

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 1.1

20 December 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.

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	12
	Appendix 1: Progression timetable	14
	Appendix 2: Glossary	14

This document also has five 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) Impact Assessment response.
- **Annex D** contains the full responses received to the Refinement Consultation.
- **Annex E** contains the MP268 DCC Full End to End costs (including regression testing).

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 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 Proposed 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.

This modification will impact Suppliers and the DCC. The Proposed Solution implementation will cost £289,000. If approved, implementation is targeted for the November 2025 SEC Release. This modification will be progressed as a Self-Governance Modification.

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 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 installed by the Supplier which have the original Organisation Certificates 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 longer if approved by the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) and 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 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 solution which allows for an extended Validity Period beyond 10 years, on the basis the information from that Organisation Certificate is replaced as soon as reasonably practicable, following the I&C process

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 could pose a slightly increased 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

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 and interoperability of Devices, which may negatively impact consumers.

3. Solution

Proposed Solution

The Proposed Solution will provide 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. An automatic replacement of Manufacturer Access Control Broker (ACB) Organisation Certificates will be amended in order to meet these new obligations. This will address the security risks associated with using Organisation Certificates with extended Validity Periods in Devices installed after the 2024 manufacturing pack release. 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 for the solution can be found in Annex A.

The full redlined changes to the SEC required to deliver the Proposed Solution are in Annex B.

Full details of the Proposed Solution can be found in the DCC's Impact Assessment in Annex C.

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

All Suppliers, Electricity Network Operators and the DCC, 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

The Data Service Provider (DSP) will create an automation initiation of 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 Impact Assessment response in Annex C.

DCC System traffic

The DCC Impact Assessment response notes no impacts to the DCC System traffic. Additional processing and storage are likely to be required. However, they are not sufficiently large enough to warrant the procurement of additional compute power or storage.

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

The selected Devices are impacted as they have ACB Organisation Certificates in their Trust Anchor Cells.

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 DCC implementation costs to implement this modification is £289,000

The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design, Build and Pre-Integration Testing (PIT)	£204,500
integration Testing, Systems Integration Testing (SIT) and User Integration Testing (UIT)	£62,357
Implement to Live	£15,976
Application Support	£6,167

More information can be found in the DCC Impact 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 6 February 2025; or
- **25 June 2026** (June 2026 SEC Release) if a decision to approve is received after 6 February 2025.

This modification is aiming to be implemented at latest, in November 2025, in order for 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 SMKI PMA, having first considered the views of the 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.

Devices will continue to be installed in 2026 and following years, that contain Organisation Certificates from the original manufacturing pack. This means that Devices will be installed containing expired Organisation Certificates.

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 and interoperability of Devices, which may negatively impact consumers.

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the TABASC, SSC, SMKI PMA, Testing Advisory Group (TAG), and the Privacy Sub-Committee (PSC) 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	Post-PIT testing durations
PSC	No input required

Views from the CSC

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.

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. These recommendations were reflected in the changed requirements.

A Working Group member queried what would happen if Devices which have successfully been installed and commissioned were to not undergo Organisation Certificate replacement. If this Modification is not implemented, the lifetime of impacted assets will be limited to the lifetime of certificates which is Q2 2026. In addition, not rotating certificates proactively is a risk to both devices and security and may impact network capacity.

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.

The Working Group was presented with the DCC Impact Assessment. They queried if the Proposed Solution would target the Supplier Anchor Slot or replacing an expired ACB Certificates. They also queried if this would happen in the I&C phase. The DCC confirmed that the Proposed Solution is targeting the Trust Centre Swap Out (TCSO) and ACB Anchor Slots, and it can replace expired ACB Certificates, however the main goal is to prioritise expired, expiring or revoked Certificates.

The Working Group also had queries regarding the UIT duration, and if it can be reduced. The DCC noted the UIT length was derived from previous SEC Release related testing periods; however, the DCC has indicated there is no functional UIT testing required or recommended for this modification. They added that UIT for SEC Releases will be discussed with the TAG.

Views from the TABASC

The Technical Architecture and Business Architecture Sub Committee (TABASC) support this change 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.

Following the return of the DCC Impact Assessment, the TABASC challenged the need for MP268, stating that managing the DCC's estate is part of the DCC's License Conditions, and queried why a SEC Obligation is needed for the DCC to be able to replace the ACB Organisation Certificates. In addition, TABASC members noted they were not aware of the PPMID exclusions and wanted reasoning as to why they are out of scope. The DCC and SECAS noted they are in conversations with PPMID Device Manufacturers in regard to their exclusion. The TABASC concluded that they are not in support of the modification.

Views from the SMKI PMA

The SMKI PMA supported the change and believed that this change 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.

Following the return of the DCC Impact Assessment, the SMKI PMA members noted they do not see an issue with having a SEC obligation, however wanted to challenge the cost associated with this modification. They queried spending almost £300,000 for something which the DCC should already be doing, or which will be included in the new DSP. SMKI PMA members noted that Enduring Change of Supplier (ECoS) has this capability, and they are aware that the current DSP already does it for multiple certificates. SMKI PMA members also noted that they did not think the SMKI PMA should dictate to the DCC how they manage the DCC's risk appetite.

Views from the SSC

The 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

Following the return of the DCC Impact Assessment, the SSC queried why an explicit SEC Obligation is needed, as they are aware this was already being done by DCC. They added that ACB Organisation Certificates are currently being rotated, and the new DSP has this requirement to rotate the ACB Organisation Certificates. The SSC also noted that ACB Organisation Certificates rotation is a requirement within the new DSP, therefore do not see a need for this modification.

Views from the Proposer

The Proposer notes that exclusion of PPMIDs into the scope of this modification was confirmed by the DCC, due to a large proportion of PPMID Devices which do not properly support the ACB Certificate replacement command and will fail the procedure therefore they are exempt from Certificate replacement. While developing the business requirements, it was agreed that certificate rotation for PPMIDs be raised in a separate modification, due to the time constraints in getting MP268 to a decision and implemented before the new Manufacturing Pack goes live. The Proposer also noted the DSP performs manual and ad hoc ACB Certificate rotation, however there are no SEC Obligations to do so. In addition, there are no SEC Obligations nor mandate for the DCC to exchange expired Certificates apart from rotating WAN Provider credentials, which is managed by Communications Service Providers (CSPs). The Proposer also noted that there is a large backlog of Device Certificates (over 100,000 ACB Key Agreement, Digital Signature, and ECOS certificates every week) and the DCC are unable to use existing ad hoc measures to clear the backlog.

Discussions at CSC

At the December 2024 CSC, the DCC presented more detailed background information of what MP268 entails, highlighting that as of December 2024, there are over 16 million Devices still using

2016 ACB Certificates which will expire in 2026. The DCC also noted that they have not seen a huge amount of activity in upgrading legacy PPMIDs firmware versions and there are legacy Defects on PPMIDs around certificate rotation, which is why they are currently out of scope in MP268.

The TABASC Chair queried what was preventing the DCC from rotating the certificates currently and added that they did not see a need for this change to be explicitly added to the SEC. The DCC noted there is nothing preventing them undertaking this activity; however, the certificate rotations are currently manual and are done on an ad hoc basis. They added that with MP268, this would bring in an automation element.

The TABASC Chair raised concerns on the total cost, including the SEC Release costs, specifically why industry is funding the DCC on this change, when it should be a requirement that the DCC should already be undertaking. The DCC noted they have a requirement around depleting TCOS estate, however there is no obligations regarding the number of days or any of the SSC Requirements for Post-Commissioning within ECOS.

The CSC Chair concluded that SECAS will facilitate discussions offline with the DCC, TABASC Chair and SSC Chair, and to progress the modification into the Report Phase in order not to miss the November 2025 SEC Release. They added that there would be an additional question included in the Modification Report Consultation on whether this change is already implicit in the SEC, and whether this needs to be explicit in the SEC. If the conclusions of the offline discussions are that this modification is needed, then this timetable must be adhered to in order to be included in the November 2025 SEC Release. This change would need to be included into the November 2025 SEC Release, as this is the last scheduled SEC Release before Devices installed and commissioned with the new manufacturing pack, may contain information from an Organisation Certificate that has a Validity Period of more than ten years.

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. However, the SEC Sub-Committees have questioned if this should be a modification with associated costs or if the DCC should be determining and implementing the security procedures. They have indicated that the DCC should bear the costs, leaving only a text change to be made to the SEC. If this modification is not implemented, then there will be no enduring obligations on the DCC licence holder nor on Parties to adhere to these protocols and timings.

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 will be neutral against this consumer benefit area.

Reduced environmental damage

This modification will be neutral against this consumer benefit area.

Improved quality of service

This modification will be neutral against this consumer benefit area.

Benefits for society as a whole

This modification will be neutral against this consumer benefit area.

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

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
Impact Assessment costs approved by Change Board	25 Sep 2024
Impact Assessment requested	25 Sep 2024
Impact Assessment returned	27 Nov 2024
Modification discussed with Working Group	4 Dec 2024
Modification discussed with TABASC	10 Dec 2024
Modification discussed with SSC	11 Dec 2024
Modification discussed with SMKI PMA	11 Dec 2024
Modification Report approved by CSC	17 Dec 2024
Modification Report Consultation	18 Dec 2024 – 13 Jan 2025
<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
CSC	Change Sub-Committee
CSP	Communications Service Provider
DCC	Data Communications Company

Glossary	
Acronym	Full term
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
TCSO	Trust Centre Swap Out
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.

MP268 ‘Certificate rotation and expired Certificates’

Annex A

Business requirements – version 0.6

About this document

This document contains the business requirements that support the solution 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	MoSCoW
1	Following Installation and Commission (I&C) completion (after 48 hours but before seven days have elapsed), the Change of Supplier (CoS) extended life Organisation Certificate (Transitional or Enduring) on that Device will under all reasonable steps be replaced	DCC	M
2	Following I&C completion (after 48 hours but before 23 days have elapsed), the “accessControlBroker” extended life Organisation Certificates on that Device will under all reasonable steps be replaced	DCC	M
3	Under all reasonable steps, the Relevant Subscriber will replace a Certificate before it expires, or has expired	Suppliers Network Parties DCC	M
4	Under all reasonable steps, the Relevant Subscriber will replace a revoked Certificate	Suppliers Network Parties DCC	M
5	Provide reporting capabilities to confirm Relevant Subscriber compliance with SEC Section G ‘Security’ and SEC Appendix AC ‘Inventory, Enrolment and Decommissioning Procedures’	DCC	C
6	The Relevant Subscriber’s User Independent Security Assurance Service Provider will provide security assurance services according to SEC Section G8.3(f) in relation to expired and revoked Certificates	Suppliers Network Parties DCC	M

Key

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

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)2 Devices.

The solution addresses Devices with Organisation Certificates which are required to be replaced.

The “recovery” Organisation Certificates falls outside the scope of this solution.

The ‘wanProvider’ Organisation Certificate falls outside the scope of this solution as there is an existing obligation for the WAN Provider to replace the WAN Certificate within seven days following I&C.

2.2 Requirement 1: Following Installation and Commission (I&C) completion (after 48 hours but before seven days have elapsed), the Change of Supplier (CoS) extended life Organisation Certificate (Transitional or Enduring) on that Device will under all reasonable steps be replaced

Once a Device has successfully undergone the I&C process, any existing “transitionalCoS” Certificates will promptly be replaced to ensure ongoing network security. This requirement aims to mitigate potential security risks associated with outdated or expired Certificates, focusing on Change of Supplier (CoS).

There are two different CoS Certificates which are presented to the DCC as part of the I&C. The “transitionalCoS” manufacturing Certificate which has a 10-year Validity Period which is set to expire in 2026. The other Certificate has a 17-year Validity Period being generated by the ECoS system. In any circumstance both Certificates must be replaced due to the DCC requiring to maintain capability to install Devices with the first manufacturing pack beyond 2026.

Please note there is an existing obligation for the WAN Provider to replace the WAN Certificate within seven days following I&C.

2.3 Requirement 2: Following I&C completion (after 48 hours but before 23 days have elapsed), the “accessControlBroker” Organisation Certificates on that Device will under all reasonable steps be replaced

Following Working Group, Security Sub-Committee (SSC), Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) and Technical Architecture and Business Architecture (TABASC) discussions, the Proposer has agreed that the Access Control Broker (ACB) Organisation Certificates are to be replaced after 48 hours but before 23 days following a Device's successful I&C. 48 hours also aligns with DCC's Service Providers (WAN Provider, CoS and ACB). For completeness, the 21-day period aligns with the DSP retry mechanism for ACB replacement if the Certificate replacement fails (it will be retried each day for the first seven days and then once a week for the next two weeks).

2.4 Requirement 3: Under all reasonable steps, the Relevant Subscriber will replace a Certificate before it expires, or has expired

When a Certificate's Validity Period is due to expire or is expired, the Subscriber will take all reasonable steps to change the Certificate. This should be a planned activity in order to manage capacity, for example a notification could be provided to the DCC.

An expired Certificate is a Certificate which has surpassed its Validity Period. This makes it unsuitable for secure communication and requires replacement with a new, valid Certificate to maintain network security. For a successful replacement of a Certificate the Relevant Subscriber should under all reasonable steps replace the Certificate prior to the Certificate expiring. Note that this is a proactive process.

2.5 Requirement 4: Under all reasonable steps, the Relevant Subscriber will replace a revoked Certificate

When a Certificate is revoked, the Relevant Subscriber will, under all reasonable steps, replace the Certificate. This ensures that the system remains secure.

A revoked Certificate is a Certificate which is no longer considered trustworthy for authentication of Devices and is deemed compromised. The SMKI PMA can approve the revocation of Organisation Certificates and request the DCC to do so. This may happen in circumstances where a Party exits the market or, has its licence revoked or a Supplier of Last Resort (SoLR) event occurs.

The revoked Certificate should be replaced with a new, valid Certificate to maintain network security. A revoked Certificate must be replaced with a new Certificate as soon as possible once deemed revoked. Note that the act of replacing a revoked Certificate is a reactive process.

2.6 Requirement 5: Provide reporting capabilities to confirm User compliance with SEC Section G 'Security' and SEC Appendix AC 'Inventory, Enrolment and Decommissioning Procedures'

This reporting expectation is subject to agreement with the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) and the Security Sub Committee (SSC).

This requirement mandates the provision of reporting capabilities to enable security assurance activities. Focusing on confirming User compliance with obligations outlined in the Smart Energy Code (SEC) Appendix AC 'Inventory, Enrolment and Decommissioning Procedures' section 5.2.

The reporting process will include, as a minimum:

- Devices holding any Certificates which have a Validity Period which exceeds ten years;
- Devices holding any revoked Certificates;
- Devices holding any expired Certificates;
- Devices holding any Certificates which will expire in 18 months on Devices (subject to change upon completion of the Preliminary Assessment); and
- Devices holding any Certificates in an incorrect Trust Anchor Cell.

DCC proposes that the reporting contains the following attributes:

- Global Unique Identifier (GUID);
- Device ID;

- Device Type;
- Device Operational Status;
- Key Location;
- Key Type;
- Certificate;
- Manufacturer Certificate (Y/N); and
- Certificate Expiration Date.

By identifying these sets of Devices, Parties can take timely actions to replace Certificates.

This additional reporting will be part of the existing monthly PCO report.

2.7 Requirement 6: The Relevant Subscriber's User Independent Security Assurance Service Provider will provide security assurance services according to SEC Section G8.3(f) in relation to expired and revoked Certificates

This requirement is in line with what is currently stated in the SEC, while widening the scope to include expired and revoked Certificates as per the Proposed Solution. This requirement is applicable to DCC Users.

3. 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
DSP	Data Service Provider
ECoS	Enduring Change of Supplier
I&C	Install and Commission
SEC	Smart Energy Code
SMETS	Smart Metering Equipment Technical Specifications
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SoLR	Supplier of Last Resort
SSC	Security Sub-Committee
WAN	Wireless 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.

MP268 ‘Certificate rotation and expired Certificates’

Annex B

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.

Section G 'Security'

These changes have been redlined against Section G version 23.0.

Amend Section G.8.3 as follows:

G8. USER SECURITY ASSURANCE

Scope of Security Assurance Services

G8.3 The security assurance services specified in this Section G8.3 are services in accordance with which the User Independent Security Assurance Service Provider shall:

- (a) carry out User Security Assessments at such times and in such manner as is provided for in this Section G8;
- (b) produce User Security Assessment Reports in relation to Users that have been the subject of a User Security Assessment;
- (c) receive and consider User Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;
- (d) otherwise, at the request of, and to an extent determined by, the Security Sub- Committee, carry out an assessment of the compliance of any User with its obligations under Sections G3 to G6 where:
 - (i) following either a User Security Self-Assessment or Verification User Security Assessment, any material increase in the security risk relating to that User has been identified; or
 - (ii) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;
- (e) review the outcome of User Security Self-Assessments;
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to:
 - (i) the compliance of any User with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan;
 - ~~(ii)~~ changes in security risks relating to the Systems, Data, functionality and processes of any User which fall within Section G5.14 (Information Security: Obligations on Users); and
 - ~~(ii)(iii)~~ the compliance of any User with obligations under SEC Appendix AC Section 5.22 and SEC Appendix AC Section 5.23;
- (g) at the request of the Panel, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

- (h) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
- (i) undertake such other activities, and do so at such times and in such manner, as may be further provided for in this Section G8.

Amend Section G9.2 as follows:

G9. DCC SECURITY ASSURANCE

Scope of Security Assessment Services

G9.2 The security assessment services specified in this Section G9.2 are services in accordance with which the DCC Independent Security Assessment Service Provider shall:

- (a) carry out DCC Security Assessments at such times and in such manner as is provided for in this Section G9;
- (b) produce DCC Security Assessment Reports in relation to the DCC that have been the subject of a DCC Security Assessment;
- (c) receive, consider and validate DCC Security Assessment Responses and carry out any Follow-up Security Assessments at the request of the Security Sub-Committee;
- (d) otherwise, at the request of, and to an extent determined by, the Security Sub Committee, carry out an assessment of the compliance of the DCC with its obligations under:
 - (i) Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
 - (ii) the requirements of Sections G2 and G4 to G6 or any CPA Certificate Remedial Plan; and where:
 - (iii) following either a DCC Security Assessment, any material increase in the security risk relating to the DCC has been identified; or
 - (iv) the Security Sub-Committee otherwise considers it appropriate for that assessment to be carried out;
- (e) at the request of the Security Sub-Committee, provide to it advice in relation to:
 - (i) the compliance of the DCC with its obligations under SEC Section G or any CPA Certificate Remedial Plan; ~~and~~
 - ~~(ii)~~ changes in security risks relating to the Systems, Data, functionality and processes of the DCC which fall within SEC Section G5 (Information Security: Obligations on the DCC); ~~and~~
 - ~~(ii)(iii)~~ the compliance of the DCC with the obligations under SEC Appendix AC Section 5.20 and SEC Appendix AC Section 5.21;
- (f) at the request of the Security Sub-Committee, provide to it advice in relation to the suitability of any remedial action plan for the purposes of Section M8.4 of the Code (Consequences of an Event of Default);

- (g) at the request of the Security Sub-Committee Chair, provide a representative to attend and contribute to the discussion at any meeting of the Security Sub-Committee; and
 - (i) undertake such other activities and do so at such times and in such manner, as may be further provided for in this Section G9;
 - (ii) assess the DCC's compliance with the requirements of Condition 8 (Security Controls for the Authorised Business) of the DCC Licence;
 - (iii) such other requirements relating to the security of the DCC Total System as may be specified by the Security Sub-Committee or the Panel from time to time.

Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

These changes have been redlined against Appendix AC version 7.0.

Add Section 5.20 to 5.23 as follows:

5. Post-Commissioning Obligations in relation to SMETS2+ Devices

General Obligations on DCC

- 5.18 The DCC shall monitor Responses it receives from Devices in order to determine whether any of the Device Certificates held on each Device have been successfully replaced. On the basis of this information the DCC shall establish and maintain a record of the most up-to-date active Device Certificates for each Device.
- 5.19 Where, following the addition of a Device to the Device Log of a Communications Hub Function, the DCC identifies that a Trust Anchor Cell of that Device has been populated with Security Credentials derived from a DCC CoS Certificate that has a subject field that is populated with an identifier of a DCC Service Provider that does not provide services to the CoS Party, the DCC shall send a DCC Alert to the Responsible Supplier for the Device, notifying them of the situation.

Certificate Validity Periods

- 5.20 As soon as reasonably practicable (and in any event after 48 hours but before 7 days have elapsed) following the Commissioning of any Device that has one or more Trust Anchor Cells that are populated with information from an Organisation Certificate with a Remote Party Role of "transitionalCoS" that has a Validity Period of more than 10 years, the DCC shall take all reasonable steps to replace that information with that from an Organisation Certificate with a Remote Party Role of "transitionalCoS" that has a Validity Period of 10 years.
- 5.21 As soon as reasonably practicable (and in any event after seven days but before 23 days have elapsed) following the Commissioning of any Device that has one or more Trust Anchor Cells that are populated with information from an Organisation Certificate with a Remote Party Role of "accessControlBroker" that has a Validity Period of more than 10 years, the DCC shall take all reasonable steps to replace that information with that from an Organisation Certificate with a Remote Party Role of "accessControlBroker" that has a Validity Period of 10 years.

Revoked and Expired Certificates

- 5.22 As soon as reasonably practicable:
- (a) following the revocation of a Certificate from which information is used (in part) to populate the Device Security Credentials of any Device that forms part of an installed Smart Metering System; or
 - (b) following the installation of a Device (as part of a Smart Metering System) that holds Device Security Credentials that are populated (in part) with information from a Certificate that has been revoked, the Subscriber for the relevant Certificate shall take all reasonable steps to replace the relevant information with that from a Certificate that has not been revoked.
- 5.23 As soon as reasonably practicable:

- (a) before the expiry of the Validity Period of a Certificate from which information is used (in part) to populate the Device Security Credentials of any Device that forms part of an installed Smart Metering System; or
- (b) following the Commissioning of a Device (as part of a Smart Metering System) that holds Device Security Credentials that are populated (in part) with information from a Certificate that has a Validity Period that has expired, the Subscriber for that relevant Certificate shall take all reasonable steps to replace the relevant information with that from a Certificate that has a Validity Period that has not expired.

SEC Modification Proposal, SECMP0268, DCC CR5407

Certificate Rotation Post Commissioning Full Impact Assessment (FIA)

Version:	0.2
Date:	22nd November 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	DSP Technical Solution	9
4.2	Application Components	10
4.2.1	Technical Specifications	10
4.2.2	Key Management	10
4.2.3	Data Management.....	10
4.2.4	Infrastructure Impact.....	10
4.2.5	Other DSP Changes.....	10
4.3	Impacts on ECOS Provider (Accenture).....	11
4.4	Data Science and Analytics Team	11
5	Implementation Timescales and Approach.....	12
5.1	DSP Pre-Integration Testing.....	12
5.2	System Integration Testing (SIT)	12
5.3	User Integration Testing (UIT)	13
5.4	Changes to DS&A Reporting.....	13
5.5	Transition to Operations.....	13
6	Costs and Charges.....	14
6.1	Changes to the Agreement.....	15
	Appendix A: Glossary	16

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement SECMP0268 Certificate Rotation and Expired Certificates Post Commissioning of **£289,000**, which comprises:
 - £204,500 in Design, Build, and Pre-Integration Testing (PIT)
 - £84,500 in Implementation, including integration testing and deployment
- Expected effort of nine months to complete with a target release of November 2025.

Problem Statement

Currently the obligations to rotate Access Control Broker (ACB) and Enduring Change of Supplier (ECOS) certificates are not formalised in the SEC. Manufacturing certificates are not trusted credentials and require the replacement of older certificates with newer versions, a process referred to as *certificate rotation*. There are currently no requirements for ACB rotation, but this has been managed informally with the Data Service Provider (DSP). The current ECOS migration is about to complete, meaning there is no method of rotating certificates after migration for new install and commissions.

If this Modification is not implemented, the lifetime of impacted assets will be limited to the lifetime of certificates which is Q2 2026. In addition, not rotating certificates proactively is a risk to both devices and security, and may impact network capacity.

Devices will continue to be installed in 2026 and following years that contain Organisation Certificates from the original manufacturing pack. This means that Devices will be installed containing expired Organisation Certificates.

Modification Benefits

This Modification mandates post commissioning obligations on Service Providers for the ACB and ECOS roles, will reduce the risks for DCC operational functions, and will increase the speed of response to certificate rotation in the case of a compromise. Without any obligations for post-commissioning replacement of Organisation Certificates, it leaves consumers with increased security risk of credentials being compromised following the implementation of extended Certificate lifetimes.

Currently the DSP replaces ACB certificates on devices when “convenient” with respect to other operational considerations. This Modification mandates replacement between two (2) and 23 days after the commissioning of a device. For the ECOS solution, a new configuration will ensure devices holding TCOS or ECOS certificates at the time of install are rotated by the ECOS solution.

This Modification mandates post commissioning obligations on Service Providers for the ACB and ECOS roles, will reduce the risks for DCC operational functions, and will increase the speed of response to certificate rotation in the case of a compromise.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
12/11/2024	0.1	Initial version, for DCC internal review
22/11/2024	0.2	Post review, approved costs

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	DP268 Modification Report v0.1	SECAS	02/07/2024
2.	MP268 business requirements v0.6	SECAS	12/11/2024
3	SECMP0268 CR5170 - PIA - Certificate Rotation and Expired Certificates v0.21	DCC	28/08/2024

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Bradley Baker from the Data Communications Company (DCC).

The Preliminary Impact Assessment (PIA) was requested of DCC on 4th July, 2024. and submitted on the 24th July.

The FIA was requested on 30th September 2024.

The technical solution for this Modification has been referred to as “Post Commissioning Obligation on Access Control Broker (ACB) and Enduring Change of Supplier (ECOS) Providers”, and “Certificate Rotation and Expired Certificates “, but the Modification title has been updated for accuracy.

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, and have been validated by SSC and TABASC.

This solution will be applied to Smart Metering Equipment Technical Specifications (SMETS)2 Devices. It addresses Devices with Organisation Certificates which are required to be replaced.

The “recovery” Organisation Certificates falls outside the scope of this solution.

The ‘wanProvider’ Organisation Certificate falls outside the scope of this solution as there is an existing obligation for the WAN Provider to replace the WAN Certificate within seven days following the Installation and Commission (I&C) process.

3.1 Current Arrangements

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 I&C process. The Smart Energy Code (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. SECMP0261 ‘Extending the Organisation Certificate Validity Period’ was implemented in February 2024, and allows the DCC to align the new Organisation Certificate with the existing Issuing Organisation Certification Authority (OCA) Certificate which has a Validity Period of 17 years and is set to expire in 2041 to prevent a new manufacturing pack being created prematurely. Once the 2024 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. However, there is no explicit requirement in the SEC specifying the post-commissioning replacement of the Organisation Certificate information, for which the DCC is responsible. 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). Currently 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.

3.2 What is the Issue?

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 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 Service Reference Variants (SRVs) can be sent to and received from the responsible Parties.

Devices which have the Organisation Certificates installed by the Supplier, are then replaced with the Supplier’s own Certificates. The SEC Appendix B ‘Organisation Certificate Policy’ currently specifies the Validity Period of each Organisation Certificate must be ten years. As such, the expiry date for the current Organisation Certificates within the first and current manufacturing pack is 2026.

The DCC will issue a new manufacturing pack, expected in April 2025. No further manufacturing packs would be issued, until required by either the Issuing Certification Authority or because of any risks posed by Quantum Computing or other future technological advances.

3.3 Impact of 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 SECMP261 solution to allow for an extended Validity Period, provided that the information from that Organisation Certificate is replaced as soon as reasonably practicable following I&C. The information will be replaced with that of a Certificate with a ten-year Validity Period.

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 following years that contain Organisation Certificates from the original manufacturing pack. This means that Devices will be installed containing expired Organisation Certificates.

This Modification mandates post commissioning obligations on Service Providers for the ACB and ECOS roles, will reduce the risks for DCC operational functions, and will increase the speed of response to certificate rotation in the case of a compromise. Without any obligations for post-commissioning replacement of Organisation Certificates, it leaves consumers with increased security risk of credentials being compromised following the implementation of extended Certificate lifetimes.

3.4 Business Requirements

The business requirements are as follows.

Ref	Requirement	MOSCOW
1	Following I&C completion (after 48 hours but before seven days have elapsed), the Change of Supplier (CoS) extended life Organisation Certificate (Transitional or Enduring) on that Device will, under all reasonable steps, be replaced	Must
2	Following I&C completion (after 48 hours but before 23 days have elapsed), the “accessControlBroker” extended life Organisation Certificates on that Device will under all reasonable steps be replaced.	Must
3	Under all reasonable steps, the Relevant Subscriber will replace a Certificate before it expires, or has expired	Must
4	Under all reasonable steps, the Relevant Subscriber will replace a revoked Certificate	Must
5	Provide reporting capabilities to confirm Relevant Subscriber compliance with SEC Section G ‘Security’ and SEC Appendix AC ‘Inventory, Enrolment and Decommissioning Procedures’	Could
6	The Relevant Subscriber’s User Independent Security Assurance Service Provider will provide security assurance services according to SEC Section G8.3(f) in relation to expired and revoked Certificates	Must

Requirement 1: Once a Device has successfully undergone the I&C process, any existing “transitionalCoS” (TCOS) certificates will promptly be replaced to ensure ongoing network security. This requirement aims to mitigate potential security risks associated with outdated or expired Certificates, focusing on Change of Supplier (CoS).

There are two different and separate CoS Certificates presented to the DCC as part of the I&C:

- The “transitionalCoS” manufacturing Certificate which has a 10-year Validity Period set to expire in 2026.
- The other Certificate has a 17-year Validity Period being generated by the ECOS system.

In any circumstance both Certificates must be replaced due to the DCC being required to maintain capability to install Devices with the first manufacturing pack beyond 2026.

Note there is an existing obligation for the WAN Provider to replace the WAN Certificate within seven days following I&C.

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 2: Following Working Group discussions and engagement with a Large Supplier Party, the Proposer has agreed that ACB Organisation Certificates are to be replaced between after 48 hours but before 23 days after a successful device’s I&C has completed. The Large Supplier highlighted concern that Device key cycling should not be attempted during the I&C activity, as it can result in an install and leave scenario, or Device exchange in the worst cases. Replacing ACB Organisation Certificates seven days post-I&C will mean that it does not conflict or interfere with Device key cycling that Suppliers have an obligation to complete, within the first seven days after I&C.

For completeness, the 21-day period after I&C aligns with the DSP retry mechanism for ACB replacement if the Certificate replacement fails (it will be retried each day for the first seven days and then once a week for the next two weeks).

Requirement 3: When a Certificate’s Validity Period is due to expire or is expired, the Subscriber will take all reasonable steps to change the Certificate. This should be a planned activity to manage capacity, for example a notification could be provided to the DCC.

An expired Certificate is a Certificate which has surpassed its Validity Period. This makes it unsuitable for secure communication and requires replacement with a new, valid Certificate to maintain network security. For a successful replacement of a Certificate the Relevant

Subscriber should under all reasonable steps replace the Certificate prior to the Certificate expiring. Note that this a proactive process.

Requirement 4: When a Certificate is revoked, the Relevant Subscriber will, under all reasonable steps, replace the Certificate. This ensures that the system remains secure. A revoked Certificate is a Certificate which is no longer considered trustworthy for authentication of Devices and is deemed compromised. The SMKI PMA can approve the revocation of Organisation Certificates and request the DCC to do so. This may happen in circumstances where a Party exits the market or, has its licence revoked or a Supplier of Last Resort (SoLR) event occurs.

The revoked Certificate should be replaced with a new, valid Certificate to maintain network security. A revoked Certificate must be replaced with a new Certificate as soon as possible once deemed revoked. Note that the act of replacing a revoked Certificate is a reactive process.

Requirement 5: The reporting has been agreed with the SMKI PMA and the Security Sub Committee (SSC), and mandates the provision of reporting capabilities to enable security assurance activities while focusing on confirming User compliance with obligations outlined in SEC Appendix AC 'Inventory, Enrolment and Decommissioning Procedures' section 5.2.

The reporting process will include, as a minimum, devices holding:

- any Certificates which have a Validity Period which exceeds ten years;
- any revoked Certificates;
- any expired Certificates;
- any Certificates which will expire in 18 months on Devices (subject to change upon completion of the Preliminary Assessment); and
- any Certificates in an incorrect Trust Anchor Cell.

DCC proposes that the reporting contains the following attributes:

- Global Unique Identifier (GUID);
- Device ID
- Device Type;
- Device Operational Status;
- Key Location;
- Key Type;
- Certificate;
- Manufacturer Certificate (Y/N); and
- Certificate Expiration Date

By identifying these sets of Devices, Parties can take timely actions to replace Certificates. This additional reporting will be part of the existing monthly Post Commissioning Obligations (PCO) report.

Requirement 6: This requirement is in line with what is currently stated in the SEC, while widening the scope to include expired and revoked Certificates as per the Proposed Solution. This requirement is applicable to DCC Users.

4 Description of Solution

The automatic replacement of manufacturer ACB certificates will be amended in order to meet new obligations.

4.1 DSP Technical Solution

The DSP solution already provides a capability to rotate ACB certificates on devices. This capability has been used successfully to move a large proportion of the device estate away from manufacturing ACB certificates to operational (Business as Usual) ACB certificates.

The DSP solution will be updated for this Modification to include the following features:

- setting ACB certificate replacement as a regular daily task
- selection of devices which currently hold a manufacturing ACB certificate for which 48 hours has passed since the device became commissioned;
- replacement of the manufacturing ACB certificate on these devices with a specified operational ACB certificate; and
- if unsuccessful, continuing attempts at ACB certificate replacement every seven calendar days for up to three re-attempts (21 calendar days).

The solution shall be configurable through a set of parameters as follows:

- initial rotation delay period following commissioning (set to 48 hours);
- rotation retry period following initial attempt (set to 7 calendar days);
- maximum retry attempts (set to 3 retries); and
- maximum ACB rotations per day (a default value will be agreed between the Parties as part of the design stage).

In order to cope with the backlog of already commissioned devices which still retain manufacturing ACB certificates, the solution will also include the following features:

- when selecting devices, priority will be given to devices that have been commissioned within the last 23 calendar days (i.e. any newly commissioned devices will be picked up first and the backlog will only be addressed if there is further capacity before reaching the configured daily limit)
- when selecting devices there will be an “exclusion list” based on Device Model details which will exclude certain categories of device from ACB certificate replacement

The “exclusion list” is a feature of the existing ACB certificate replacement capability, and was introduced to deal with the large proportion of PPMID devices do not properly support the ACB certificate replacement command and will always fail¹.

¹ Many legacy firmware versions of PPMIDs do not support certificate rotation. In addition there are a large number of PPMIDs not supported by SECMP0007

4.2 Application Components

The DSP solution described above will require changes to the Key Management System and Data Management components.

4.2.1 Technical Specifications

There are no changes required to any SEC Technical Specifications – GBCS, DUIS, DUGIDS, or Message Mapping Catalogue (MMC).

4.2.2 Key Management

Data Management will be called periodically (e.g. every 15 minutes between 8am and 10pm), passing in a list of manufacturer ACB certificates.

4.2.3 Data Management

To limit the worklist size to a configurable value, Devices will be selected, and added to the replacement worklist which:

- have one of the manufacturer certificates
- have been commissioned between 48 hours and 23 calendar days ago
- are not marked as excluded

If there is still capacity (N) then, using current functionality, a further selected N devices will be selected and added to the replacement worklist which:

- have one of the manufacturer certificates;
- have not had a device status change in the last 7 calendar days; and
- are not marked as excluded.

Note that the functionality in the DCC Total System (DSP) already includes:

- if a device's manufacturer/model/firmware is on the replacement exclusion list then permanently exclude
- when a device is added to the worklist then temporarily exclude for the next seven calendar days
- when replacement of the same certificate has been attempted four times then permanently exclude

4.2.4 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.

4.2.5 Other DSP Changes

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

No impact on performance is anticipated, although should be monitored.

No penetration testing will be required, and DSP anticipate no material impact to the DSP security implementation as the solution proposed is making use of pre-set patterns which are security assured.

4.3 Impacts on ECOS Provider (Accenture)

The changes to the existing ECOS solution will be relatively straightforward because the change has already been tested as part of the ECOS programme. The configuration change is planned to technically be in place within 12 weeks of the private key transfer programme going live. The Production version of the configuration is referred to as Config File 2.0:

Config File 1.0	Config File 1.5	Config File 2.0
- Targets 1M devices that failed migration, these devices are contained within the DCC Ops non-communicating device report that is managed via SECOPS / OPSG. - The file was going to future date rotations however it has been decided that <u>this config file will not be implemented at any stage.</u> - Failed migrated devices will be covered by no-comms projects.	- Targets all new installed devices. - The file is a temporary solution that ensures devices holding TCOS certificates at the point of install are captured and recorded by the ECOS solution. This config file will go live day 1 of PKT go live. - Due to operational reporting not being in place file 1.5 does not enable any level of rotation and simply captures the build up of TCOS devices.	- Targets all new installed devices. - The file is an enduring solution that ensures devices holding TCOS/ECOS certificates at the point of install are rotated by the ECOS solution. This config file will go live as soon as operational reporting is in place. - This solution has been tested extensively in SIT & is going live in UIT ahead of its production release. This file ensures all devices have their ECOS certificate rotated within 7 days of install.

4.4 Data Science and Analytics Team

The DCC Data Science and Analytics (DS&A) team will provide the reporting required for this Modification, and will continue to use the Device Key Mapping table delivered to obtain information of device key rotation. The work for providing a regular feed of SMKI certificate details from the DSP to the DS&A is already included in phase 2 of SECMP0239 (CR5170), so there is no extra DSP effort for this element of the solution, nor any further charges beyond the reporting content and layout. The current data reports align to SECMP0268, they simply become mandatory.

5 Implementation Timescales and Approach

The pre-integration phase is expected to take approximately **one** month for each Phase of Detailed Design, Build, and Pre-Integration Testing (PIT). Allowing for post-PIT integration testing, the change will be ready to schedule to a production release after approximately nine months, which allows for a defined period of User Integration Testing (UIT) common to previous Releases, even though there is no stated requirement for functional UIT.

DCC anticipates the change will be implemented in the November 2025 SEC Release.

5.1 DSP Pre-Integration Testing

The scope of this FIA includes activities required to:

- update the build process and deployments to PIT environments up until the point of PIT complete; and
- deploy new application builds to PIT environments during the PIT phase.

PIT testing will include testing both existing updated DSP Use Cases, and new Use Cases developed for SECMP0268 to check the selection of devices for ACB replacement with recently installed devices being prioritised. As part of PIT there will also regression test other parts of ACB replacement to ensure there are no unintended consequences.

Automated testing will be used where possible, and no performance testing is required for this change.

5.2 System Integration Testing (SIT)

This SIT response covers only activities and deliverables that are specific to functionality in this Modification. The SIT team will plan, prepare, and execute tests that demonstrate the correct behaviour of the Change, verifying the successful rotation of ACB and ECoS certificates based on the configured durations.

For each device set required for SIT Solution Testing will comprise:

- Install & Commission of an ESME, GSME and PPMID;
- verifying that, following commissioning of the devices and, at the time configured, a script is executed to initiate the relevant ACB or ECoS certificate rotation;
- verifying that the certificates are rotated successfully (from their manufacturing certificate) through submission of SRV 6.24.1 and querying the Smart Metering Inventory; and
- decommissioning.

To carry out the scope of SIT testing, EDMI, Toshiba, and 4G Toshiba Comms Hubs will be required, each with ESME, GSME, and PPMID devices. There is no requirement for SMETS1 devices.

The number of tests and durations for eh functional SIT testing is expected to be as follows.

Test Phase	Type	Total Tests	Plan Start	Plan End	Workdays	Envir Avail	Net Days	Re-Test	Total Test	Test per Day
I&C	Automated	84	01/07/2025	11/08/2025	30	85%	26	1.1	92	3.6
I&C	Manual	6	01/07/2025	11/08/2025	30	85%	26	1.1	7	0.3
Functional Testing	Automated	12	01/07/2025	11/08/2025	30	85%	26	1.4	17	0.7
Functional Testing	Manual	1	01/07/2025	11/08/2025	30	85%	26	1.4	1	0.1
Decommission	Automated	27	01/07/2025	11/08/2025	30	85%	26	1.1	30	1.2
Decommission	Manual	3	01/07/2025	11/08/2025	30	85%	26	1.1	3	0.1
Totals/Averages		133							150.2	

5.3 User Integration Testing (UIT)

There is no perceived need to test this separately in the UIT environment. However, as part of the SEC Release, it may be decided that Users will be allowed to carry out a set amount of UIT. No costs for this are included in the costs for this Modification, and those costs will be calculated as part of the post-PIT CR.

5.4 Changes to DS&A Reporting

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

5.5 Transition to Operations

All efforts and costs for these elements of the solution reflect Business as Usual support activities.

Knowledge transfer from the Development team to Application Management Services (AMS team) will be required with a review of the Production system configuration to ensure it can support the required daily certificate replacements efficiently. Alerting and dashboards will be updated for this functionality also.

A brief period of Early Life Support will be required to support performance monitoring.

As the changes to ECoS have already been tested, they will be implemented in the production system. There will be some effort required from the ECOS Service Provider, but this is limited.

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 separate estimate of these costs is provided by DCC.

A detailed calculation of the two sets of costs will be carried out through a "Release CR" also referred to as a "Post-PIT CR" when the contents of the targeted SEC Release are finalised.

£	Design, Build, and PIT	Integration Testing, SIT and UIT	TTO	Application Support	Total
SECMP0268	204,500	62,357	15,976	6,167	289,000

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 Service Provider has allowed for an increase of four low complexity support cases per month for the duration of two months, immediately following the release to Production.

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

No changes to Schedule 2.2 (Performance Measures and Reporting) are expected as a result of this Change Request.

Other Service Providers are not impacted.

Appendix A: Glossary

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

Acronym	Definition
ACB	Access Control Broker
AMS	Application Management Services
CAN	Contract Amendment Note
Comms Hub	Communications Hub
COS	Change of Supplier
CR	DCC Change Request
CSP	Communications Services Provider
DCC	Data Communications Company
DS&A	(DCC) Data Science and Analytics
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DS&A	Data Science and Analytics
DUIS	DCC User Interface Specification
ECOS, ECoS	Enduring Change of Supplier
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
GUID	Global Unique Identifier
I&C	Install and Commission
MMC	Message Mapping Catalogue
OCA	Organisation Certification Authority
PIA	Preliminary Impact Assessment
PCO	Post Commissioning Obligations
PIT	Pre-Integration Testing
PPMID	Pre-Payment Meter user Interface Device
RAID	Risks, Assumptions, Issues, and Dependencies

ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SoLR	Supplier of Last Resort
SR	Service Request
SRV	Service Reference Variant
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TCOS	Transitional Change of Supplier
TTO	Transition to Operations (Implementation)
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.

MP268 ‘Certificate rotation and expired Certificates’

Annex D

Refinement Consultation responses

About this document

This document contains the full collated responses received to the MP268 Refinement Consultation.

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

Question 1			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	Yes	
British Gas	Large Supplier	Yes	
Utilita	Large Supplier	Yes	We agree that the solution proposed will resolve the issue, however, we question the scale of costs presented as part of the PIA, as we are being forced to pay a relatively large sum of money to resolve a problem that was caused by the implementation of MP261, which was also raised by the DCC
UK Power Networks	Network Party	Yes	UK Power Networks agrees with the Proposed Solution because it established a standard procedure for updating Smart Meter security Certificates that have a Validity Period longer than ten years. If the Certificate is revoked or is expired to ensure ongoing network security and compliance.
National Grid Electricity Distribution	Network Party	Yes	-
Scottish and Southern Electricity Networks	Network Party	Yes	By developing clear guidelines within the SEC, we believe that SEC MP268 will reduce the risk of unauthorised access thereby mitigating data being compromised by proactively investing in security measures in turn resulting in a reliable Smart Metering Network.
Electricity North West Limited	Network Party	Yes	This approach is sensible and targeted for security assurance and is an appropriate and proportionate.

Question 2: Do you agree that the legal text will deliver MP268?

Question 2				
Respondent	Category	Response	Rationale	SECAS Response
E.ON	Large Supplier	Yes	In the legal text, should the time periods shown in 5.20 and 5.21 be the same, i.e., after 48 hours but before 7 days? Subject to the correct time periods being shown, the changes to the legal text clearly address the DCC's obligations which this modification introduces.	Initially a seven-day window was set based on DCC's design which is not mandated but followed as good practice by the DSP. After the DCC's consulting with SSC and SMKI PMA, a 48-hour window was deemed to prevent longer life Certificates remaining on Devices.
British Gas	Large Supplier	-	Not reviewed	
Utilita	Large Supplier	Yes	-	
UK Power Networks	Network Party	Yes	We agree that the legal text will deliver MP268 because it has been updated to provide guidance on Certificate Validity Periods and the requirement to update Certificates.	
National Grid Electricity Distribution	Network Party	Yes	-	
Scottish and Southern Electricity Networks	Network Party	Yes	We agree the legal text on Section G 'Security' will deliver MP268.	

Question 2				
Respondent	Category	Response	Rationale	SECAS Response
Electricity North West Limited	Network Party	Yes	-	

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

Question 3			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	Yes	-
British Gas	Large Supplier	Yes	From a purely Supplier perspective, this is a beneficial change. It increases the time before Certificate expiry, and therefore reduces the risk of loss communications to a Device, were an expired Certificate to result in a meter becoming non comms.
Utilita	Large Supplier	Yes	The proposed approach makes sense.
UK Power Networks	Network Party	Yes	We agree with the proposed implementation approach because it ensures the modification is implemented soon after it is approved and before expiry of the original Certificates.
National Grid Electricity Distribution	Network Party	Yes	-
Scottish and Southern Electricity Networks	Network Party	Yes	We agree with the proposed implementation approach that is aimed to be implemented at latest in November 2025, as part of the SEC Release including DCC System changes before the original Certificates expire.
Electricity North West Limited	Network Party	Yes	-

Question 4: Will there be any impact on your organisation to implement MP268?

Question 4			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	No	This change relates to the Organisation Certificates which the DCC is responsible for managing and has no direct effect on Suppliers.
British Gas	Large Supplier	No	This change will not place any extra requirements on Suppliers. It will also reduce the frequency of future Certificate replacements, which will have a longer-term reduction on Supplier workload.
Utilita	Large Supplier	No	As this modification is being implemented on DCC's side, there would be no impact to us.
UK Power Networks	Network Party	Yes	UK Power Networks will be required to assess which meters will require replacement of a Certificate and then to apply a new Certificates. We are already aware that Certificates will need to be updated ahead of their expiry dates and had been planning for this situation. As we approach the ten-year period from the original date of 2015, we will develop a process for the regular review of Certificate expiry dates and update of those requiring replacement.
National Grid Electricity Distribution	Network Party	No	-
Scottish and Southern Electricity Networks	Network Party	No	n/a
Electricity North West Limited	Network Party	Yes	As a network operator we will have 3 areas of responsible for delivery under the business requirements.

Question 5: Will your organisation incur any costs in implementing MP268?

Question 5			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	N/A	
British Gas	Large Supplier	No	
Utilita	Large Supplier	No	As there are no changes required, there will be no costs to us
UK Power Networks	Network Party	Less than £100k	As mentioned in response to question four. UK Power Networks will develop a process to review and replace Certificates, therefore we can only provide an approximated estimate of likely costs to be incurred for the initial effort and ongoing work.
National Grid Electricity Distribution	Network Party	No	-
Scottish and Southern Electricity Networks	Network Party	No costs	-
Electricity North West Limited	Network Party	-	-

Question 6: How long from the point of approval would your organisation need to implement MP268?

Question 6			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	n/a	-
British Gas	Large Supplier	-	-
Utilita	Large Supplier	None	As there are no changes required, there would be no lead time required
UK Power Networks	Network Party	1 Year	Currently, there are 4.6 million Smart Meters in UK Power Network's' regions. UK Power Networks have initiated a project to schedule and plan the replacement of the ten year Certificates. Activities include: • Develop project plan • Procurement of resource from third party support • A schedule of the work to update the Certificates associated with 460,000 meters per month, taking into consideration DCC approval/awareness of increased Service Request Variant traffic • Testing of changes • Deployment of new Certificates into production
National Grid Electricity Distribution	Network Party	n/a	-
Scottish and Southern	Network Party	n/a	-

Question 6			
Respondent	Category	Response	Rationale
Electricity Networks			
Electricity North West Limited	Network Party	-	-

Question 7: Do you believe that MP268 would better facilitate the General SEC Objectives?

Question 7			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	Yes	Better facilitates General SEC Objective (f). The Proposed changes address the potential security and obligation gap which currently exists
British Gas	Large Supplier	-	
Utilita	Large Supplier	Yes	We believe this modification will better facilitate objective (f), as these Certificates not being rotated could pose a security risk
UK Power Networks	Network Party	Yes	We agree with the proposer's view that the modification will support the General SEC Objective (f) to ensure the protection of Data and the security of Data and Systems in the operation of this Code.
National Grid Electricity Distribution	Network Party	Yes	-
Scottish and Southern Electricity Networks	Network Party	Yes	We believe MP268 will better facilitate General SEC Objective (f) as the Proposed Solution mitigates data being compromised.
Electricity North West Limited	Network Party	Yes	We agree the modification supports SEC Objective (f)

Question 8: Do you believe there will be any impacts on or benefits to consumers if MP268 is implemented?

Question 8			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	Yes	The benefit is the enduring security of data and smart meter systems.
British Gas	Large Supplier	No	-
Utilita	Large Supplier	Yes	This modification would potentially prevent unauthorised access to Smart equipment which could be of benefit to consumers, but we do not believe there would be any direct and tangible benefits.
UK Power Networks	Network Party	Yes	We do not believe there will be any direct impact on consumers other than to benefit the consumer by providing improved network security and to reduce the risk of unauthorised access to the consumer's Smart Meter.
National Grid Electricity Distribution	Network Party	Yes	We believe consumers will benefit for the reasons stated in the Modification Report.
Scottish and Southern Electricity Networks	Network Party	Yes	We believe MP268 will benefit the consumer as the Proposed Solution looks to mitigate data being compromised thereby improving safety and reliability of devices on the Smart Metering network.
Electricity North West Limited	Network Party	-	-

Question 9: Noting the costs and benefits of this modification, do you believe MP268 should be approved?

Question 9			
Respondent	Category	Response	Rationale
E.ON	Large Supplier	Yes	For reasons previously given.
British Gas	Large Supplier	Yes	We would expect expert opinions from the various sub-groups (TABASC, SMKI PMA, SSC) to make the recommended decision, but from a Supplier-only perspective, we would support this.
Utilita	Large Supplier	Yes	Given the potential security concerns and the risk of unauthorised access, we believe this modification should be implemented. However, we note that this has only become an issue because of a previous modification raised by the DCC and must once again call out the fact that we are being forced to pay to fix an issue created by another party.
UK Power Networks	Network Party	Yes	Please see response to question 8.
National Grid Electricity Distribution	Network Party	Yes	-
Scottish and Southern Electricity Networks	Network Party	Yes	We believe the benefits around risk mitigation in the long term outweigh the costs that will be undertaken to implement MP268.
Electricity North West Limited	Network Party	Yes	Refer to response to Q1.

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

Question 10		
Respondent	Category	Comments
E.ON	Large Supplier	-
British Gas	Large Supplier	-
Utilita	Large Supplier	-
UK Power Networks	Network Party	-
National Grid Electricity Distribution	Network Party	-
Scottish and Southern Electricity Networks	Network Party	-
Electricity North West Limited	Network Party	-

A large, dark purple circle is centered on the page. Inside the circle is a faint, intricate network pattern of thin lines and small dots, some of which are highlighted in a lighter shade of purple. The text 'MP268' and 'Full End to End costs (inc regression testing)' is centered within this circle in a white, sans-serif font.

MP268

Full End to End costs (inc regression testing)

Version: 1.2
Date: 20/12/2024
Author: Robbie McMillan

SECMP0268 Supporting Test Costs Overview

The table below details the estimate of testing costs that might be incurred if this SEC Modification was to be deployed via a SEC Release but in isolation. Other Modifications or Change Requests in a SEC Release might well split the costs across multiple changes, possibly with minimal increases to overall testing costs.

The functional testing is described, and costs broken out, in the Full Impact Assessment (FIA). The FIA description includes the number of test sets, and anticipated number of tests required to fully test the functional change introduced by the Modification.

Regression testing covers additional testing and administrative overhead to ensure that the DCC Total System is fully functioning. System Integration Testing (SIT) costs are initially established by the Service Providers for the DCC Total System, but are refined as part of the Release Change Request and Implementation phase, for which the former is also referred to as the post-PIT Change Request.

User Integration Testing (UIT) as part of the Regression testing refers to the testing period which is made available for SEC parties to test their systems against the future state of the DCC Total System.

There is no perceived need to test this separately in the UIT environment. However, as part of the SEC Release, it may be decided that Users will be allowed to carry out a set amount of UIT. No costs for this are included in the costs for this Modification, and those costs will be calculated as part of the post-PIT CR.

The figures have been estimated based on previous SEC Releases, where a diverse environment supporting multiple GBCS versions and has been open for up to six weeks previously which must be supported by Service Providers.

All the testing activities and estimates will be reviewed as part of post approval implementation activities, which as suggested above, will be impacted by additional Modifications or Change Requests in that SEC Release.

The table also presents two options that shows value for money choice, based on scope and risk appetite.

Description	Cost
FUNCTIONAL	
Design, Build, PIT, functional testing in SIT, Path to Live	£289,000
REGRESSION	
Option 1 and 2: 6 weeks SIT regression testing including CSP support	£169,800
UIT Option 1: 6 weeks UIT Testing costs (as per policy document)	£480,000
UIT Option 2: 0 weeks UIT Testing costs (as per FIA statement)	£0
Total (Option 1)	£ 938,800
Total (Option 2)	£ 458,800

Costs are estimated ONLY and will likely change if scope within a target SEC System Release window, changes.