SEC
Smart Energy Code

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'

Modification Report

Version 0.4

20 March 2024

Corporate member of Plain English Campaign
Committed to clearer communication
592

Gemserv

This document has a Classification of Clear

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. Solution 8
4. Impacts 8
5. Costs 11
6. Implementation approach 11
7. Assessment of the proposal 12
8. Case for change 15

Appendix 1: Progression timetable 16

Appendix 2: Glossary 17

This document also has four annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the full Data Communications Company (DCC) Preliminary Assessment response.
- **Annex C** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex D** contains the contains the full non-confidential responses received to the Refinement Consultation.

Contact

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

Elizabeth Woods

020 4566 8335

elizabeth.woods@gemserv.com

1. Summary

This proposal has been raised by Ian Turner from E.ON.

As part of Post Commissioning Obligations, Suppliers and Wide Area Network (WAN) Providers are expected to update the Device Certificate. This must be carried out within seven days following installation, via Service Request (SR) 6.17 'Issue Security Credentials' and Service Reference Variant (SRV) 6.15.2 'Update Security Credentials (Device)'. In some instances, 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.

It is estimated that approximately 140,000 Devices could be affected currently.

The Smart Energy Code (SEC) currently requires the DCC to manually correct errors in the Smart Meter Inventory (SMI) where there is no other available method. Suppliers have indicated they would like an enduring solution to resolve the Device certificate misalignment issue without involving a manual SMI update.

The Proposed Solution will allow Suppliers to identify the correct Device Certificates and update any misaligned Certificates on Devices via the Self-Service Interface (SSI) or Self-Service Management Interface (SSMI) instead of raising an Incident with the DCC for manual correction.

This modification will impact Suppliers and the DCC. If approved, this modification is targeted for the June 2026 SEC Release and will be progressed as a Self-Governance Modification.

The estimated cost of the DCC System changes up to the end of Pre-Integration Testing (PIT) is between £161,000 and £360,000.

2. Issue

What are the current arrangements?

What is a Device Certificate and what are they used for?

A Device Certificate is used to ensure that only the correct Party is communicating with the Device, and they are the authorised and valid Party. Some Service Requests (SRs) require a Certificate check to ensure the Party sending the SR are authorised to communicate with the Device before the command is processed.

Updating Device Certificates

As part of SEC Post Commissioning Obligations, Suppliers and WAN Providers are expected to update the Device certificate (Electricity Smart Metering Equipment (ESME), Gas Smart Metering Equipment (GSME) and Gas Proxy Function (GPF) for Suppliers, and Communications Hub Function (CHF) for Communication Service Providers (CSPs)). This must be carried out within seven days following installation via SR 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.

Device Processing of Service Requests

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 by the DSP Access Control Broker (ACB) using the 'old' Device key. On receiving the GBCS Use Case command, the Device is expected to validate the MAC (with an exception for GBCS Use Case CS02d) using the "new" Device key.

What is the issue?

Overview

Device Certificate misalignment will cause all Service Requests to fail on a Device, except for SRV 6.24.2 'Retrieve Device Security Credentials (Device)'. Therefore, the DCC User will be unable to communicate with that Device.

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.

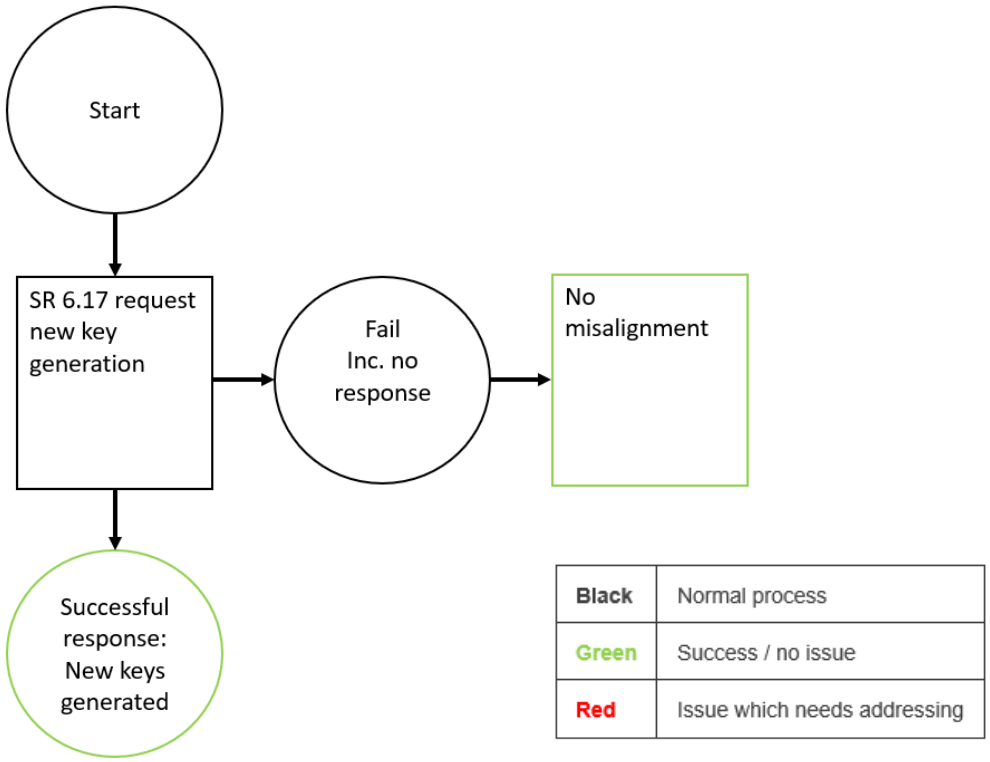
There are some Devices that become non-communicable after this process. Root cause analysis has identified that due to the reasons above, the Device Certificate (Device Signature (DS) or Key Agreement Key (KAK)) is misaligned with what is held within the DSP Master Key Store.

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.

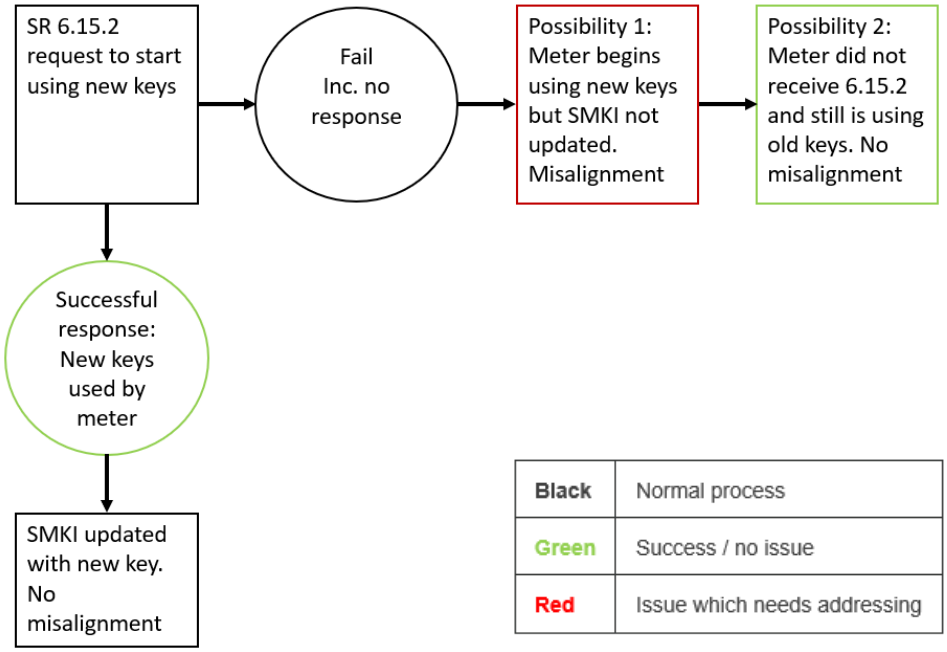
The below diagrams set out the current process and issues:

Starting point when Supplier request for new key:



Black	Normal process
Green	Success / no issue
Red	Issue which needs addressing

Issue when Supplier tries to use new keys:

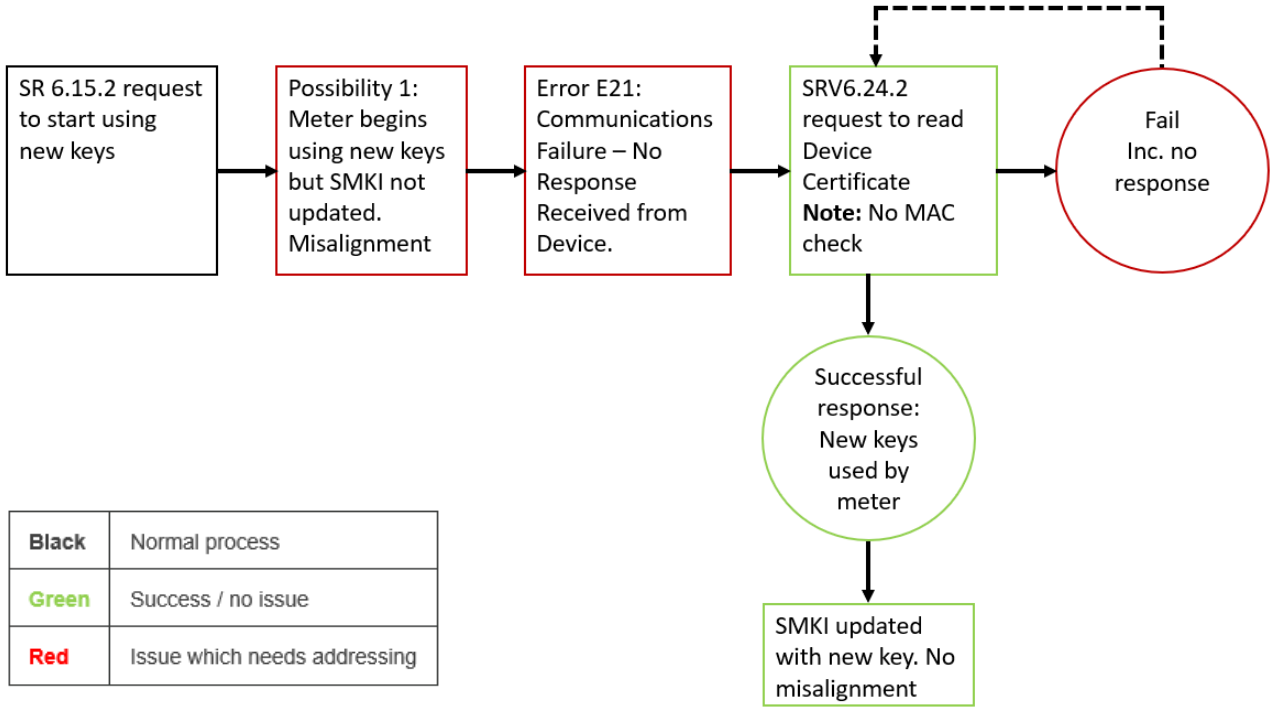


Black	Normal process
Green	Success / no issue
Red	Issue which needs addressing

Possible resolution via SRV6.24.2 and GBCS Use Case CS02e:

This below diagram sets out a scenario where a possible resolution works if the initial SR 6.17 has made it down to the Device and the Supplier can attempt to resolve the issue by using SRV 6.24.2 and GBCS Use Case CS02e.

This is the existing process which used by Energy Suppliers on those Devices supporting GBCS Use Case CS02e correctly and not had any Change of Supplier (CoS) since installation.



Black	Normal process
Green	Success / no issue
Red	Issue which needs addressing

There are two scenarios where the above, using SRV 6.24.2 and GBCS Use Case CS02e method cannot resolve the Device Certificate misalignment issue, where:

- a Device, where a Device Defect is present, in which these known Devices will perform a MAC check at while using GBCS Use Case CS02e; and
- a CoS has occurred, and the Device Certificates are misaligned prior to the CoS.

The only way to resolve the above scenarios is by manual SMI correction by raising an Incident in accordance with the Incident Management Policy.

Older firmware versions

Some Devices utilising specific old firmware versions reject SRV 6.24.2 'Retrieve Device Security Credentials (Device)' and GBCS Use Case CS02e. Although GBCS Use Case CS02e does not require any MAC validation, there are two Device Manufacturers' Devices which does validate the MAC and can take a prolonged period to do so. 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).

Scale of the issue

A DCC Data Science and Analytics (DS&A) report was produced to identify the potential Devices that suffer from this Device Certificate misalignment issue. There is approximately a combined 140,000 ESME and GSME Devices identified to date which will increase. The number of Devices with misaligned Certificates fluctuates at any given time, due to ongoing manual corrections by the DCC.

What is the impact this is having?

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.

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 CoS event. The only way to resolve the issue is with a manual DSP SMI correction.

The DCC has advised that it 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.

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.

3. Solution

Proposed Solution

The Proposed Solution will:

- Amend the Certificate Confirmation Scheme (CCS) cycle to work through all possible Access Control Broker (ACB) Key Agreement Key (KAK) and Key Agreement Device Certificates, which will help to identifying the correct Device Certificate; and
- Allow triggering the CCS in response to, the timeout of SRV 6.15.2, Install and Commission (I&C) process, or via the SSI/SSMI. Which will help to identify and record the correct Device Certificate in early stage of I&C process, post-I&C Certificate Update process and via SSI/SSMI during in-life operation; and
- Add information to Service Audit Trail (SAT) logs for CCS timeout to indicate which cycle and the stage of the current cycle; and
- Amend SSMI to allow an authorised User to set the current Certificate(s) for a Device; and
- Produce required reports on Device and Certificate misalignment.

The business requirements for the solution can be found in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
	Electricity Network Operators		Gas Network Operators
	Other SEC Parties	✓	DCC

The Proposed Solution aims to allow only authorised Users to amend Certificates on Devices which is linked back to SRV 6.15.2 'UpdateSecurityCredentials(Device)'. Only Suppliers can send SRV 6.15.2, and therefore will be impacted directly.

The DCC will have to make system and internal process changes, therefore would also be impacted.

DCC Systems

DCC System changes

DSP changes

- Amend the Certificate Confirmation Scheme (CCS) cycle to work through all possible Access Control Broker (ACB) Key Agreement Key (KAK) and Key Agreement Device Certificates, which will help to identifying the correct Device Certificate; and
- Allow triggering the CCS in response to:
    - the timeout of SRV 6.15.2;
    - Install and Commission (I&C) process; or
    - via the SSI/SSMI.

  Which will help to identify and record the correct Device Certificate in early stage of I&C process, post-I&C Certificate Update process and via SSI/SSMI during in-life operation; and
- 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 SSMI to allow an authorised User to set the current Certificate(s) for a Device; and
- Add information to Service Audit Trail (SAT) logs for CCS timeout to indicate which cycle and the stage of the current cycle; and
- Provide required information to DCC's DS&A team to allow to produce required reports on Device and Certificate misalignment.

The full impacts on DCC Systems and DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex B.

Technical Specifications

There will be changes in DUIS and corresponding changes in the DCC User Gateway Interface Design Specification (DUGIDS). The DUIS Guidance document may need to be updated.

DCC System traffic

Based on information in DCC's Preliminary Assessment response there will be no impact on DCC System traffic

DCC DS&A Reporting

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 DCC Impact Assessment.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix AC 'Inventory Enrolment and Decommissioning Procedures'
- Appendix AD 'DCC User Interface Specification'
- Appendix AH 'Self-Service Interface Access Control Specification

The changes to Appendices AC and AH required to deliver the Proposed Solution can be found in Annex C. Changes to Appendix AD will be provided as part of the DCC Impact Assessment.

Technical specification versions

This modification will impact Appendix AD 'DCC User Interface Specification' (DUIS). The proposed changes will be made clear after the Impact Assessment is returned by the DCC.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
	Communications Hubs	✓	Gas Proxy Functions
	In-Home Displays	✓	Prepayment Meter Interface Devices
✓	Standalone Auxiliary Proportional Controllers		Home Area Network Connected Auxiliary Load Control Switches
	Consumer Access Devices		Alternative Home Area Network Devices

This would affect all variations of ESME including Standalone Auxiliary Proportional Controllers (SAPCs), GSME and Gas Proxy Functions (GPFs), as it is set out in the DUIS that these Device Types are applicable for SRV 6.15.2.

Prepayment Meter Interface Devices (PPMIDs) are indirectly positively impacted. This is due to incorrect Device Certificates on ESME, GSME or GPF making the joining impossible on a PPMID. Those situations will be alleviated by this solution.

Consumers

Consumers are likely to indirectly benefit from this modification. With the Device Certificates aligned, their current Supplier would be able to connect to a consumer's Device. This would negate the need to replace the Device at a consumer's premises, therefore improve the overall consumer experience.

Other industry Codes

This modification will not impact any other industry Codes.

Greenhouse gas emissions

This modification will not impact greenhouse gas emissions.

5. Costs

DCC costs

The DCC's Service Providers have provided a rough order of magnitude (ROM) cost.

The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and PIT	£161,000 - £360,000
Systems Integration Testing (SIT)	TBC
User Integration Testing (UIT)	TBC
Implement to Live	TBC
Application Support	TBC

More information can be found in the DCC Preliminary Assessment response in Annex B.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

During the Refinement Consultation, all respondents supported the approval of this modification. All respondents expected not to incur any material costs and could implement within three months.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **25 June 2026** (June 2026 SEC Release) if a decision to approve is received on or before 25 June 2025; or

- **24 June 2027** (June 2027 SEC Release) if a decision to approve is received after 25 June 2025 but on or before 24 June 2026.

This modification will impact the DUIS which is only updated annually. It is not possible to target the June 2025 SEC Release, which is the next scheduled DUIS uplift, due to the 12 months' timescale required for implementation. There is a possibility to target the June 2025 SEC Release, if the DCC Impact Assessment details a reduced timescale.

7. Assessment of the proposal

Areas for assessment

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. The key points can be found below:

Sub-Committee input	
Sub-Committee	**Input sought**
OPSG	Does this issue have any operational impact on the smart metering infrastructure?
SMKI PMA	Does this issue impact the Smart Metering Key Infrastructure?
SSC	Does this issue or potential solution have any security impacts?
TABASC	Does this issue or potential solution have any technical or business architecture impacts?

During the Chair Triage meeting, the SSC / SMKI PMA Chair noted the potential link with DP232 'ACB Certs on I&C', however this modification has since been withdrawn. This is part of a wider concern that relates to several issues with Certificates. They stated that the DCC has been asked to provide a plan of how all the issues relate and will be resolved. SECAS will keep the OPSG, SMKI PMA and SSC updated as this modification progresses.

The DCC has undertaken the project looking to resolve Certificate-related issues, however it has stated that this modification is still necessary. The Proposer has confirmed that the issue identified under this modification relates specifically to Device Certificates.

Observations on the Issue

Are Devices physically removed?

SECAS presented the Draft Proposal to the Change Sub-Committee (CSC) for initial comments in April 2023. A CSC member asked if it can be investigated how many meters are physically removed prior to the resolution. They commented that they had seen many meters being physically removed shortly after installation due to a failed commission, and queried if this could be related to the issue being considered under this modification. SECAS raised this with the DCC who stated it is not aware

of any Devices that have been physically removed due to this issue. The DCC advised that the issue may result in Devices losing smart capability, but they should not be physically removed.

Scale of the issue

During the Development Stage the Proposer expressed concern with the lack of reporting on Device Certificates. They advised that they were faced with a large quantity of Certificate issues in differing forms. They added that a common area of concern is the CoS (Gain) scenario where visibility of Device Certificate misalignment is especially opaque. The Proposer added that identifying misalignments is only beneficial if they can also remediate the issue. They commented that they have many customers where the CoS (Gain) cannot progress beyond SR 6.23 'Update Security Credentials (CoS)' due to either DSP or Device Certificate misalignment. Raising an incident to request Device Certificate misalignment is pointless at present as Parties are asked to provide information that they do not have access to.

Number of Devices impacted

When returning to the CSC, a member commented that they believe there may be more Devices suffering from this issue than the 120,000 listed within the DCC's report. The member also commented that this has been a known issue for some time and would like to see this modification progressed as a priority.

During Working Group discussions, although it was noted from an initial DCC report from March 2023 that 120,000 Devices have certificate misalignment, the figure was reduced to 44,000 Devices in September 2023. This was likely due to manual corrections and further reporting refinements. The DCC stated the latest reported number is 42,000 Devices. The Working Group noted that the number is likely to steadily increase as the rollout continues and added that it is difficult to determine accurate figures due to ongoing resolutions. The DCC added the cost associated with manual corrections for the DCC and SEC Parties is very significant. Also, that the DCC are aware of a large number of correction requests pending submission from Suppliers as of February 2024. The Working Group acknowledged that this is an enduring issue which needs to be resolved. The Proposer emphasised that the current process to manually correct the misalignment via the ticketing system is very expensive, difficult and problematic.

Solution development

Root cause of the issue

During CSC discussions, members questioned whether this modification should focus on addressing the root of the issue (responses not reaching the DSP), instead of automating Device Certificate correction within the SMI. The CSC commented that if the costs are similar amongst both solutions, priority should be given to addressing the root of the issue. A CSC member commented that the industry is aware that a percentage of messages do not get received at various points across the smart infrastructure, which may be a difficult issue to solve (due to potential hardware defects).

Change of Supplier and Device Defects

The Proposer 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 CoS and they

already 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. The DCC added that a large portion of the issue is occurring at CoS (Gain), where the Device is doing the MAC validation correctly. SECAS requested from the DCC, an additional flow chart 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 advised the whole scope of the modification is for situations where SRV6.24.2 isn't working. The Proposer added that even if you are the installer for those Devices, you cannot get them to realign without manual intervention. A Working Group member 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 Working Group member added that it is impossible for gaining Supplier perspective to know what has historically happened to the Device.

The DCC confirmed that the Proposed Solution would fix both the issues discussed and the scenarios are stated in Business Requirement 2.

SSI/SSMI

Currently the DCC uses the Certificate Confirmation Scheme (CCS) cycle to check the different Access Control Broker (ACB) Certificates held at the DSP, when the MAC verification using first ACB Certificate does not work on the Device.

By amending the SSI/SSMI to allow the Supplier to initiate the CCS, they can identify and record of the correct Device Certificate at earlier stages of Install & Commissioning (I&C) process, post-I&C Certificate Update process and during in-life operation. This also allow the Supplier to set the correct Certificate for a Device.

Reporting

The Proposer stated that the DCC had provided some useful data that would be advantageous if turned into a regular report. The Proposer and the DCC have agreed to consider this when building the Proposed Solution and has now been included in the Business Requirements, and the subsequent DCC Preliminary Assessment.

DNO Device Certificate Misalignment

During the Refinement Consultation, a Network Party queried if the Proposed Solution would also resolve the misalignment of Distribution Network Operators (DNOs) Device Certificates in slot 6 and 7. SECAS and the DCC noted that MP239's focus is on the Device Certificate associated with credentials generated by the Devices, e.g. a Certificate belongs to a Device, not a Remote Party. Therefore, any Certificate in the Device Trust Anchor Cell belongs to Remote Party, not the Device itself. The scope of MP239 does not cover any Certificates held in the Trust Anchor Cells. The DCC advised that as slots 6 & 7 holds certificates for DNOs, it is possible for the DNO to resolve the misalignment by triggering SR6.24.1.

8. Case for change

Business case

Implementing this modification will resolve the misalignment of Device Certificate with DSP Master keystore. This will reduce a time-consuming and costly process of manual corrections for Energy Suppliers and the DCC, also have less issues with prepayment top-up operation by having the Certificate misalignment issue is resolved. By having functional and operating Devices at consumer premises', especially after a CoS event, would allow for consumers to benefit from improved tariffs from the gaining Supplier.

During the Refinement Consultation, all respondents were supportive of this modification. One Large Supplier respondent noted the implementation would result in a reduction of unnecessary site visits to exchange meters where CoS gains are unable to be completed.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that MP239 will facilitate SEC Objective (a)[1] as it will ensure that Devices at a consumer's premises is functioning as intended without replacing the existing Smart Meter.

Industry views

All Refinement Consultation respondents were supportive, and they believed it would better facilitate SEC Objective (a). With one Larger Supplier respondent also noting it better facilities SEC Objectives (c)[2] and (d)[3].

Views against the consumer areas

Improved safety and reliability

This modification will be neutral against safety and security for consumers.

Lower bills than would otherwise be the case

This modification will be neutral against this consumer benefit area. However, it would indirectly benefit consumers by ensuring the current Device on site is not replaced, and therefore not have additional cost to industry (as all Smart Metering is ultimately funded by consumers through their bill).

[1] Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

[2] Facilitate the Energy Consumers' management of their use of electricity and gas through the provision to them of appropriate information by means of Smart Metering Systems.

[3] Facilitate the effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy.

Reduced environmental damage

This modification will be neutral against this consumer benefit area. However, it would indirectly benefit consumers by ensuring the current Device on site is not replaced.

Improved quality of service

This modification will be neutral against this consumer benefit area. However, it would indirectly benefit consumers by ensuring existing Smart Meters already at their premises is functional without needed a replacement.

Benefits for society as a whole

This modification will be neutral against this consumer benefit area.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	3 Apr 2023
Presented to CSC for initial comment	18 Apr 2023
Draft Proposal discussed with Sub-Committee Chairs	19 Apr 2023
Presented to Sub-Committees for initial comment	Apr – May 2023
DCC Certificate issue project	May – Jul 2023
Business requirements developed	Aug 2023
CSC converts Draft Proposal to Modification Proposal	15 Aug 2023
Business requirements workshop	4 Sep 2023
Modification discussed with the Working Group	6 Sep 2023
DCC Preliminary Assessment requested	14 Sep 2023
DCC Preliminary Assessment returned	20 Oct 2023
Modification discussed with SMKI PMA	8 Nov 2023
Modification discussed with Working Group	7 Feb 2024
Refinement Consultation	21 Feb 2024 – 13 Mar 2024
Impact Assessment costs approved by Change Board	*27 Mar 2024*
Impact Assessment requested	*27 Mar 2024*
Impact Assessment returned	*28 May 2024*
Modification discussed with Working Group	*5 Jun 2024*
Modification discussed with SMKI PMA	*12 Jun 2024*
Modification Report approved by CSC	*18 Jun 2024*
Modification Report Consultation	*19 Jun 2024 – 9 Jul 2024*
Change Board Vote	*24 Jul 2024*

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
CCS	Certificate Confirmation Scheme
CHF	Communications Hub Function
CoS	Change of Supplier
CSC	Change Sub-Committee
CSP	Communication Service Provider
DCC	Data Communications Company
DNO	Distribution Network Operator
DS	Device Signature
DS&A	Data Science and Analytics
DSP	Data Service Provider
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
GBCS	GB Companion Specification
GSME	Gas Smart Metering Equipment
GPF	Gas Proxy Function
GUID	Global Unique Identifier
HAN	Home Area Network
I&C	Install & Commission
KAK	Key Agreement Key
MAC	Message Authentication Code
OPSG	Operations Group
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
SAPC	Standalone Auxiliary Proportional Controller
SAT	Service Audit Trail
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMI	Smart Metering Inventory
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority

Glossary	
Acronym	**Full term**
SR	Service Request
SRV	Service Reference Variant
SSC	Security Sub-Committee
SSI	Self-Service Interface
SSMI	Self-Service Management Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
UIT	User Integration Testing
WAN	Wide Area Network

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'

Annex A

Business requirements – version 0.1

About this document

This document contains the business requirements that support the solution(s) for this Modification Proposal. It sets out the requirements along with any assumptions and considerations. The Data Communications Company (DCC) will use this information to provide an assessment of the requirements that help shape the complete solution.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements		
Ref.	**Requirement**	**Responsible for delivery**
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.	DCC
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)'.	DCC
3	Addressing Device certificate misalignment issues should not require a manual Smart Metering Inventory (SMI) update except in exceptional circumstances.	DCC
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.	DCC
5	Device certificate reporting must not duplicate information contained within current Post-Commissioning reporting.	DCC

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

This solution will be applied to Smart Metering Equipment Technical Specifications (SMETS)1 and SMETS2 Devices.

2.2 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 44,000 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.

2.3 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.

2.4 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.

2.5 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.

2.6 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.

3. Solution development

This section contains a must-have, should-have, could-have, won't-have (MoSCoW) analysis for the different requirement components to be considered as part of the solution.

MoSCoW Analysis			
Requirement Ref.	**Description**	**Responsible for delivery**	**MoSCoW**
1	The Proposer and DCC have agreed that the Proposed solution must deliver this requirement.	DCC	M
2	The Proposer and DCC have agreed that the Proposed solution must deliver this requirement.	DCC	M
3	The Proposer and DCC have agreed that the Proposed solution must deliver this requirement.	DCC	M
4	The Proposer and DCC have agreed that this requirement is 'should-have' as further details regarding the reporting such as the contents will be investigated during the Preliminary Assessment.	DCC	S
5	The Proposer and DCC have agreed that this requirement is 'should-have' as further details regarding the reporting such as the contents will be investigated during the Preliminary Assessment.	DCC	S

Key

- M = Must have
- S = Should have
- C = Could have
- W = Won't have

4. Glossary

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

Glossary	
Acronym	**Full term**
CoS	Change of Supplier
DCC	Data Communications Company
DS&A	Data Science and analytics
DSP	Data Service Provider
SEC	Smart Energy Code
SMETS	Smart Metering Equipment Technical Specifications
SMI	Smart Metering Inventory
SoLR	Supplier of Last Resort
SR	Service Request
SRV	Service Reference Variant

Data Communications Company

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**

Data Communications Company

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 SR 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 SSMI 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/SSMI 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

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'

Annex C

Legal text – version 0.2

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

These changes have been redlined against Appendix AC version 7.0.

Amend Section 2 as follows:

2. Smart Metering Inventory

2.1 The DCC shall establish and maintain the Smart Metering Inventory.

2.2 The DCC shall ensure that the Smart Metering Inventory reflects the most up-to-date information provided (or made available) to it from time to time in accordance with this Code (subject to Section F2.9 (Publication and Use by the DCC)).

2.3 Parties shall not seek to add Devices to the Smart Metering Inventory (and the DCC shall not add Devices to the Smart Metering Inventory) otherwise than in compliance with this Appendix.

2.4 Prior to delivering a Communication Hub to a Party pursuant to the Communications Hub Service, the DCC shall add the Communications Hub Function and Gas Proxy Function that comprise that Communications Hub to the Smart Metering Inventory (to be identified with an SMI Status of 'pending'); provided that such Devices may only be added to the Smart Metering Inventory where the Communications Hub is of a Device Model identified in the Central Products List.

2.5 No Party shall add Communications Hub Functions to the Smart Metering Inventory without also adding the Gas Proxy Function that forms part of the same Communications Hub (and vice versa).

2.6 Any User may send a Service Request requesting that the DCC adds a Device to the Smart Metering Inventory (to be identified with an SMI Status of 'pending'); provided that only Devices of (or forming part of) a Device Model that is identified in the Central Products List are eligible to be added to the Smart Metering Inventory. This Clause 2.6 does not apply to Type 2 Devices (which are covered in Clause 2.9).

2.7 The DCC shall not send any communication to a Device unless the Device is listed in the Smart Metering Inventory; save for communications sent for the purposes of testing under Section H14 (Testing Services).

2.8 In the case of Communications Hub Functions and Gas Proxy Functions, the only Communications Hubs that may be added to the Smart Metering Inventory (subject to Clause 12.3) are those that comprise either a SMETS1 CH or a Communications Hub that is to be provided by the DCC pursuant to the Communications Hub Service.

2.9 Any User may send a Service Request requesting that the DCC adds a Type 2 Device to the Smart Metering Inventory. For the avoidance of doubt, a Type 2 Device shall not be identified in the Central Products List, and shall have no SMI Status.

2.10 The Responsible Supplier for each Smart Metering System shall keep under review the information recorded in the Smart Metering Inventory in respect of the Devices that comprise that Smart Metering System. Where circumstances change or the Responsible Supplier identifies an error in such information, the Responsible Supplier shall;

(a) submit Service Requests requesting that the DCC updates the Smart Metering Inventory ~~(or,~~;

(b) ~~-~~where it is not possible to correct the error via (a)~~do so~~, ~~shall~~use the Self-Service Interface to correct the error; or

(c) Where neither (a) nor (b) have been successful in correcting the error, raise an Incident in accordance with the Incident Management Policy~~)~~.

Where a correction is made in respect of the relationship between one or more Smart Meters / Standalone Auxiliary Proportional Controllers and an MPAN and/or MPRN, then the DCC shall notify the Electricity Distributor and/or Gas Transporter for the affected MPANs and/or MPRNs.

2.11 Where a User other than the Responsible Supplier for a Smart Metering System becomes aware of an error in the information recorded within the Smart Metering Inventory in respect of a Device that comprises that Smart Metering System, it shall raise an Incident in accordance with the Incident Management Policy.

2.12 Where a User receives a Response or Alert other than via the SM WAN, the User shall, where the Response or Alert is listed in the DCC User Interface Specification as one that is required to be returned to the DCC, send a 'Return Local Command Response' Service Request containing the Response or Alert to the DCC.

Appendix AH 'Self-Service Interface Access Control Specification

Add the additional row below to the table in clause 1.5.1 (DCC defined access).

BFD ID	Business Functional Domain Name	Service capability	Functional Component	DCC Defined Access
BFD15	Device Certificate realignment	Enable Users to trigger the process of Device Certificate realignment between the Smart Metering Inventory and a Device, where the User suspects there is a misalignment of Device Certificate between the Smart Metering Inventory and a Device.	Device Certificate realignment UC_CertificateAlign_001	Conditional. Access shall be granted to the Responsible Supplier.

This document has a Classification of **Clear**

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'

Annex D

Refinement Consultation responses

About this document

This document contains the full non-confidential collated responses received to the MP239 Refinement Consultation.

Question 1: Do you agree that the solution put forward will effectively resolve the identified issue?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	-
Scottish and Southern Electricity Networks	Network Party	Yes	The solution proposed looks to resolve the identified issue with the two scenarios highlighted on the modification report when this would not be possible. The five functional business requirements listed on Annex A Business Requirements detail this what is required of the solution.
E.ON Next Energy Limited	Large Supplier	Yes	The proposed solution will not prevent device certificate misalignment from happening and this was always unlikely due to the nature of how generation of device certificates works on devices. However, the solution does provide more timely and efficient mechanisms for remediation supporting delivery of services to energy consumers.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Yes	It enables Suppliers to update Certificates via the SSI rather than relying on raising DCC service requests.
EDF Energy	Large Supplier	Yes	We agree the proposed modification will address the issue raised.
Octopus Energy Ltd	Large Supplier	Agree	The proposal sets out clear steps which allow for the certificate misalignment to be corrected more readily than the current system.

Question 2: Do you agree that the legal text will deliver MP239?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	-
Scottish and Southern Electricity Networks	Network Party	Yes	The legal text clearly defines the requirements for error correction and user defined access.
E.ON Next Energy Limited	Large Supplier	Yes	While the legal text is updated to reflect the new way of working there are no changes to obligations.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	-	We have not reviewed the legal text.
EDF Energy	Large Supplier	Yes	The legal text appears to clearly state how the new process will be delivered.
Octopus Energy Ltd	Large Supplier	Yes	-

Question 3: Do you agree with the proposed implementation approach?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	We've been fully involved in the development of the modification, and fully support planned approach, resolution and outcome.
Scottish and Southern Electricity Networks	Network Party	Yes	Recommended dates for implementation allow for assessment.
E.ON Next Energy Limited	Large Supplier	Yes	An ideal implementation would involve full automation, but in the absence of this an SSI portal for raising misalignment issues in bulk is a considerably better approach than the current arrangement and will result in substantial time savings for all DCC Users and DCC partners.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Yes	We accept that the earliest possible implementation is June 2026 due to the requirement to amend the DUIS and the 12 month lead time for doing so.
EDF Energy	Large Supplier	Yes	The Implementation approach appears well thought out with delivery methodologies specified etc.
Octopus Energy Ltd	Large Supplier	Yes	The proposed implementation approach appears to cover the key issues initially introduced.

Question 4: Will there be any impact on your organisation to implement MP239?

Question 4				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
British Gas	Large Supplier	No	We do not need to make any changes.	-
Scottish and Southern Electricity Networks	Network Party	Unsure	We assume by the scenario highlighted by the SEC mod when the supplier updates the device certificates this scenario is also applicable for replacing slots 6 & 7 for DNO's, we would like to understand if this proposed change will have a positive impact on misaligned DNO device certificates. It would also be useful to understand how many devices are misaligned over and above the 140,000 detailed on this modification proposal.	MP239's focus is on the Device Certificate associated with credentials generated by the Devices, e.g. a Certificate belongs to a Device, not a Remote Party. Therefore, any Certificate in the Device Trust Anchor Cell belongs to Remote Party, not the Device itself. The scope of MP239 does not cover any Certificates held in the Trust Anchor Cells. The DCC has noted that as slots 6 & 7 holds certificates for DNOs, it is possible for the DNO to resolve the misalignment by triggering SR6.24.1. The number of Devices with misaligned Certificates fluctuates at any given time, due to ongoing manual corrections by the DCC. SECAS has requested the DCC to try quantifying historic manual corrections, which may provide clarity on the number of Devices impacted.
E.ON Next Energy Limited	Large Supplier	No	There is little impact other than rollout of training to demonstrate how to use the new SSI interface. The time and effort involved is going to be affected by how DCC elect to implement access to the new tool. i.e. what	The DCC has noted these details would only be expected to be defined during the detailed design stage, which would then be shared with customers at the Design Release Forum.

Question 4				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
			level of access is required? Will it work similarly to SMKI repo access? This has not been indicated at this time.	
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Yes	Staff will need to be trained on the new process and we will have to ensure that the SSI interface is available to appropriate users who will carry out the process.	-
EDF Energy	Large Supplier	Yes	Minor retraining and amendments to BAU processes.	-
Octopus Energy Ltd	Large Supplier	No	It appears that the proposal for MP239 covers automatically resolving some of these issues and preventing them in future. Any manual requirement from us will likely be less onerous than the current process of manual correction.	-

Question 5: Will your organisation incur any costs in implementing MP239?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	No costs	See above.
Scottish and Southern Electricity Networks	Network Party	No costs	N/A
E.ON Next Energy Limited	Large Supplier	No costs	Implementation of this SECMOD would result in a reduction in unnecessary site visits to exchange meters where gains are unable to be completed. Additional confidential rationale.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Less than £100k	We do not expect any material costs from implementing MP239.
EDF Energy	Large Supplier	No costs	No significant costs as no system changes required, all amendments are internal.
Octopus Energy Ltd	Large Supplier	No	Cost savings will be made where we are able to resolve certificate misalignment issues which sometimes end in meter replacement. By avoiding this unnecessary meter replacement and keeping the meter on the wall, there is a cost saving to be made.

Question 6: How long from the point of approval would your organisation need to implement MP239?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	No time required	See above.
Scottish and Southern Electricity Networks	Network Party	N/A	N/A
E.ON Next Energy Limited	Large Supplier	Very little time	But does depend on who can access the new SSI tools. DCC's procurement activity to replace specific services providers (e.g. DSP) will need to be considered to ensure any MP239 solution is maintained over the longer term.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	3 months	This will provide long enough to prepare briefing materials and ensure the correct staff had access to the SSI.
EDF Energy	Large Supplier	Nominal / Less than a week	No system changes required for EDF. Training and process changes should be implemented quickly.
Octopus Energy Ltd	Large Supplier	No Time needed	-

Question 7: Do you believe that MP239 would better facilitate the General SEC Objectives?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	We agree it will better facilitate General SEC Objective (a).
Scottish and Southern Electricity Networks	Network Party	Yes	This modification should better facilitate SEC Objective (a), as it will ensure that Devices are functioning as intended without replacing the existing Smart Meter.
E.ON Next Energy Limited	Large Supplier	Yes	This change would benefit a number of SEC objectives, but particularly in relation to energy consumer management and the ongoing efficient operation of smart meters, this change should only be seen as a win for everyone from the customer through to SECAS.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Yes	We agree with the Proposer's view "that MP239 will facilitate SEC Objectives (a)1 as it will ensure that Devices at a consumer's premises is functioning as intended without replacing the existing Smart Meter".
EDF Energy	Large Supplier	Yes	The modification should lead to an increase in healthy meters in line with the SEC objectives.
Octopus Energy Ltd	Large Supplier	Yes	The proposal meets SEC objectives: a) by ensuring the operation and interoperability of smart meters in consumers' premises which might currently be restricted due to certificate misalignment. c) by allowing working smart meters with aligned certificates d) by ensuring that after a COS certificates are able to be aligned allows for fair competition for the supply of energy as all have equal opportunities.

Question 8: Do you believe there will be any impacts on or benefits to consumers if MP239 is implemented?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	The quicker we can get the device out of a mismatched state (non comms), the quicker the customer will see a return to a full Smart service.
Scottish and Southern Electricity Networks	Network Party	Yes	This modification will ensure efficiency and functionality of meters at consumers properties.
E.ON Next Energy Limited	Large Supplier	Yes	This change provides us with a better route to green for non-communicating smart meters where the underlying cause is certificate alignment without the need to inconvenience a customer with a site visit. The change will also result in faster resolution of cos gain failures, restoring smart functionality to meters. Non-operating and cos gain failures are a current focus area for both DESNZ and The Authority.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Yes	Consumers will benefit as this will reduce the risk that meters are non-communicating for extended periods due to certificate mismatches.
EDF Energy	Large Supplier	Yes	The modification would support the efficient operation of smart meters in line with the first SEC objective.
Octopus Energy Ltd	Large Supplier	Yes	We believe there will be a positive impact on consumers if MP239 is implemented.

Question 8			
Respondent	**Category**	**Response**	**Rationale**
			By resolving or allowing a mechanism to more easily resolve certificate misalignment issues, as MP239 suggests, more consumers will have working smart meters allowing them to gain the benefits associated with a functioning smart meter.

Question 9: Noting the costs and benefits of this modification, do you believe MP239 should be approved?

Question 9			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	We think this makes sense. Currently there is a very longwinded manual process which can lead to long-term non-comms on meters. This would really help, and will directly avoid meter replacements etc.
Scottish and Southern Electricity Networks	Network Party	Yes	This will ensure more communicable meters moving forward without the need to replace meters.
E.ON Next Energy Limited	Large Supplier	Yes	-
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	Yes	There are sufficient meters affected by the issue to justify the cost, there are clear benefits to consumers and the efficiency of the Smart metering arrangements will be increased.
EDF Energy	Large Supplier	Yes	As per above replies, the costs and time to implement are negligible however there will be benefits to customers and DCC users which will outweigh these.
Octopus Energy Ltd	Large Supplier	Yes	The costs indicated seem reasonable when considering the volume of meters which could have certificate issues resolved by this modification. We note however that indicative costs vary largely between £161,000-£360,000 with no understanding of what would cause this to be towards the lower or high end of the range. We will monitor the proposed costs throughout the stages of the proposal considering the large range currently proposed.

Question 10: Please provide any further comments you may have.

Question 10		
Respondent	**Category**	**Comments**
British Gas	Large Supplier	Fully supportive of this mod. It will bring clear benefits to the whole supplier community and other parties (network operators etc.).
Scottish and Southern Electricity Networks	Network Party	N/A
E.ON Next Energy Limited	Large Supplier	We have significant concerns at the proposed implementation date of 2026 and would like to take the opportunity to underscore why this change is needed sooner. We sponsored and drove this SECMOD because of the significant operational pain and cost associated with the existing method of dealing with device certificate misalignment. Particularly in relation to failures within the change of supplier process where device certificate status is opaque and self-help impossible, we are forced to inconvenience customers with site visits and replace meters unnecessarily. Additional confidential rationale.
ENGIE Power Limited, ENGIE Gas Limited	Small Supplier	No further comment.
EDF Energy	Large Supplier	N/A
Octopus Energy Ltd	Large Supplier	-