

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 1.0

1 June 2024

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

1. Summary.....	3
2. Issue.....	3
3. Solution	8
4. Impacts	9
5. Costs	13
6. Implementation approach	13
7. Assessment of the proposal	14
8. Case for change.....	16
Appendix 1: Progression timetable	18
Appendix 2: Glossary	18

This document also has four annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the full Data Communications Company (DCC) Impact 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 Certificates. 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 number of Devices with misaligned Certificates fluctuates at any given time, due to ongoing manual corrections by the DCC and new submission for corrections by Suppliers.

The SEC currently requires the DCC to manually correct errors in the Smart Meter Inventory (SMI) where there is no other available method. Updating these manually is resource intensive and costly. The DCC noted that the Design, Built and PIT cost is less than the cost of processing the current number of manual corrections. 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. The Proposed Solution implementation is in two phases with a total cost of £504,542. If approved, implementation of Phase 1 is targeted for the DCC maintenance release in November 2024; and Phase 2 is targeted for the June 2025 SEC Release. This modification will be progressed as a Self-Governance Modification.

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, 0x8F3D 'Trusted Source Authentication Failure' or 0x8F1E 'Integrity check of content or format of command failed'). 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.

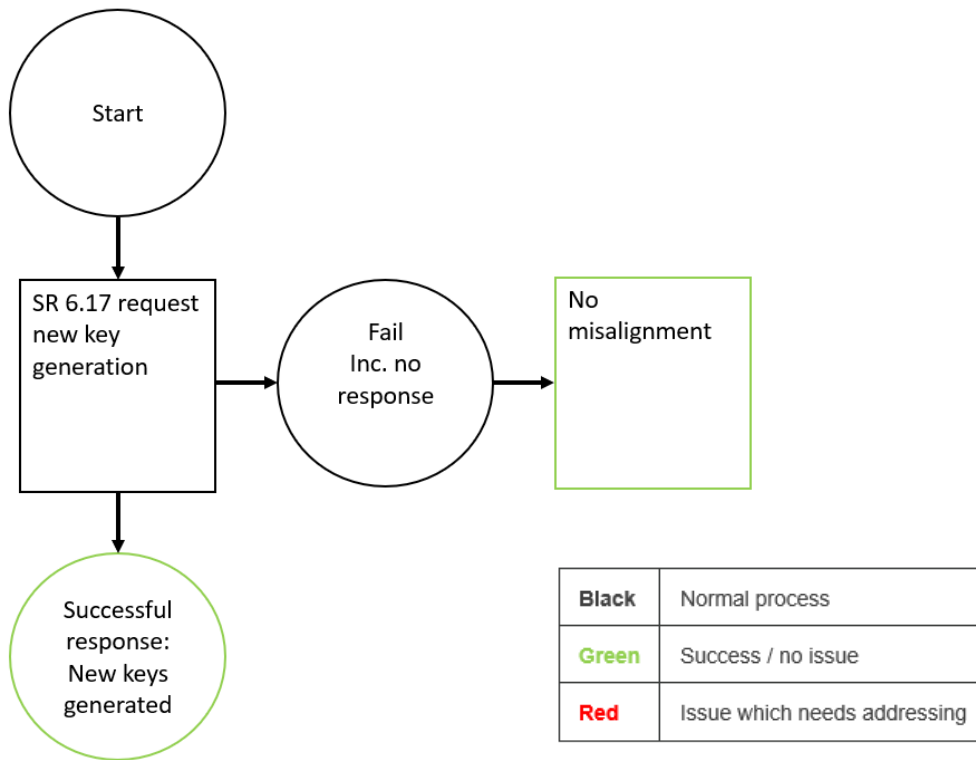
There are some Devices that become non-communicable after this process. Root cause analysis has identified that due to the reasons above, the Device Certificate (Device Signature (DS) or Key Agreement Key (KAK)) is misaligned with what is held within the DSP Master Key Store.

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.

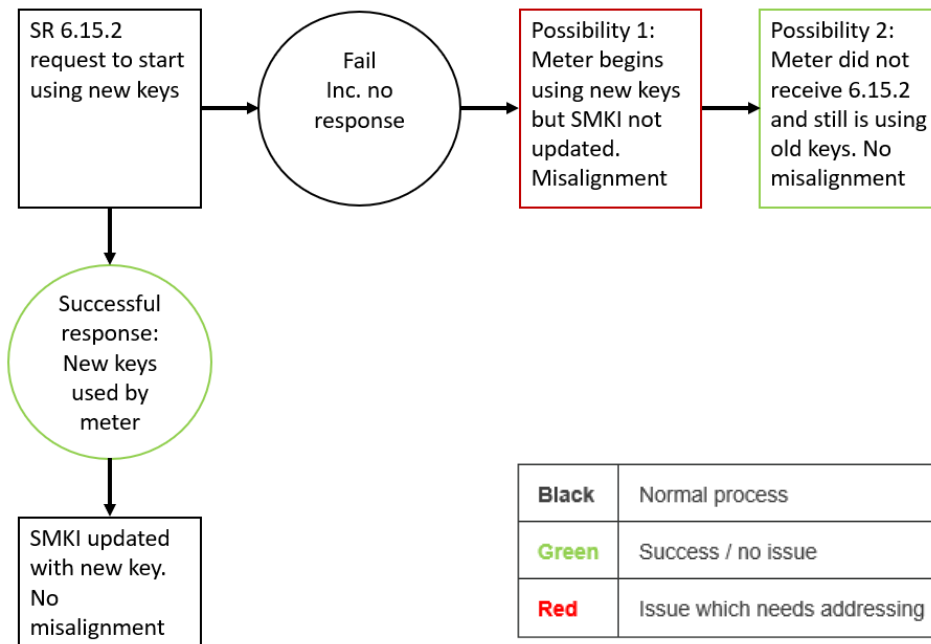
Suppliers have indicated they would like an enduring solution to resolve the Device Certificate misalignment issue without involving a manual SMI update.

The below diagrams set out the current process and issues:

Starting point when Supplier request for new key:



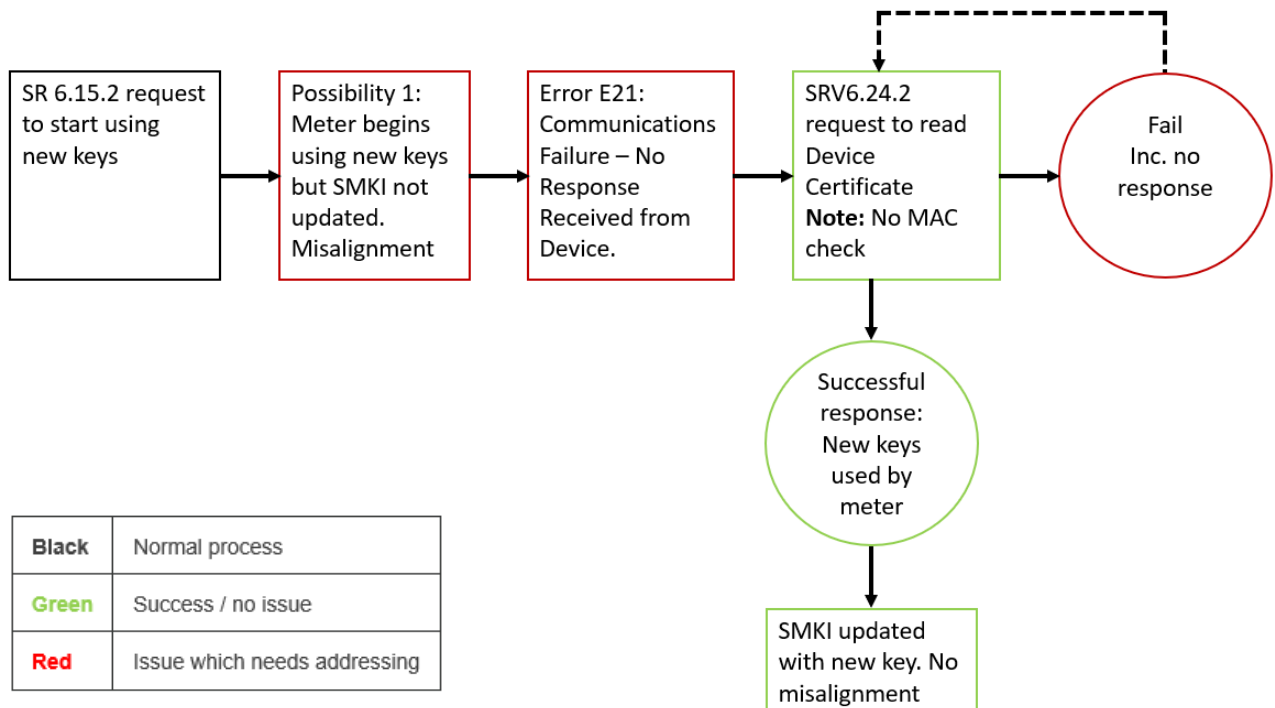
Issue when Supplier tries to use new keys:



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.



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 and new submission for corrections by Suppliers.

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

SEC Appendix AC Section 2.10 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 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 for them to gather this information.

The DCC has noted that the manual fix is costly and inefficient.

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.

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 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 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. The DCC are also 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.

3. Solution

The Proposed Solution will allow Suppliers to update the appropriate Certificates through the SSI or SSMI:

- Amend the Certificate Confirmation Scheme (CCS) cycle to work through all possible Access Control Broker (ACB) Key Agreement Keys (KAK) and Key Agreement Device Certificates, which will help to identifying the correct Device Certificate;
- 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

Managed by

Certificate in early stage of I&C process, post-I&C Certificate Update process and via SSI/SSMI during in-life operation;

- Add information to Service Audit Trail (SAT) logs for CCS timeout to indicate which cycle and the stage of the current cycle;
- 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.

The DCC recognised the urgency of getting a solution in place as early as possible due to the current scale of the issue and are delivering the Proposed Solution in a phased approach.

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.

Suppliers noted in the Refinement Consultation that their impacts would be limited to staff training and adapting new business processes which would not be onerous.

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.

DCC recognises the urgency of getting a solution in place as early as possible due to the current scale of the issue and are delivering a phased implementation approach.

Phase 1

The solution requires several individual changes as described below, and would be delivered in a Phase 1, as part of a maintenance release.

1. Enhancement of the Certificate Confirmation Scheme (CCS) to use the current "in use" device KA certificate along with all "pending" device KA certificates for that device. The Certificate Confirmation Action will be amended so that the processing will loop through each candidate device KA certificate and ACB certificate combination, and on successful response will set the device KA certificate used in the successful request as "in use".
2. Enhance the logging during the execution of the CCS so that unsuccessful attempts (indicated by a response timeout) will record in the Service Audit Trail, the CCS cycle, and the stage of the current cycle.
3. Provide a new screen in the SSMI to allow an authorised DCC User to upload a list of devices for which the CCS should be invoked.
4. Provide a one-off report of devices which have a device KA certificate marked as "pending" with a later start date than the device KA certificate currently marked as "in use". This report thus creates a candidate list of devices which may have an inconsistency in the DSP system's view of the device KA certificate held on the device. This list can then be filtered by the DCC's DS&A team, and an internal report provided to identify those devices which are not currently communicating. DCC will then and submit those devices via the SSMI to invoke the enhanced CCS (see point 1 above).

These changes will provide DCC with initial functionality for correction of device certificate issues within the current device estate.

Phase 2

The following remaining changes will be delivered as Phase 2 as part of the next scheduled SEC release.

1. Invocation of the enhanced CCS (see point 1 in Phase 1) during the Install and Commission process when the DSP attempts to communicate with a device for the first time.
2. Provide a new screen in the SSI to allow an authorised Service User (the Responsible Supplier) to request the enhanced CCS (see point 1 in Phase 1) to be invoked for a single device.
3. Invocation of the CCS when there is a timeout for the response to a SRV6.15.2 request to place new device certificates on the device. In this scenario the CCS will be modified to only iterate over the current “in use” device KA certificate and the “new” device KA certificate that was contained in SRV6.15.2.
4. Provide a new screen in the SSMI to allow an authorised DCC User to set the “in use” certificates for a single device. This will provide the ability to set KA and DS certificates for both ACB and device certificates.
5. Provide a new capability to deliver a report to DCC’s DS&A team which provides an agreed set of information for all the certificates held in the DSP’s Key Management System database¹. This reporting will follow a similar pattern to other high volume Inventory extracts, with a capability for a full extract if necessary but with an incremental report of changes provided on a daily basis as the normal reporting pattern. The details of the report will be agreed between DSP and the DS&A team as part of the Design phase.

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

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’

¹ Which is a copy of the data held in the SMKI repository.

- 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 to update the processing rules in SRV 6.15.2 and SRV 8.11.

Technical specification versions

This modification will impact Appendix AD 'DCC User Interface Specification' (DUIS). The proposed changes will be to update the processing rules in SRV 6.15.2 and SRV 8.11.

There will also be changes to the DCC User Gateway Interface Design Specification (DUGIDS).

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 implementation cost to implement this modification is £504,542.

The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design, Build and PIT	£339,178
Integration Testing, Systems Integration Testing (SIT) and User Integration Testing (UIT)	£147,331
Implement to Live	£5,649
Application Support (3 months)	£12,384

More information can be found in the DCC Impact 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

Approved implementation approach

The CSC has agreed an implementation date of:

- **26 June 2025** (June 2026 SEC Release) if a decision to approve is received on or before 26 June 2024; or
- **25 June 2026** (June 2026 SEC Release) if a decision to approve is received on or before 25 June 2025.

This modification will impact the DUIS which is only updated annually. This implementation approach is based on the DCC's assessment of a ten-month delivery time from procurement to implementation, including a DCC maintenance release four months after approval.

It is not possible to target the June 2024 SEC Release, which is the next scheduled DUIS uplift, due to the ten months' timescale required for implementation.

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.

Solution development

Root cause of the issue

During CSC discussions, members questioned whether this modification should focus on addressing the root cause 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 would be a difficult issue to solve (due to potential hardware defects) as there are a myriad of reasons why messages may fail.

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 Impact 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.

Links to DP267

During Working Group discussions, a member queried if the solution proposed for MP239 could be used to resolve the issue raised in [DP267 'Facilitating the installation and commissioning of meters triaged under Use Case 004'](#). SECAS noted this has been investigated and discussed with the DCC. The DCC concluded that the MP239 solution would not resolve the DP267 issue.

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. This will also reduce issues with prepayment top-up operation by having the Certificate misalignment issue resolved. The DCC noted that the Design, Built and PIT cost is less than the cost of processing the current number of manual corrections. 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.

The Working Group agreed the benefits of the modification justified the cost and were supportive for this modification to progress.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that MP239 will facilitate SEC Objective (a)² 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 facilitates SEC Objectives (c)³ and (d)⁴.

² Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

³ 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.

⁴ Facilitate the effective competition between persons engaged in, or in Commercial Activities connected with, the Supply of Energy.

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).

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.

Final conclusions

Working Group

The Working Group supported the Proposed Solution and two phased implementation approach noted in the DCC Impact Assessment. They also noted DCC's comment that the Design, Built and PIT cost is less than the cost of processing the current number of manual corrections.

Change Sub-Committee

The CSC agreed that the modification should proceed to Report Phase. One CSC member highlighted that the benefit was not quantified in the report. They also advised that release-based regression testing costs were noted but a quantified figured was not provided. They acknowledged that this issue with regression test costs being detailed post Release was recently realised but wished to flag this.

SECAS notes that the DCC has confirmed that the cost of Design, Build and PIT is less that the cost of the manual corrections, although no exact costings have been provided. The DCC also noted Supplier inconvenience to manage and organise the corrections, and Suppliers are keen to have this resolved as soon as possible. The CSC are actively addressing the issue of unknown regression testing costs to develop a suitable solution whereby they are governed more closely however in order

to schedule this modification for the June 2025 Release approval by the Change Board is needed before the end of June 2024.

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	29 May 2024
Modification discussed with Working Group	5 Jun 2024
Modification Report approved by CSC	7 Jun 2024
Modification Report Consultation	11– 17 Jun 2024
Change Board Vote	26 Jun 2024

Italics denote planned events that could be subject to change

Appendix 2: Glossary

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

Glossary	
Acronym	Full term
ACB	Access Control Broker
CCS	Certificate Confirmation Scheme

Managed by

Glossary	
Acronym	Full term
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
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

SEC Modification Proposal, SECMP0239, DCC CR5170

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

Full Impact Assessment (FIA)

Version:	0.31
Date:	29th May 2024
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	Phase 1 Technical Solution.....	9
4.2	Phase 2 Technical Solution.....	10
4.3	Application Components	11
4.4	Technical Specifications	12
4.5	Infrastructure Impact.....	12
4.6	Other Changes	12
5	Implementation Timescales and Approach.....	13
5.1	Pre-Integration Testing (PIT).....	13
5.2	System Integration Testing (SIT)	13
5.3	User Integration Testing (UIT).....	14
5.4	Changes to DS&A Reporting	15
6	Costs and Charges.....	16
6.1	Changes to the Agreement	16
	Appendix A: Glossary	18

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement SECMP0239, Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue of **£504542**, which comprises:
 - £339,178 in Design, Build, and Pre-Integration Testing (PIT)
 - £165,364 in Implementation, including integration testing and deployment
- Expected effort of 10 months to complete, including a maintenance release after four months.

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 require an enduring solution to resolve the certificate misalignment issue without involving a manual SMI update.

Modification Benefits

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

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

By dividing the solution implementation into two phases, resolving existing certificate misalignments, which is a major concern for SEC Parties, can be addressed in the short-term through a Maintenance Release, while an enduring solution becomes available at a later stage in a SEC Release.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
18/05/2024	0.1	Initial version, for DCC internal review
22/05/2024	0.2	Technical solution reviewed and approved
29/05/2024	0.31	Commercials challenged and accepted, typo corrected

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
3	SECMP0239 CR5170 - PIA - Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue v0.21	DCC	30/10/2023

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, and submitted on the 30th October.

The FIA was requested on 2nd April 2024.

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 Service Reference Variant (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 (DS&A) 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 while 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. As things stand, each change must be carried out in a single operation by the DCC, and batches of changes cannot be made.

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 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, e.g., 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. • When the previous Supplier has ceased to trade, and a Supplier of Last Resort (SoLR) has been nominated.

Ref.	Requirement
	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 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 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.

DCC derived the following detailed requirements for the necessary reporting which impact the DSP and the DCC Data Science and Analytics (DS&A) team:

1. for any installed Device (commissioned, suspended, and whitelisted, install Not commissioned), all the certificates associated with that Device.
2. full file monthly and daily delta (or follow DeviceKeyMapping method, which is full file by exception, and then delta every four hours).
3. the Device certificates whether or not there is a newer certificate than the current in use, the certificate serial number, and certificate generated by a Certificate Signing Request (CSR).
4. status of the certificates.

4 Description of Solution

The modification impacts the DSP only and DS&A.

The solution will amend the Certificate Confirmation Scheme (CCS) so that where there is uncertainty as to which device Key Agreement (KA) certificate is on a device then a retrieval will be attempted using each possible such certificate until a response is received and the certificate is identified. The Service Audit Trail (SAT) logging will be enhanced to indicate the current stage of CCS processing. This revised functionality can be initiated through installation, SRV 6.15.2 timeout, SSI, and SSMI. Additionally, there will be a new report of devices which may have the wrong certificate marked as “in use” and the ability for a SSMI user to explicitly set the “in use” certificates on a device.

DCC recognises the urgency of getting a solution in place as early as possible due to the current scale of the issue, and are delivering a phased approach. This, and the increased detailed reporting requirements, has led to an increase in the anticipated costs for this Modification.

4.1 Phase 1 Technical Solution

The solution requires several individual changes as described below, and would be delivered in a Phase 1, as part of a maintenance release.

1. Enhancement of the Certificate Confirmation Scheme (CCS) to use the current “in use” device KA certificate along with all “pending” device KA certificates for that device. The Certificate Confirmation Action will be amended so that the processing will loop through each candidate device KA certificate and ACB certificate combination, and on successful response will set the device KA certificate used in the successful request as “in use”.
2. Enhance the logging during the execution of the CCS so that unsuccessful attempts (indicated by a response timeout) will record in the Service Audit Trail, the CCS cycle, and the stage of the current cycle.
3. Provide a new screen in the SSMI to allow an authorised DCC User to upload a list of devices for which the CCS should be invoked.
4. Provide a one-off report of devices which have a device KA certificate marked as “pending” with a later start date than the device KA certificate currently marked as “in use”. This report thus creates a candidate list of devices which may have an inconsistency in the DSP system’s view of the device KA certificate held on the device. This list can then be filtered by the DCC’s DS&A team, and an internal report provided to identify those devices which are not currently communicating. DCC will then and submit those devices via the SSMI to invoke the enhanced CCS (see point 1 above).

These changes will provide DCC with initial functionality for correction of device certificate issues within the current device estate.

4.2 Phase 2 Technical Solution

The following remaining changes will be delivered as Phase 2 as part of the next scheduled SEC release.

1. Invocation of the enhanced CCS (see point 1 in section 4.1) during the Install and Commission process when the DSP attempts to communicate with a device for the first time.
2. Provide a new screen in the SSI to allow an authorised Service User (the Responsible Supplier) to request the enhanced CCS (see point 1 section 4.1) to be invoked for a single device.
3. Invocation of the CCS when there is a timeout for the response to a SRV6.15.2 request to place new device certificates on the device. In this scenario the CCS will be modified to only iterate over the current “in use” device KA certificate and the “new” device KA certificate that was contained in SRV6.15.2.
4. Provide a new screen in the SSMI to allow an authorised DCC User to set the “in use” certificates for a single device. This will provide the ability to set KA and DS certificates for both ACB and device certificates.
5. Provide a new capability to deliver a report to DCC’s DS&A team which provides an agreed set of information for all the certificates held in the DSP’s Key Management System database¹. This reporting will follow a similar pattern to other high volume Inventory extracts, with a capability for a full extract if necessary but with an incremental report of changes provided on a daily basis as the normal reporting pattern. The details of the report will be agreed between DSP and the DS&A team as part of the Design phase.

¹ Which is a copy of the data held in the SMKI repository

4.3 Application Components

Components impacted by this Modification are detailed in the following tables.

Component	Phase 1 Description
SSMI	Allow a user to initiate CCS for a list of devices
Physical Data Model	Add attributes to manage candidate KA lists for a device
Data Management	New web service to initiate CCS for a list of devices. For each device: * Call Key Management System (KMS) to determine the list of candidate device KA certificates and store against the device * Initiate CCS for the device Amend CCS processing to include iterating through the candidate device KA certificate list where one is present.
Transform	Where a device KA certificate is provided in the metadata of a CCS request then pass that to the security component to use for the MAC
Security	Add new variant where device KA certificate can be passed for generating a MAC
Request Management	When creating a Service Request for CCS, include the candidate device KA certificate in the metadata. When processing a response for CCS, then use the device KA certificate from the request's meta data when validating the GMAC and set the current in-use device KA certificate to that certificate. When writing SAT, include retrieval metadata in the SAT record's ResponseCode element.
Key Management System	New one-off query to identify all devices where there is a later pending certificate than the one marked as "in use" (<i>DCC will use SAT data to determine whether devices are communicating</i>) New service to provide list of device KA certificates (in use, then pending most recent first)

Table 1: Application Components impacted by Phase 1

Component	Phase 2 Description
SSI	Allow user to initiate CCS for a device
SSMI	New screen to allow user to enter a Certificate Serial Number (CSN) to be marked as in-use for a device
Data Management	Add Service to validate CSN for a device and to either update the SMI (and Motorway Cache) with ACB certificate or call KMS to set the device certificate as in use.

	When initiating CCS as a result of installation, call KMS to determine the list of candidate device KA certificates and store against the device. New CCS initiation to be passed old and new device KA certificates.
Request Management	On timeout of SRV6.15.2, initiate CCS for the old and new device KA certificates
Key Management System	Service to mark a specific certificate as in use on a device. New extract to provide information about all certificates held within the KMS, and an incremental extract to provide changes. Amend update logic to record last change time for certificates (used for incremental selection and included in report).
ESI/Routing Rules	Add routing rules to deliver the certificate extracts to DCC via ESI

Table 2: Application Components impacted by Phase 2

4.4 Technical Specifications

Although this Modification requires a DCC User Interface Specification (DUIS) change, the changes will only impact the wording of the DUIS and DCC User Gateway Interface Design Specification (DUGIDS) documentation (to update the processing rules in SRV 6.15.2 and SRV 8.11).

4.5 Infrastructure Impact

There is no impact to infrastructure as part of this Modification. Additional processing and storage are likely to be required. However, they are not sufficiently large to warrant the procurement of additional compute power or storage.

4.6 Other Changes

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

5 Implementation Timescales and Approach

The changes identified as Phase 1 as part of a maintenance release as soon as they can be implemented and scheduled for release. These changes are intended to provide DCC with an initial set of facilities for correction of device certificate issues within the current device estate.

Phase 2 changes are anticipated to be part of a full SEC Release.

The pre-integration phase is expected to take approximately three months for each Phase. Allowing for integration testing, the change will be ready to schedule to a production release after approximately ten months.

5.1 Pre-Integration Testing (PIT)

PIT testing will include testing both existing updated DSP Use Cases, and new Use Cases developed for the SECMP0239 Change. A series of regression tests will also be run.

Automated testing will be used where possible. This includes the legacy framework used by the PIT System Test team and the Early Automated System Testing approach.

No performance testing is required for this change.

5.2 System Integration Testing (SIT)

This Modification is planned to be implemented in two separate phases. Phase 1 will be implemented in the SIT-A environment and tested via a maintenance release. Phase 2 will be implemented in the SIT-B environment and will be part of a SEC System Release.

For Phase 2, there will be a Post-PIT CR that provides the SIT response for the release as a whole, covering the testing of individual CRs in the scope of the release, as well as activities that are common to all CRs in the scope, e.g. Test Plans, SIT Management and Governance.

The change would require an element of release-based regression testing outside the DSP in SIT and UIT as the changes impact devices. The SIT volumes of testing are anticipated as follows.

Test Phase	Type	Total Tests	Plan Start	Plan End	Workdays	Envir Avail	Net Days	Re-Test
SMETS2 Device Certificate Resolution SIT A Nov 24	Automated	30	11/10/2024	24/10/2024	10	85%	9	1.4
SMETS2 Device Certificate Resolution SIT A Nov 24	Manual	18	11/10/2024	24/10/2024	10	85%	9	1.4
SMETS2 Device Certificate Resolution SIT B June 25	Automated	164	01/02/2025	01/04/2025	42	85%	36	1.4
SMETS2 Device Certificate Resolution SIT B June 25	Manual	46	01/02/2025	01/04/2025	42	85%	36	1.4
Totals/Averages		258	11/10/2024	01/04/2025	120	85%	102	1.4

Figure 1: Expected SIT Test Volumes

The percentage of manual testing is higher than usually seen during SIT testing due to the Solution Test scope shown in the table following, where manual verifications of reporting are required throughout the testing, as well as Non-Motorway testing such as SSI and SSML.

Solution Testing	Phase 1 /2
Verify a Potential Problem Devices Report is generated with the relevant information and correct formatting and sent to the DCC via the ESI Gateway.	November 2024 maintenance release June 2025 SEC System Release
Verify that a report on the certificates held in DSP can be generated.	November 2024 maintenance release June 2025 SEC System Release
Verify that via the SSMI, an audit log is updated with certificate updates.	June 2025 SEC System Release
For each scenario, update the device DS or KA certificate for an ESME and GSME to 'pending' state in the Master Key Store (MKS).	November 2024 maintenance release June 2025 SEC System Release
For Scenario 1, execute SRV 6.15.2, observing the DSP timeout and verify the Certificate Confirmation Scheme (CCS) is initiated.	June 2025 SEC System Release
For Scenario 2, execute SRV 6.24.2 for an ESME and GSME and verify that SMI updates the KA certificates to 'in-use' state.	June 2025 SEC System Release
For Scenario 3, verify that a DCC User is able to trigger a CCS via the Self-Service Management Interface (SSMI) and ensure the ESME and GSME are able to respond to Service Requests following completion of the CCS.	November 2024 maintenance release June 2025 SEC System Release
For Scenario 4, verify that a DCC Service User is able to trigger a CCS via the Self-Service Interface (SSI) and ensure the ESME and GSME are able to respond to Service Requests following completion of the CCS.	June 2025 SEC System Release
For Scenario 5, execute SRV 6.15.2, observe the DSP timeout and verify the CCS is initiated.	June 2025 SEC System Release

Table 3: SIT Test Areas alongside the phases planned for Modification

For the SIT-A testing (maintenance release), it is expected that the SIT team will make use of existing devices. For the SEC Release phase 2 SIT testing, a CSP North and CSP South & Central Comms Hub will be required, both with ESME and GSME devices.

SIT Regression testing scope and costs will be determined as part of a separate post-PIT (or Release) Change Request.

There is no requirement for any SMETS1 devices in SIT or UIT, as the testing scope does not apply to SMETS1.

5.3 User Integration Testing (UIT)

A limited amount of testing is required to confirm that device certificate misalignments can be successfully resolved in each UIT test environment. Phase 1 will be implemented in the UIT-A environment and tested via a maintenance release. Phase 2 will be implemented in the UIT-B environment and will be part of a SEC System Release.

For phase 2, three different SMETS2 device sets (for CSP North, and CSP South & Central) will exercise both automated CCS initiation where no response is forthcoming for a SRV 6.15.2, and manual CCS initiation via SSI/SSMI.

The facility to directly update certificate data via SSI/SSMI will be tested by running the following tests:

- amend SSI/SSMI to allow an authorised user to initiate CCS using:

- o SSI – for a single device (phase 2); and
- o SSMI – for a set of devices (phase 1)
- amend SSMI to allow an authorised user to set the current certificate(s) for a device (phase 2).

The enhanced Service Audit Trail (SAT) logging and SSMI audit logging associated with the new functionality will also be verified.

The following total test volumes and test throughputs are required as part of developing the Modification:

CR5170						
Test Type	Cost per Test Categorisation	Type	Number of Tests	Re-Test Factor	Total Tests	Notes
Functional (SMETS2)	Complex	Manual	0	1.4	0	
Functional (SMETS2)	Medium	Manual	3	1.4	4	3 I&C
Functional (SMETS2)	Simple - SRs	Manual	141	1.4	197	3 Decomm; 6 CCS Resolutions; SR checks (72); SSI/SSMI/SAT checks
SMETS2 Regression	Regression Test Packs - SRs	Automated	0	1.1	0	
			144		202	

Table 4: UIT Test Volumes

For the Phase 2 UIT testing, both CSPs will be required, both with ESME and GSME devices. UIT Regression testing scope and costs will be determined as part of a separate post-PIT (or Release) Change Request.

5.4 Changes to DS&A Reporting

The design for the DS&A reporting to meet the detailed requirements above will take place as part of the detailed design phase of implementation.

6 Costs and Charges

This section indicates the costs for all phases of application development for this Modification. Note these costs assume a release of just this SEC Modification without any other Modifications or Change Requests in the release, and without the regression testing required during the Integration Testing, which is not truly reflective of the post-PIT test costs. A calculation of those costs will be carried out when the contents of the future SEC Release are finalised, and the post-PIT costs determined through a "Release CR" also referred to as a "Post-PIT CR".

£	Design, Build, and PIT	Integration Testing, SIT and UIT	TTO	Application Support	Total
SECMP0239	£339,178	£147,331	£5,649	£12,384	£504,542

Design	The production of detailed System and Service designs to deliver all requirements.
Build	The development of the designed Systems and Services to create a solution (e.g., code, systems, or products) that can be tested and implemented.
Pre-Integration Testing (PIT)	Each Service Provider tests their own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.
Systems Integration Testing (SIT)	All the Service Provider's PIT-complete solutions for a Release are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution.
User Integration Testing (UIT)	Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.
Implementation to Live (TTO)	The solution is implemented into production environments and made ready for use by Users as part of a live service.
Application Support	The Contractor has allowed for an increase of four low complexity support cases per month for the duration of three months, immediately following the release to Production of both Phase 1 & 2.

6.1 Changes to the Agreement

The DSP contract updates will be agreed and detailed within the Contract Amendment Note (CAN) and will impact the following schedules:

- Schedule 2.1 (DCC Requirements): addition of new requirements for this change
- Schedule 3 (DCC Responsibilities): update to reflect the addition of new DCC Responsibilities

- Schedule 4.1 (DSP Solution): solution design documents
- Schedule 6.1 (Implementation Planning): addition of new milestones
- Schedule 7.1 (Charges and Payment): revisions to incorporate charges and payment

Appendix A: Glossary

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

Acronym	Definition
ACB	Access Control Broker
CAN	Contract Amendment Note
CCS	Certificate Confirmation Scheme
CHF	Communications Hub Function
CoS	Change of Supplier
CR	DCC Change Request
CSP	Communications Services Provider
DCC	Data Communications Company
DS&A	Data Science and Analytics
DS	Digital Signature
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
GBCS	Great Britain Companion Specification
GPF	Gas Proxy Function
GSME	Electricity Smart Metering Equipment
GUID	Global Unique Identifier
KA	Key Agreement
KAK	Key Agreement Key
KMS	Key Management System
MAC	Message Authentication Code
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
RAID	Risks, Assumptions, Issues, and Dependencies
ROM	Rough Order of Magnitude (cost)
SAT	Service Audit Trail
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
SMKI	Smart Metering Key Infrastructure
SoLR	Supplier of Last Resort
SR	Service Request
SRV	Service Reference Variant
SSMI	Self Service Management 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 1.0

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 AD ‘DCC User Interface Specification’

These changes have been redlined against Appendix AD version 5.2.

Amend Clause 3.8.68.4 as follows:

3.8.68 Update Security Credentials (Device)

3.8.68.1 Service Description

Service Request Name	UpdateSecurityCredentials(Device)	
Service Reference	6.15	
Service Reference Variant	6.15.2	
Eligible Users	Import Supplier (IS) Gas Supplier (GS)	
Security Classification	Critical	
BusinessTargetID - Device applicable to this request	Type Electricity Smart Meter (ESME) Gas Smart Meter (GSME) Gas Proxy Function (GPF)	
Can be future dated?	No	
On Demand?	Yes	
Capable of being DCC Scheduled?	No	
Command Variants applicable to this Request - (Only one populated)	For Service Request 4 - Transform For Signed Pre-Commands, choice of: 5 - Send (Critical) 6 - Return for local delivery (Critical) 7 - Send and Return for local delivery (Critical)	
Common Header Data Items	See clause 3.4.1.1	
Data Items Specific to this Service Request	See Specific Data Items Below	
Possible responses from this Service Request	These are the possible responses applicable to this Service Request. Please see clause 3.5 for more details on processing patterns • Acknowledgement • Response to Transform Request - PreCommand Format • Service Response from Device – GBCSPayload • Response to a Command for Local Delivery Request – LocalCommand Format Also see Response Section below for details specific to this request	
Response Codes possible from this Service Request	See clause 3.5.10 for Common Response Codes	
GBCS Cross Reference	Electricity	Gas
GBCS MessageCode	0x000B	0x000B

GBCS Use Case	CS02d	CS02d
---------------	-------	-------

3.8.68.2 Specific Data Items for this Request

UpdateSecurityCredentialsDevice Definition

Data Item	Description / Valid Set	Type	Mandatory	Default	Units
DeviceCertificate	The Device Digital Signing or Key Agreement Public Security Credentials to replace the existing one.	sr:Certificate (xs:base64Binary)	Yes	None	N/A

Table 1 : UpdateSecurityCredentialsDevice (sr:UpdateSecurityCredentialsDevice) data items

3.8.68.3 Specific Validation for this Request

No specific validation is applied for this Request, see clause 3.2.5 for general validation applied to all Requests and clause 3.10.2 for Public Security Credentials validation.

3.8.68.4 Additional DCC System Processing

When the DCC receives a Response indicating Success from an Update Security Credentials (Device) the DCC Systems are updated to record which Device Certificates are currently in use by the Device.

When the DCC receives no Response from an Update Security Credentials (Device) the DCC Systems shall initiate a Command using both the old and new Device Certificates to determine which Device Certificates are currently in use by the Device. If the DCC receives a Response to the Command using the new Device Certificate, then the DCC Systems are updated to record which Device Certificates are currently in use by the Device.

Amend Clause 3.8.114.4 as follows:

3.8.114 Update HAN Device Log

3.8.114.1 Service Description

Service Request Name	UpdateHANDeviceLog
Service Reference	8.11
Service Reference Variant	8.11
Eligible Users	Import Supplier (IS) Gas Supplier (GS) Other User (OU) (Type 2 CAD Only) Other Users may only add (or remove) Type 2 Devices that are not IHDs to (from) a HAN Device Log.
Security Classification	Non Critical

BusinessTargetID - Device Type applicable to this request	Communications Hub Function (CHF)
Can be future dated?	DSP
On Demand?	Yes
Capable of being DCC Scheduled?	No
Command Variants applicable to this Request (Only one populated)	1 – Send (Non-Critical) 2 – Return for local delivery (Non-Critical) 3 – Send and Return for local delivery (Non-Critical)
Common Header Data Items	See clause 3.4.1.1
Data Items Specific to this Service Request	See Specific Data Items Below
Possible responses from this Service Request	These are the possible responses applicable to this Service Request. Please see clause 3.5 for more details on processing patterns • Acknowledgement • Service Response (from Device) – GBCSPayload • Response to a Command for Local Delivery Request – LocalCommand Format Also see Response Section below for details specific to this request
Response Codes possible from this Service Request	See clause 3.5.10 for Common Response Codes
GBCS Cross Reference	Communications Hub Function
GBCS MessageCode	Request Type Add - 0x0001 Request Type Remove - 0x0002
GBCS Use Case	Request Type Add - CCS01 Request Type Remove - CCS02

3.8.114.2 Specific Data Items for this Request

UpdateHANDeviceLog Definition

Data Item	Description / Values	Type	Mandatory	Default	Units
ExecutionDateTime	A User shall only add this Data Item to the Service Request where they require the Service Request to be executed at a future date and time. The UTC date and time the User requires the command to be executed on the Device. Date-time in the future that is either $\leq$ current date + 30 days or the date = '3000-12-31T00:00:00Z'	xs:dateTime	No	None	UTC Date-Time
DeviceID	Device ID of a Device to be added to or removed from the Communications Hub Function Whitelist or removed from it. A User must send one Service Request per Device to add or remove from the Communications Hub Function (CHF) Device Log.	sr:EUI (See clause 3.10.1.3)	Yes	None	N/A
RequestType	Indicates whether the request is to add or remove the Device from the Communications Hub Function Whitelist. Valid set: - Add - Remove	Restriction of xs:string (Enumeration)	Yes	None	N/A
AddDeviceToCHF Whitelist	List of data items required to add the Device to the Communications Hub Function Whitelist.	sr:AddDeviceToCHF Whitelist	Device to be added to Whitelist: Yes Device to be removed from Whitelist: N/A	None	N/A

Table 2 : UpdateHANDeviceLog (sr:UpdateHANDeviceLog) data items

AddDeviceToCHFWhitelist Definition

Data Item	Description / Values	Type	Mandatory	Default	Units
JoinTimePeriod	Defines the time period in seconds during which the Communications Hub Function will permit the device being added to join the HAN and communicate with the Communications Hub Function.	Restriction of xs:positiveInteger (minInclusive = 1 maxInclusive = 3600)	Yes	None	Seconds
InstallCode	Installation Credentials. Minimum length 6 (octets) to Maximum Length 16 (octets) equating to from 12 to 32 characters	Restriction of xs:hexBinary (minLength = 6, maxLength = 16)	Yes	None	N/A
ImportMPxN	The reference number identifying an electricity or a gas metering point.	sr:ImportMPxN (Restriction of xs:string (minLength = 1, maxLength = 13))	ESME, HCALCS and GSME: Yes Otherwise: N/A	None	N/A
SecondaryImportMPAN	The reference number identifying a Twin Element Import electricity secondary metering point.	sr:MPAN (Restriction of xs:string (minLength = 13, maxLength = 13))	No	None	N/A
ExportMPAN	The reference number identifying an Export electricity metering point.	sr:MPAN (Restriction of xs:string (minLength = 13, maxLength = 13))	No	None	N/A

Table 3 : AddDeviceToCHFWhitelist (sr:AddDeviceToCHFWhitelist) data items

3.8.114.3 Specific Validation for this Request

See clause 3.2.5 for general validation applied to all Requests and clause 3.10.2 for Execution Date Time validation.

For this Request, the general Authorisation Checks as defined below shall not be carried out where an IHD is being added to the Device Log by a User and the command is requested for Local Delivery only.

- a Response Code of E4 as defined in clause 3.2.4 “Verify that the User, in the User Role defined in the Service Request is a Eligible User for the Device”

Response Code	Response Code Description
E081101	The Device ID of a Device to be added to the CHF Whitelist is already associated with another CHF Whitelist

E081102	The Device ID of a Device to be removed is not included in the CHF Whitelist
E081104	The Device Type of the Device to be added to the Whitelist is invalid, e.g. if it is a Communications Hub Function or Gas Proxy Function
E081105	The status of the Device being added to the Whitelist is not 'Pending' or 'Whitelisted'
E081106	If the Request Type is: • 'Add'. It doesn't include the Add Device CHF Whitelist element • 'Remove'. It does include the Add Device CHF Whitelist element
E081107	The Device ID of the Device to be added to or removed from the Whitelist does not exist
E081108	The User Role is not authorised to add this Device Type to the HAN Device Log or remove it from it
E081109	The User is not the registered organisation for all of the MPxNs in the Service Request (This check supersedes the general Authorisation Check associated to Response Code E4 only for Request Type 'Add' (please note the check associated to Response Code E4 is applicable to Request Type 'Remove'))
E081110	The Service Request contains an Invalid MPAN Type, e.g. the Import MPxN is populated with an Export MPAN
E081111	The Service Request refers to a SMETS2+ Device and the InstallCode field is not 32 characters (representing 16 octets) in length.

3.8.114.4 Additional DCC System Processing

Upon receipt of a successful Response resulting from the UpdateHANDeviceLog Service Request to Add a Device, the DCC shall, for the specified DeviceID identified within the Service Request, perform the following action.

- a) Update the Smart Metering Inventory and set the Device status of the DeviceId to 'Whitelisted'
- b) Where the DeviceID to be added to HANDeviceLog is an Electricity Smart Meter or a Gas Smart Meter, the association between the DeviceID and its MPxN(s) is recorded in the Smart Metering Inventory and DCC Alert N16 is sent to the Electricity Distributor(s) or Gas Transporter (as applicable)

The DCC Systems shall wait for a timeout period to receive the updated Device Log from the CHF following the successful execution of an UpdateHANDeviceLog Service Request to Add a Device. The timeout period that the DCC Systems shall wait for the Alert is defined as "JoinTimePeriod" as specified within the Service Request plus a configurable network transmission time to allow delivery of the Alert over the SM WAN.

- a) If the CHF Device Log confirming communications have been established with the Device specified in the Service Request is received within the timeout period, then the DCC Systems shall notify the Responsible Supplier for the specified Device via a DCC Alert N24, and;
 - i. For ESME, GSME, HCALCS and PPMID the Device Status is set to 'InstalledNotCommissioned' in the Smart Metering Inventory; and
 - ii. The DCC Systems shall initiate a Command to the Device using each available Device Certificate to determine which Device Certificate is

currently in use by the Device. If the DCC receives a Response to a Command using a particular Device Certificate, then the DCC Systems are updated to record this Device Certificate as currently in use by the Device.

- b) If the CHF Device Log confirming communications have been established with the Device specified in the Service Request is not received within the timeout period, then the DCC Systems informs the User via a DCC Alert N25.

When a User requests the Request Type “Add” variant of this Service Request 8.11, then an unsuccessful Command Response indicates that the CHF did not execute the Command, the details provided in the Service Request have NOT been successfully added to the CHF Device Log and no further actions are triggered by the DCC Systems.

When a User requests the Request Type “Remove” variant of this Service Request 8.11, then the Command Response indicates whether the specified Device provided in the Service Request was either successfully removed from the CHF Device Log or the removal was unsuccessful. Upon receipt of a successful Response resulting from the UpdateHANDeviceLog Service Request to Remove a Device, the DCC shall, where the Device Status is currently ‘Whitelisted’, set the Device status to ‘Pending’. No additional DCC Alerts are produced by the DCC Systems.

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
<u>BFD15</u>	<u>Device Certificate realignment</u>	<u>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.</u>	<u>Device Certificate realignment UC CertificateAlign 001</u>	<u>Conditional. Access shall be granted to the Responsible Supplier.</u>

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	-