. This notification can be process based; for example, a file loaded via the Self-Service Interface (SSI). Another option for DCC to obtain ACB Certificates before I&C would be through the introduction of a new attribute to Service Request 12.2 which would be implemented in a new version of DUIS to allow a DCC user to pre-notify a Device and inform DCC which certificates were put on a device.

For Communications Hubs, the DCC will include certificate information as part of Network Evolution Programme (NEP) Communication Hub & Network (CH&N) requirement. The full solution options will be assessed as part of the refinement process for this modification.

Sub-Committee input

The Smart Energy Code Administrator and Secretariat (SECAS) has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC) and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	To determine the severity of how the I&C affected.
SMKI PMA	No input required
SSC	No input required
TABASC	To confirm solutions are implemented as expected – Input required for solution development

Observations on the issue

Views of the Change Sub-Committee

A Change Sub-Committee (CSC) member noted that if the new Certificates are entering the Supply Chain from 2023 then an earlier implementation time would be desirable. SECAS agreed to prioritise this modification's progression to target the earliest release date possible. If system changes are required, then it is likely this will not be delivered until November 2024.

Views of the TABASC

The TABASC has recommended that SECAS coordinates with the DCC on new manufacturing packs with the OPSG. They have also requested clarification from the DCC on how the DSP can query a device and determine if certificates have been installed. In addition, TABASC has requested confirmation from the DCC on the scenarios in which the DSP can reject the processing of an ACB certificate. These suggestions aim to ensure effective management, operation, and deployment of new devices in compliance with standard industry practices.

Appendix 1: Progression timetable

SECAS will present the Proposal to the CSC for final comment and decision, with the recommendation that it proceeds to the Refinement Process. SECAS will then work with the Proposer to develop the Proposed Solution before presenting to the Working Group.

Timetable	
Event/Action	Date
Draft Proposal raised	14 Feb 2023
Presented to CSC for initial comment	21 Feb 2023
Modification discussed with TABASC	02 Mar 2023
Business requirements developed with Proposer and DCC	20 Mar 2023
<i>CSC converts Draft Proposal to Modification Proposal</i>	<i>18 Apr 2023</i>
<i>Modification discussed with Working Group</i>	<i>3 May 2023</i>
<i>Preliminary Assessment requested</i>	<i>8 May 2023</i>
<i>Preliminary Assessment returned</i>	<i>5 Jun 2023</i>
<i>Modification discussed with Working Group</i>	<i>5 Jul 2023</i>
<i>Modification discussed with TABASC</i>	<i>3 Jul 2023</i>
<i>Refinement Consultation</i>	<i>10 Jul 2023 – 24 Jul 2023</i>

Italics denote future events that may be subject to change.

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
ACB	Access Control Broker
CH&N	Communications Hub & Network
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
GBCS	Great Britain Companion Specification
I&C	Install and Commission
MAC	Message Authentication Code
MAP	Meter Asset Provider
NEP	Network Evolution Programme
OPSG	Operations Group
SECAS	Smart Energy Code Administrator and Secretariat
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SR	Service Request
SSC	Security Sub-Committee
SSI	Self Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee