

SEC Modification Proposal, SECMP0239, DCC CR5170

**Enduring Solution for Resolving SMETS2 Device
Certificate Misalignment Issue**

Preliminary Impact Assessment (PIA)

Version:	0.2
Date:	20th October 2023
Author:	DCC
Classification:	DCC PUBLIC

Contents

1	Executive Summary	3
2	Document History	4
2.1	Revision History	4
2.2	Associated Documents.....	4
2.3	Document Information	4
3	Context and Requirements.....	5
3.1	Current Arrangements	5
3.2	What is the Issue?	5
3.3	Impact of the Issue	6
3.4	Business Requirements.....	6
4	Description of Solution.....	9
4.1	Impacts on DSP	9
4.2	Impacts on DCC DS&A Reporting.....	9
5	Impact on DCC Systems, Processes and People	10
5.1	Security Impact.....	10
5.2	Integration Impact	10
5.3	Infrastructure Impact	10
5.4	Service Impact	10
6	Implementation Timescales and Approach.....	12
6.1	Implementation Approach	12
6.2	Testing and Acceptance	12
7	Costs and Charges.....	12
7.1	Design, Build and Testing Cost Impact.....	12
8	Risk, Assumptions, Issues, and Dependencies	13
8.1	Risks and Issues	13
8.2	Assumptions.....	13
8.3	Dependencies	13
	Appendix A: Glossary	14

1 Executive Summary

The Change Board are asked to approve the following:

- Cost to complete the Full Impact Assessment of **£20,684**.
- The timescales to complete the Full Impact Assessment of 40 working days.
- ROM costs for SECMP0239, up to the end of Pre-Integration Testing (PIT) of £161,000 to £360,000.

Only DSP component and DCC Data Science and Analytics (DS&A) team for Reporting are impacted by this Modification.

Problem Statement and Solution

As part of Post Commissioning Obligations, Suppliers and WAN Providers are expected to update the Device certificate. However, in some instances (estimated to be 120,000 Devices at the time the DCC generated a report (March 2023)), 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. This renders the Device incommunicable.

The Smart Energy Code (SEC) currently requires the Data Communications Company (DCC) to manually correct errors in the Smart Metering Inventory (SMI) where there is no other available method.

Suppliers have indicated they would like an enduring solution to resolve the certificate misalignment issue without involving a manual SMI update.

Modification Benefits

Resolving misalignment of Device Certificate with DSP Master keystore will have following benefits.

- Reduction in time-consuming process of manual correction for Energy Suppliers.
- Consumer will benefit from improved tariffs from the gaining Supplier following the Change of Supplier (CoS) event.
- Less issue in prepayment top-up operation if certificate misalignment issue is resolved.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
20/10/2023	0.1	Initial version, for DCC internal review
20/10/2023	0.2	Updated following DCC internal review

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP239 Modification Report v0.3	SECAS	30/08/2023
2.	MP239 Business Requirements v0.1	SECAS	14/09/2023

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Ian Turner from E.ON. An Initial Modification Report was prepared and published in May 2023.

The Preliminary Impact Assessment (PIA) was requested of DCC on 14th September 2023.

3 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by SECAS, the Proposer and the Working Group.

3.1 Current Arrangements

As part of SEC Post Commissioning Obligations, Suppliers are expected to update the Device certificate for Electricity Smart Metering Equipment (ESME), Gas Smart Metering Equipment (GSME), Gas Proxy Function (GPF) and WAN Providers are expected to update the Device certificate for Communications Hub Function (CHF). This must be carried out within seven days following installation via SRV 6.17 'Issue Security Credentials' and SRV 6.15.2 'Update Security Credentials (Device)'.

The DSP will only update the certificate upon receiving a successful response from the Device before a timeout occurs. This is 1,200 seconds (20 minutes) for ESME and 5,580 seconds (93 minutes) for GSME.

3.2 What is the Issue?

The DSP will transform all Service Requests to the appropriate Great Britain Companion Specification (GBCS) Use Case command, which contains a Message Authentication Code (MAC) generated using Access Control Broker (ACB) key and the Device Certificate. On receiving the GBCS Use Case command, the Device is expected to validate the MAC (with an exception for GBCS Use Case CS02d).

If the certificate is misaligned, MAC validation will fail and the Device will create a security Alert (for example, 8F3D or 8F1E). Due to this, the DCC User will not receive a Service Request response but will receive a timeout E21 error instead. The DCC User will only be able to send SRV 6.24.2 'Retrieve Device Security Credentials (Device)' to the Device.

It appears that for some of these Devices, the SRV 6.15.2 successfully executes on the Device, however the success response is not processed by the DSP for reasons including:

1. the response is never generated by the Device;
2. the response is lost in transit; or
3. the response reaches the DSP after timeout.

There are some Devices that become non-communicable after this process. Root cause analysis has identified that due to the reasons above, the Device certificate (Device Signature (DS) or Key Agreement Key (KAK)) is misaligned with what is held within the DSP Master Key Store.

The Proposer advises that Device certificate misalignment can also occur when attempting to address the issue of an incommunicable Device by cycling certificates, where the issue may persist due to intermittent Home Area Network (HAN) or WAN connectivity.

Suppliers have indicated they would like an enduring solution to resolve the Device certificate misalignment issue without involving a manual SMI update.

Some Devices utilising specific old firmware versions reject SRV 6.24.2 'Retrieve Device Security Credentials (Device)' and GBCS Use Case CS02e, as they take a prolonged period

to validate the MAC. It is not possible to perform a firmware update to fix the issue, as SR 11.3 'Activate Firmware' will fail (due to the Device being incommunicable).

3.3 Impact of the Issue

A DCC Data Science and Analytics (DSA) report was produced to identify the potential Devices that may suffer from this Device certificate misalignment issue. There is approximately a combined 120,000 ESME and GSME Devices identified to date which could increase.

Parties are unable to communicate with any Device that has a certificate that is misaligned with the DSP Master Key Store . Without an enduring solution there is a reliance on manual correction of each individual Device. The Proposer has advised that this is a time-consuming process, which has associated costs and can be prone to errors in relation to incorrect information provided to the DSP for manual correction. The process of producing the information require to complete manual corrections may lead to security risks.

Impact on consumers

Without an enduring solution in place, Suppliers must rely on manual corrections for each Device impacted, otherwise the Devices will not be able to receive Service Requests or the relevant responses or Alerts cannot be validated by the receiving SEC Party. An example of this is where Suppliers are unable to support a CoS, and the consumer will therefore not benefit from improved tariffs from the gaining Supplier.

Additionally, prepayment customers would be unable to perform top-up operations until the Device certificate misalignment issue is resolved.

Errors within the SMI

The SEC currently requires the DCC to manually correct errors in the SMI where there is no other available method. In the case of a Device certificate becoming misaligned between the Device and the DSP Master Key Store or Smart Metering Key Infrastructure (SMKI), it is not possible for the Supplier to fix the issue after a Change of Supplier (CoS) event. The only way to resolve the issue is with a manual DSP SMI correction.

The DCC has a process (script-based) to update the SMI based on the information energy Suppliers provide (for example, the Global Unique Identifier (GUID) of the Device, certificate serial number of the to-be-replaced certificate, and the certificate serial number of the new certificate). The Proposer has commented that it is a labour-intensive exercise to gather this information.

3.4 Business Requirements

The business requirements are as follows.

Ref.	Requirement
1	Device certificate misalignment issues are to be resolved to enable the Service User to send all Service Requests (SRs) to a Device and for the Device to respond accordingly.
2	The Proposed Solution must resolve the issue for three scenarios: Change of Supplier (CoS) when the gaining Supplier cannot rectify the issue through manual intervention.

Ref.	Requirement
	- When the previous Supplier has ceased to trade, and a Supplier of Last Resort (SoLR) has been nominated. - When the Device does not support the process of Service Reference Variant (SRV) 6.24.2 'Retrieve Device Security Credentials (Device)'
3	Addressing Device certificate misalignment issues should not require a manual Smart Metering Inventory (SMI) update except in exceptional circumstances.
4	Device certificate reporting is to be enduring as opposed to being produced on an ad-hoc basis and made available to Smart Energy Code (SEC) Parties.
5	Device certificate reporting must not duplicate information contained within current Post-Commissioning reporting.

Requirement 1: Device certificate misalignment issues are to be resolved to enable the Service User to send all Service Requests (SRs) to a Device and for the Device to respond accordingly.

The DCC Data Science and Analytics (DS&A) team has produced a report that states that approximately 120,000 Devices have misaligned certificates. The misalignment occurs between the Device and the Data Service Provider (DSP) Master Key Store. If the Device certificates are misaligned, the Device is rendered incommunicable. To address the issue and allow the Supplier to send all SRs to the Device, the certificate misalignment must be corrected. This is currently carried out manually, which is labour-intensive for the Supplier and DSP.

Requirement 2: The Proposed Solution must resolve the issue for three scenarios:

- **Change of Supplier (CoS) when the gaining Supplier cannot rectify the issue through manual intervention.**
- **When the previous Supplier has ceased to trade, and a Supplier of Last Resort (SoLR) has been nominated.**
- **When the Device does not support the process of Service Reference Variant (SRV) 6.24.2 'Retrieve Device Security Credentials (Device)'.**

The Proposer has highlighted the three most common scenarios that are impacted by Device certificate misalignment. In each scenario, the Supplier will only be able to send SRV 6.24.2 'Retrieve Device Security Credentials (Device)' to the Device, meaning that the consumer will not benefit from smart functionality. Although these are the three most common scenarios, the Proposer has indicated that there may be other instances where Device certificate misalignment occurs.

Requirement 3: Addressing Device certificate misalignment issues should not require a manual Smart Metering Inventory (SMI) update except in exceptional circumstances.

The Modification Report states that although the issue can be addressed by manual intervention by the DSP, the process is time consuming for both the Supplier and DSP, as well as there not being a consistent process for rectifying the errors. As such, it is the intention to have an automated solution, and only in exceptional circumstances will Suppliers and the DSP have to revert back to a manual update to the SMI.

The Proposer has requested that Devices that are currently impacted by the issue (approximately 44k Devices) are passed through the process in bulk to address the existing backlog.

Requirement 4: Device certificate reporting is to be enduring as opposed to being produced on an ad-hoc basis and made available to Smart Energy Code (SEC) Parties.

The Proposer has advised that they have received reports from the DCC to provide visibility on the issue which have been of use, and it would be beneficial if they are produced and made available to SEC Parties on a regular basis. The DCC will investigate the best way to make them available to SEC Parties.

Requirement 5: Device certificate reporting must not duplicate information contained within current Post-Commissioning reporting.

The Proposer has stated that there should be no duplicated data with the current contents of Post-Commissioning reports. It is advantageous to have a single source of data to not cause confusion amongst the recipients of the reports. The contents of the reports will be agreed following the completion of the Preliminary Assessment.

4 Description of Solution

The primary change to the DCC solution is on DSP component and DCC's DS&A team.

4.1 Impacts on DSP

Based on the business requirement in section 0, following changes are identified for the DSP.

- 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 require additional role on SSI/SSMI and additional Device Certificate update capability on SSMI.

- amend SSMI 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.

4.2 Impacts on DCC DS&A Reporting

For the Requirement 4 and 5, 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 FIA.

5 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0239 solution on DCC Services and Interfaces that impact Users and/or Parties.

5.1 Security Impact

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 Full Impact Assessment.

5.2 Integration Impact

An appropriate level of Systems Integration and User Integration Testing (SIT and UIT) will be carried out prior to progressing the release of this change to the Production environment, but this is not included in the PIA. A more detailed integration impact will be carried out as part of the Full Impact Assessment to evaluate CSPs and SMETS1 Service Providers need to carry out any integration testing or not.

5.3 Infrastructure Impact

No infrastructure impact is expected from this Modification. Additional processing and storage will be required. It should be noted that the aggregated impact of many such changes to the DSP solution will result in a reduction of the available processing headroom assumed as part of the original Agreement. As such, it may be necessary for DSP to raise a Business as Usual (BAU) CR for the provision/ of additional infrastructure to ensure the DCC Total System does not experience performance problems that are the direct result of the accumulation of such changes.

The change does not impact the DSP resilience or Disaster Recovery implementation.

5.4 Service Impact

The changes proposed as part of this Modification will have an ongoing service impact. The solution involves updates to SSI and SSML screens with new roles. Users will have the ability to run SRVs directly from these screens.

There is an assumption that SRV requests made by SSI/SSML could be restricted or queued if required to prevent the Production Environment from being overloaded.

A mechanism should be available to stop user requests in case of an emergency, and a detailed assessment of the implementation of this will be completed as part of the Full Impact Assessment.

Not all ACB and device certificate issues can be corrected by initiating the Certificate Confirmation Scheme. Occasionally devices do not correctly report the certificates in use.

Therefore, enquiries would be expected from users or the Service Desk in this scenario and triaging of incidents would be required to determine a way forward.

Additionally, to resolve the existing issue of Device Certificate misalignment on current Devices, Service Design team need to ensure steps are taken by the Operations Team to use enhanced SSMI screen to resolve the misalignment issue.

A detailed service impact will be completed as part of the Full Impact Assessment.

6 Implementation Timescales and Approach

This Modification is expected to be implemented in a future SEC Release. Design, Build, and PIT is expected to take approximately six months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Implementation Approach

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

6.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release and will include release based regression testing in SIT and UIT.

7 Costs and Charges

The scope of supply under this PIA includes design, development (build), system testing, and performance testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional and non-functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change. As a result, the final offer price may result in a variation.

7.1 Design, Build and Testing Cost Impact

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

£	Design, Build and PIT
SECMP0239	£161,000 to £360,000

Based on the existing requirements, the total fixed price cost for a Full Impact Assessment by the DSP is **£20,684** and would be expected to be completed in 40 working days.

8 Risk, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified.

8.1 Risks and Issues

None at this time.

8.2 Assumptions

Ref.	Assumption	Impact
MP2397-AS1	There is an assumption that SRV requests made by SSI/SSMI can be restricted or queued if required to prevent the Production Environment from being overloaded.	This should be discussed with the Business Proposer and Working Group.

8.3 Dependencies

None at this time.

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
BaU, BAU	Business As Usual
CAN	Contract Amendment Note
CHF	Communications Hub Function
CR	DCC Change Request
CSP	Communications Services Provider
DCC	Data Communications Company
DS&A	Data Science and Analytics
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
HAN	Home Area Network
GPF	Gas Proxy Function
GSME	Electricity Smart Metering Equipment
MAM	Meter Asset Manager
MOP	Meter Operator
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
RAID	Risks, Assumptions, Issues, and Dependencies
ROM	Rough Order of Magnitude (cost)
RSA	Registered Supplier Agent
S1SP	SMETS1 Service Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SMI	Smart Metering Inventory
SR	Service Request
SRV	Service Request Variant
SSI	Self Service Interface
UIT	User Integration Testing
WAN	Wide Area Network