

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.

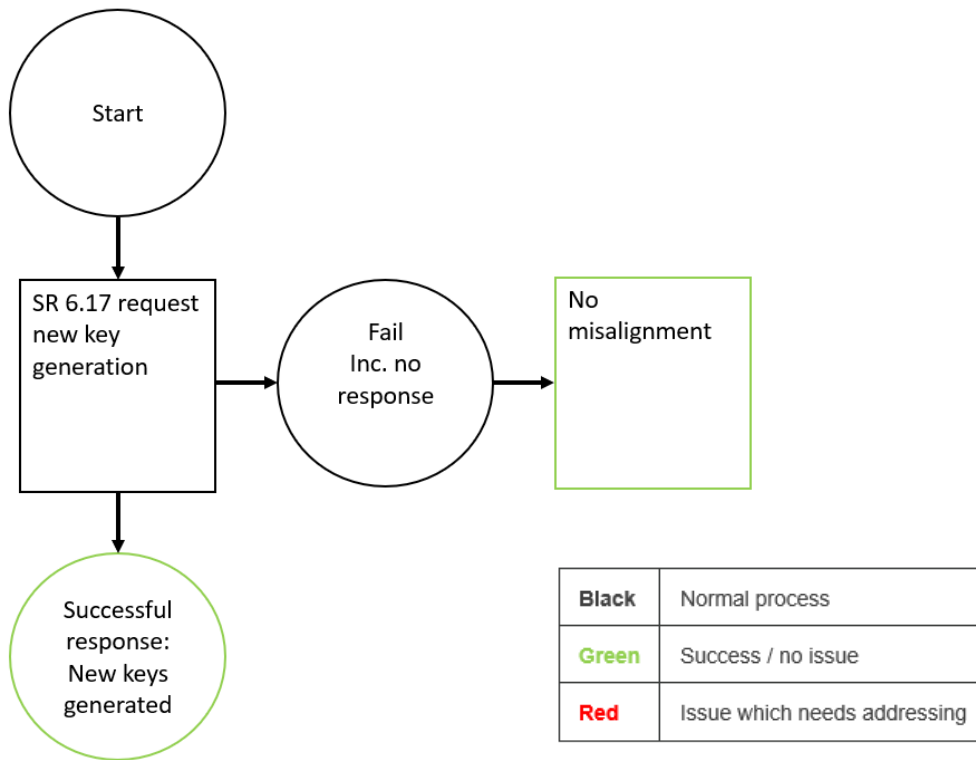
There are some Devices that become non-communicable after this process. Root cause analysis has identified that due to the reasons above, the Device Certificate (Device Signature (DS) or Key Agreement Key (KAK)) is misaligned with what is held within the DSP Master Key Store.

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.

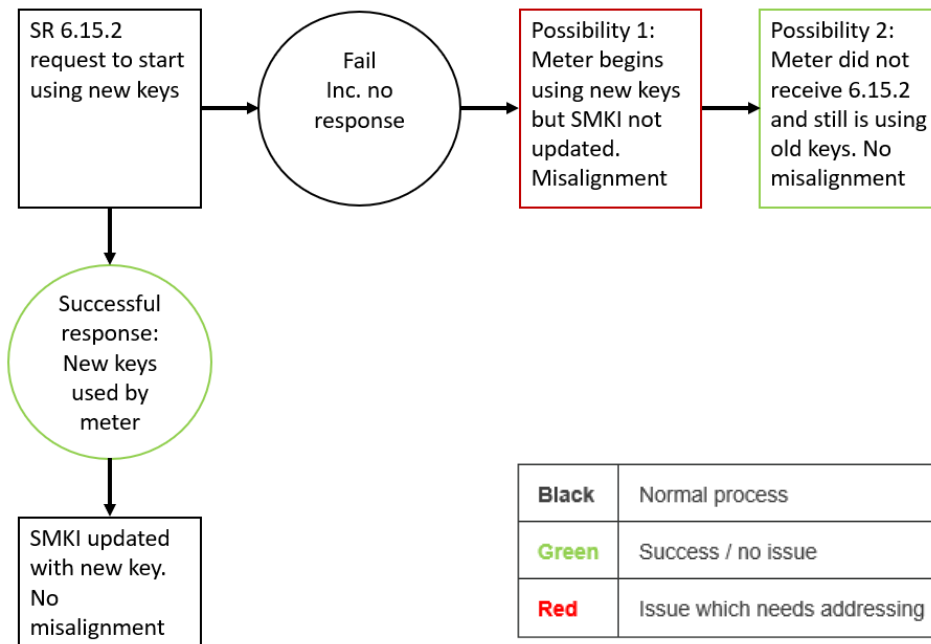
Suppliers have indicated they would like an enduring solution to resolve the Device Certificate misalignment issue without involving a manual SMI update.

The below diagrams set out the current process and issues:

Starting point when Supplier request for new key:



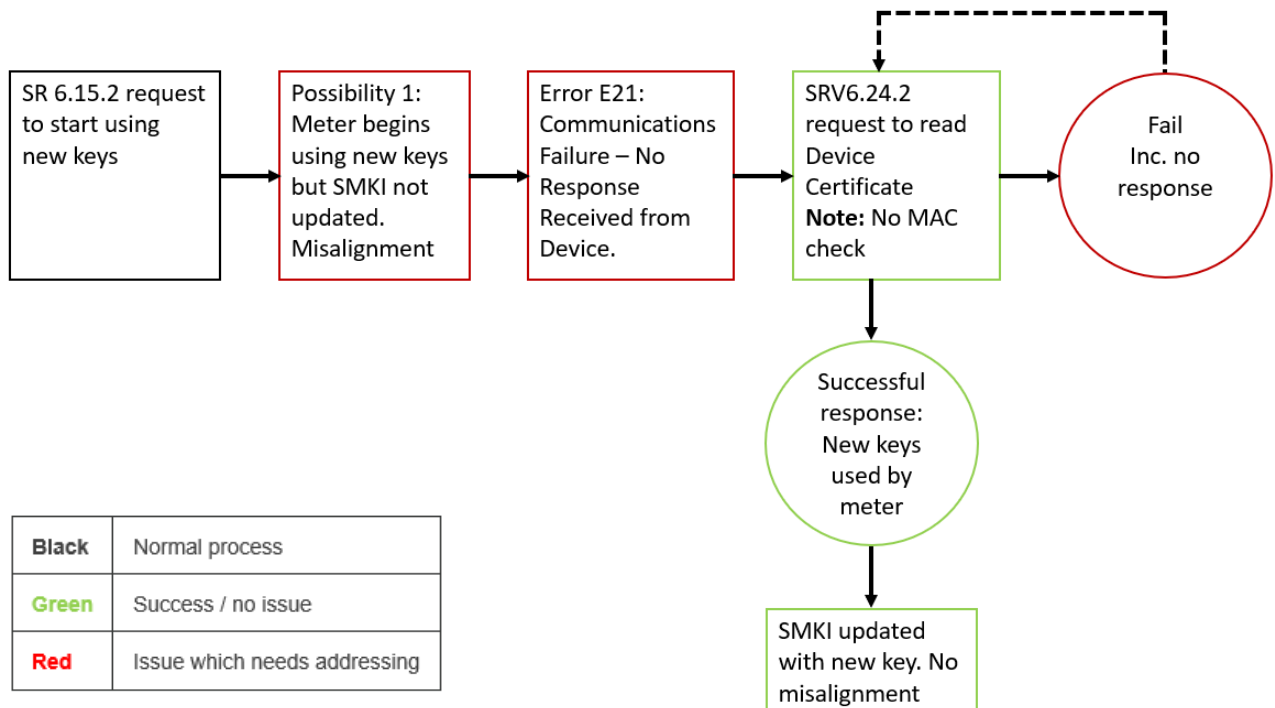
Issue when Supplier tries to use new keys:



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