

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.



MP268

‘Certificate rotation and expired Certificates’

Modification Report

Version 0.5

18 September 2024



About this document

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

Contents

1.	Summary	3
2.	Issue	3
3.	Solution	5
4.	Impacts	5
5.	Costs	7
6.	Implementation approach	8
7.	Assessment of the proposal	8
8.	Case for change	11
	Appendix 1: Progression timetable	12
	Appendix 2: Glossary	13

This document also has four annexes:

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

Contact

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

Mohammedanwar Sumro

020 2924 4506

mohammedanwar.sumro@gemserv.com

1. Summary

This proposal has been raised by Bradley Baker from the DCC.

Manufacturers use default Certificates, obtained from the DCC, to place on their Devices before the Device is installed. This enables the secure communication between the DCC and the Device during the Installation and Commissioning (I&C) process. The SEC specifies a post-commissioning obligation to replace the default Certificate information with the Device's Supplier Certificate and Network Operator Certificate.

The Organisation Certificates contained within the first (and current) manufacturing pack will expire in 2026. [MP261 'Extending the Organisation Certificate Validity Period'](#) was raised to allow the DCC to align the new Organisation Certificate with the existing Issuing Organisation Certification Authority (OCA) Certificate which has a Validity Period of 25 years and is set to expire in 2041 to prevent further manufacturing packs being created prematurely. MP261 was implemented on 29 February 2024.

Once the new manufacturing pack is made available by DCC, there will be Devices installed and commissioned that contain information from an Organisation Certificate that has a Validity Period of more than ten years. The SEC is implicit in its instruction to replace the Certificate information in the Trust Anchor Cells.

Furthermore, from 2026, there will be Devices installed that may have an expired or revoked Certificate in the Device Trust Anchor cell (due to them containing the original manufacturing pack Certificates). There is no explicit requirement in the SEC to specify the duties on the DCC and Users when a Certificate on a Device has expired or been revoked.

The solution involves developing clear guidelines within the SEC mandating post-commissioning replacement of Organisation Certificates by the DCC. These guidelines will provide explicit instructions and timelines for replacing any Organisation Certificate which has a Validity Period longer than ten years, or is revoked or expired. The costs for implementing this modification is between £10,000 - £160,000 and it is targeted to be implemented as part of the November 2025 SEC Release.

2. Issue

What are the current arrangements?

What is an Organisation Certificate and what is it used for?

For security reasons, Devices on the Smart Metering network should only be able to communicate with Parties that have the right to do so. To do this, each Device relies on Certificates placed onto the Trust Anchor Cells on the Device. There are multiple Trust Anchor Cells to reflect that Devices need to communicate with Suppliers, Network Operators, Registered Supplier Agents (RSAs) and the DCC. Those Parties will have their own Organisation Certificates that will match those held on the Device to ensure that only those Parties can communicate with the Device.

Why are default Certificates used and how long are they valid for?

The DCC issues a list of Certificates to Device Manufacturers for them to place into the Trust Anchor Cells on their Devices. This is known as the manufacturing pack. This ensures that those Devices can be initially communicated with during Install and Commission (I&C).

When a Device is installed, it will have Certificate information that assists in the I&C process. This is so that when the Devices are installed the relevant Service Reference Variants (SRVs) can be sent to the responsible Parties.

Devices which have the Organisation Certificates installed by the Supplier are then replaced with the Suppliers' own Certificates. SEC Appendix B 'Organisation Certificate Policy' currently specifies the Validity Period of each Organisation Certificate must be ten years, or in circumstances approved by the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) (having taken into account the views of the Security Sub-Committee) (SSC).

[MP261 'Extending the Organisation Certificate Validity Period'](#) was implemented as part of the February 2024 SEC Release. It allows the DCC to create the new manufacturing pack with Organisation Certificates that have a Validity Period of more than ten years. This is provided the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) approves the duration.

The DCC will issue a new manufacturing pack which is expected in the fourth quarter of 2024. No further manufacturing packs would be issued until required by either the Issuing Certification Authority or because of any risks posed by Quantum Computing and other future technological advances.

What is the issue?

Devices manufactured after the 2024 manufacturing pack release may contain information from an Organisation Certificate with a Validity Period exceeding ten years. The SMKI PMA approved the MP261 Proposed Solution to allow for an extended Validity Period on the basis the information from that Organisation Certificate is replaced as soon as reasonably practicable following the I&C process. The information will be replaced with that of a Certificate with a ten-year Validity Period. This has been specified by the SMKI-PMA.

Furthermore, the DCC advises that there is no explicit SEC requirement for post-commissioning replacement of Organisation Certificate information by the DCC. It is also expected that Devices will continue to be installed in 2026 and beyond that contain Organisation Certificates from the original manufacturing pack. This means that Devices will be installed containing expired Organisation Certificates.

What is the impact this is having?

The SMKI PMA has advised that Certificates that have a Validity Period of more than ten years pose a greater security risk, and as such should be replaced with the Supplier, Network Party, and any other relevant Party's own Certificates as soon as reasonably practicable following I&C.

Furthermore, Devices containing Certificates from the current manufacturing pack may be installed after the Validity Period has expired in 2026. As such, these will also need to be replaced following I&C with valid Certificates.

Impact on consumers

Without any explicit obligations for post-commissioning replacement of Organisation Certificates, it leaves consumers with increased an security risk of credentials being comprised following the implementation of extended Certificate lifetimes.

3. Solution

Proposed Solution

The Proposed Solution aims to address the security risks associated with using Organisation Certificates with extended Validity Periods in Devices installed after the 2024 manufacturing pack release.

The solution involves developing clear guidelines within the SEC mandating post-commissioning replacement of Organisation Certificates by the DCC. These guidelines will provide explicit instructions and timelines for replacing any Organisation Certificate which has a Validity Period longer than ten years, or is revoked or expired. This is to ensure, ongoing network security and compliance. Additionally, monitoring mechanisms will be established to ensure compliance with SEC guidelines and stakeholder collaboration will be key in communicating and enforcing the new guidelines effectively.

The business requirements supporting this solution are detailed in annex A, providing further clarity and justification for the Proposed Solution.

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

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
✓	Device Manufacturers		Flexibility Providers
	DCC Other Users		MAPs/ MAMs

All SEC Parties highlighted above are impacted by the need to update their systems and processes to manage and replace Device Certificates, ensuring continued compliance and secure communication within the smart metering network.

DCC Systems

DCC System changes

As per the DCC Preliminary Assessment, the Data Service Provider (DSP) will create an automation initiation of Access Control Broker (ACB) Organisation Certificate replacement as a daily task. This automation will prioritise Devices commissioned within the last 48 hours. Certificate replacements which fail will be retried every seven days, with a maximum of three attempts. A mechanism will be in place to address backlogged Devices if capacity allows. Prepayment Interface Devices (PPMID) will be excluded from automatic ACB Organisation Certificate replacement due to known limitations.

Data management elements are enhanced to identify Devices with:

- Certificates exceeding a ten-year Validity Period
- Revoked and expired Certificates
- Certificates nearing expiration within 18 months
- Incorrect Trust Anchor Cell Certificate placements

Reports will be formed by the following data attributes:

- Global Unique Identifier
- Device ID
- Device type
- Operational status
- Key location
- Key type
- Manufacturer Certificate status
- Certificate expiration date

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

DCC System traffic

The Preliminary Assessment response notes no impacts to the DCC System traffic.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section G 'Security'
- Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

The changes to the SEC required to deliver the proposed solution can be found in Annex B.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
✓	Communications Hubs		Gas Proxy Functions
	In-Home Displays	✓	Home Area Network Connected Auxiliary Load Control Switches

Consumers

Although consumers are not directly impacted by the implementation of this modification, having a proactive approach to replace Certificates mitigates the risk of unauthorised access to Smart Meters, protecting consumer data and privacy.

Other industry Codes

This modification will have no impact on other industry Codes.

Greenhouse gas emissions

This modification will have no impact on greenhouse gas emissions.

5. Costs

DCC costs

The estimated DCC implementation costs to implement this modification is £10,000 to £160,000. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design, Build and Pre-Integration Testing (PIT)	£10,000 – 160,000
Systems Integration Testing (SIT)	TBC
User Integration Testing (UIT)	TBC
Implement to Live	TBC
Application Support	TBC

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

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

One Refinement Consultation respondent (Network Party) highlighted that it anticipates an estimated amount of under £100,000 of costs incurred by the implementation of this modification. This is due to the Network Party replacing and apply new Certificates.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **6 November 2025** (November 2025 SEC Release) if a decision to approve is received on or before 22 July 2025 or

Ad-Hoc SEC Release 10 Working Days following a decision to approve is received after 22 July 2025.

This modification is aiming to be implemented at latest, in November 2025. This is so the Proposed Solution can be effective. This is the last SEC Release potentially featuring DCC System changes before the original Certificates expire.

7. Assessment of the proposal

Areas for assessment

Why is this modification needed?

MP261 was required to allow the DCC to create Organisation Certificates for more than 10 years, where it is agreed by the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), having first considered the views of the Security Sub-Committee (SSC). It will also allow the DCC to re-use the existing Public Key information.

The DCC were then required to carry out testing on the new manufacturing pack by SMKI PMA and the Department of Energy Security and Net Zero (DESNZ). The DCC determined that capturing the post-commissioning obligations within [MP261 'Extending the Organisation Certificate Validity Period'](#) could potentially have delayed the progression of the modification which would have prevented the DCC from commencing testing of the new manufacturing pack.

Consumer risk mitigation

With the incoming Organisation Certificate set to expire in 2041 there is heightened risk to consumers. Unauthorised access to Certificate information could lead to malicious activities negatively impacting consumers.

Observations on the issue

Views from the Working Group

A Large Supplier supported this modification and agreed that there is a lack of explicit instruction to replace Certificates. Another Large Supplier recommended that ACB and Wide Area Network (WAN) provider Organisation Certificates replacement should not impact I&C and that Certificate replacement should take place after seven days.

A Working Group member queried what would happen if Devices which have successfully been installed and commissioned were to not undergo Organisation Certificate replacement. The DCC highlighted that there are difficulties in replacing Certificates on PPMIDs and that the legal text addresses this. The DCC are sourcing information as to the repercussions of what would happen if a Certificate replacement was not to take place following I&C.

Working Group members agreed that the business requirements and the legal text deliver the Proposed Solution. Working Group members agreed that a Full Impact Assessment should be requested.

Views from the TABASC

The Technical Architecture and Business Architecture Sub Committee (TABASC) support this modification however challenged the idea that Certificate replacement should take place seven days after I&C. Members agreed that it would be better to align the time periods for post commissioning obligations. TABASC agreed that 48 hours should be the minimum time available for a Supplier to replace the Certificates and that seven days may be a more appropriate maximum time frame following the I&C.

Views from the SMKI PMA

SMKI PMA support the modification and believes that this modification will mitigate risks by creating a requirement in the SEC for Certificate rotation. A member noted that any reporting requirements must be confirmed by the SMKI PMA. The DCC have worked with the Chair of the SMKI PMA to create the reporting requirements.

Views from the SSC

The Security Sub-Committee (SSC) remained neutral in terms of support of this modification. A discussion between the SSC Chair, TABASC Chair and the DCC took place where all agreed that the initial time frame of Certificate replacement of a minimum of seven days and before a maximum of 21 days following I&C is a risk which can be reduced. The SSC Chair agreed that Suppliers can and

should replace the Certificates after a minimum of 48 hours and a maximum of seven days following I&C

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the TABASC, SSC and the SMKI PMA to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	Review operational impacts and implications
SMKI PMA	Confirm suitability of post-commissioning obligations
SSC	Clarifying the guidelines and implementation approach – potentially carry out Risk Assessment against costs to implement
TABASC	To review system changes
TAG	No input required
PSC	No input required

Observations on the issue

A member of the Change Sub-Committee (CSC) questioned if this modification will only impact the DCC, as there are already obligations on Suppliers in relation to post-commissioning. SECAS confirmed that this only impacts the DCC and that DCC system impacting costs are to be expected.

Solution development

Timeframe of Certificate replacement

The TABASC and SSC Chairs, and the DCC, have agreed that it is more suitable to have Certificates replaced after a minimum of 48 hours and a maximum of seven days following I&C. The rationale for this is because the commissioning of a Device should be completed before an engineer leaves the premises. The TABASC Chair had stated a large proportion of post commissioning obligations take place on the same day and that it does not seem optimal to cater to the small proportion of situations where it is not the case. The SSC Chair stated Devices undergoing Certificate replacement further mitigates the risk of a security issue.

Exclusion of PPMIDs

When selecting Devices there will be an exclusions list based on Device Model details which will exclude certain categories of Devices from ACB Certificate replacement. The DCC have confirmed that a large proportion of PPMID Devices do not properly support the ACB Certificate replacement command and will fail the procedure therefore they are exempt from Certificate replacement.

8. Case for change

Business case

Approval of the modification

An Organisation Certificate with an extended Validity Period poses a security risk. By implementing clear guidelines mandating post-commissioning replacement of these certificates by the DCC, the risk is mitigated against unauthorised access. This modification has a proactive approach which invests in security measures to allow a reliable Smart Metering Network.

Views against the General SEC Objectives

Proposer's views

The Proposer believes this modification supports SEC Objective (f)¹ as the Proposed Solution mitigates data being compromised.

Industry views

All Refinement Consultation respondents believe that the Proposed Solution will effectively resolve the issue. Respondents noted that by developing clear guidelines within the SEC that this modification will reduce the risk of unauthorised access. However, one Party (Large Supplier) highlighted that the issue highlighted in this modification had been caused by the implementation of [MP261 'Extending the Organisation Certificate Validity Period'](#) which was also raised by the DCC.

Six Refinement Consultation respondents believe that this modification better facilitates General SEC Objective (f).

Views against the consumer areas

Improved safety and reliability

This modification improves the safety and reliability of Devices on the Smart Metering network by ensuring that Organisation Certificates which have an expiry of more than ten years is updated to one which is equal to ten years, reducing the risk of unauthorised access.

Lower bills than would otherwise be the case

This modification does not lower bills.

Reduced environmental damage

This modification does not impact environmental damage.

¹ to ensure the protection of Data and the security of Data and Systems in the operation of this Code

Improved quality of service

This modification does not impact the quality of service.

Benefits for society as a whole

This modification does not impact society as a whole.

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	13 Feb 2024
Presented to CSC for initial comment	20 Feb 2024
CSC converts Draft Proposal to Modification Proposal	20 Feb 2024
Business requirements developed with Proposer and DCC	21 Feb 2024 – 26 Feb 2024
Business requirements workshop	4 Mar 2024
Modification discussed with Working Group	6 Mar 2024
Modification discussed with SSC	13 Mar 2024
Modification discussed with SMKI PMA	13 Mar 2024
Modification discussed with TABASC	2 May 2024
Preliminary Assessment requested	2 Jul 2024
Preliminary Assessment returned	24 Jul 2024
Modification discussed with Working Group	7 Aug 2024
Refinement Consultation	14 Aug 2024 – 5 Sep 2024
<i>Impact Assessment costs approved by Change Board</i>	<i>25 Sep 2024</i>
<i>Impact Assessment requested</i>	<i>25 Sep 2024</i>
<i>Impact Assessment returned</i>	<i>27 Nov 2024</i>
<i>Modification discussed with Working Group</i>	<i>11 Dec 2024</i>
<i>Modification Report approved by CSC</i>	<i>24 Dec 2024</i>
<i>Modification Report Consultation</i>	<i>24 Dec 2024 – 16 Jan 2025</i>
<i>Change Board Vote</i>	<i>21 Jan 2025</i>

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
DCC	Data Communications Company
DESNZ	Department of Energy Security and Net Zero
DSP	Data Service Provider
I&C	Install and Commission
OCA	Organisation Certificate Authority
OPSG	Operations Group
PIT	Pre-Integration Testing
PPMID	Prepayment Interface Device
PSC	Privacy Sub-Committee
RSA	Registered Supplier Agent
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	System Integration Testing
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SRV	Service Request Variant
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group
UIT	User Integration Testing
WAN	Wide Area Network