

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.



MP268

‘Certificate rotation and expired Certificates’

Modification Report

Version 0.5

18 September 2024



About this document

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

Contents

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

This document also has three annexes:

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

Contact

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

Mohammedanwar Sumro

020 2924 4506

mohammedanwar.sumro@gemserv.com

1. Summary

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

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

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

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

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

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

2. Issue

What are the current arrangements?

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

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

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

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

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

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

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

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

What is the issue?

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

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

What is the impact this is having?

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

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

Impact on consumers

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

3. Solution

Proposed Solution

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

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

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

4. Impacts

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

SEC Parties

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

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

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

DCC Systems

DCC System changes

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

Data management elements are enhanced to identify Devices with:

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

Reports will be formed by the following data attributes:

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

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

DCC System traffic

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

SEC and subsidiary documents

The following parts of the SEC will be impacted:

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

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

Devices

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

Consumers

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

Other industry Codes

This modification will have no impact on other industry Codes.

Greenhouse gas emissions

This modification will have no impact on greenhouse gas emissions.

5. Costs

DCC costs

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

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

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

SECAS costs

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

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

SEC Party costs

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

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **6 November 2025** (November 2025 SEC Release) if a decision to approve is received on or before 22 July 2025 or
Ad-Hoc SEC Release 10 Working Days following a decision to approve is received after 22 July 2025.

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

7. Assessment of the proposal

Areas for assessment

Why is this modification needed?

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

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

Consumer risk mitigation

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

Observations on the issue

Views from the Working Group

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

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

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

Views from the TABASC

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

Views from the SMKI PMA

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

Views from the SSC

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

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

Sub-Committee input

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

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

Observations on the issue

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

Solution development

Timeframe of Certificate replacement

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

Exclusion of PPMIDs

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

8. Case for change

Business case

Approval of the modification

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

Views against the General SEC Objectives

Proposer's views

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

Industry views

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

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

Views against the consumer areas

Improved safety and reliability

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

Lower bills than would otherwise be the case

This modification does not lower bills.

Reduced environmental damage

This modification does not impact environmental damage.

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

Improved quality of service

This modification does not impact the quality of service.

Benefits for society as a whole

This modification does not impact society as a whole.

Appendix 1: Progression timetable

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

Italics denote planned events that could be subject to change

Appendix 2: Glossary

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

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

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 0.5

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 seven days 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 seven days but before 23 days have elapsed), the “accessControlBroker” Organisation Certificates on that Device will under all reasonable steps be replaced

Following Working Group discussions and engagement with a Large Supplier Party, the Proposer has agreed that Access Control Broker (ACB) Organisation Certificates are to be replaced between after seven days but before 23 days after a 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.

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 0.1

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.

Add Section G.8.3 as follows:

G8. USER SECURITY ASSURANCE

Procurement of the User Independent Security Assurance Service Provider

G8.1 The Panel shall procure the provision of security assurance services:

- (a) of the scope specified in Section G8.3;
- (b) from a person who:
 - (i) is suitably qualified in accordance with Section G8.4;
 - (ii) is suitably independent in accordance with Section G8.7; and
 - (iii) satisfies the capacity requirement specified in Section G8.11,
- (c) and that person is referred to in this Section G8 as the “**User Independent Security Assurance Service Provider**”.

G8.2 The Panel may appoint more than one person to carry out the functions of the User Independent Security Assurance Service Provider.

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.

Suitably Qualified Service Provider

G8.4 The User Independent Security Assurance Service Provider shall be treated as suitably qualified in accordance with this Section G8.4 only if it satisfies:

- (a) the requirements specified in Section G8.5; and
- (b) the requirements specified in Section G8.6.

G8.5 The requirements specified in this Section G8.5 are that the User Independent Security Assurance Service Provider:

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2013 (Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

G8.6 The requirement specified in this Section G8.6 is that the User Independent Security Assurance Service Provider:

- (a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either the 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assurance assessments in accordance with this Section G8.

Independence Requirement

G8.7 The User Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G8.7 only if it satisfies:

- (a) the requirements specified in Section G8.9; and
- (b) the requirement specified in Section G8.10.

G8.8 For the purposes of Sections G8.9 and G8.10:

- (a) a "**Relevant Party**" means any Party in respect of which the User Independent Security Assurance Service Provider carries out functions under this Section G8; and
- (b) a "**Relevant Service Provider**" means any service provider to a Relevant Party from which that Party acquires capability for a purpose related to its compliance with its obligations as a User under Sections G3 to G6.

G8.9 The requirements specified in this Section G8.9 are that:

- (a) no Relevant Party or any of its subsidiaries, and no Relevant Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the User Independent Security Assurance Service Provider;
- (b) no director of any Relevant Party, and no director of any Relevant Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the User Independent Security Assurance Service Provider; and
- (c) the User Independent Security Assurance Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in any Relevant Party or any Relevant Service Provider,

(but for these purposes references to a Relevant Service Provider shall not include the User Independent Security Assurance Service Provider where it acts in that capacity).

G8.10 The requirement specified in this Section G8.10 is that the User Independent Security Assurance Service Provider is able to demonstrate to the satisfaction of the Panel that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with a Relevant Party or Relevant Service Provider (and for these purposes a 'commercial relationship' shall

include a relationship established by virtue of the User Independent Security Assurance Service Provider itself being a Relevant Service Provider to any Relevant Party).

Capacity Requirement

G8.11 The capacity requirement specified in this Section G8.11 is that the User Independent Security Assurance Service Provider must be capable of meeting the Panel's estimate of the demand for its security assurance services throughout the period in relation to which those services are being procured.

Compliance of the User Independent Security Assurance Service Provider

G8.12 The Panel shall be responsible for ensuring that the User Independent Security Assurance Service Provider carries out its functions in accordance with the provisions of this Section G8.

Users: Duty to Cooperate in Assessment

G8.13 Each User shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the User Independent Security Assurance Service Provider), for the purposes of facilitating an assessment of that User's compliance with its obligations under Sections G3 to G6 or any CPA Certificate Remedial Plan.

G8.14 For the purposes of Section G8.13, a User shall provide the Security Sub-Committee (or the relevant person acting on its behalf or at its request) with:

- (a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;
- (b) all such other forms of cooperation as may reasonably be requested, including in particular:
 - (i) access at all reasonable times to such parts of the premises of that User as are used for, and such persons engaged by that User as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G3 to G6; and
 - (ii) such cooperation as may reasonably be requested by the Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G8.

Categories of Security Assurance Assessment

G8.15 For the purposes of this Section G8, there shall be the following four categories of security assurance assessment:

- (a) a Full User Security Assessment (as further described in Section G8.16);
- (b) a Verification User Security Assessment (as further described in Section G8.17);
- (c) a User Security Self-Assessment (as further described in Section G8.18); and

(d) a Follow-up Security Assessment (as further described in Section G8.19).

G8.16 A **"Full User Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify the extent to which that User is compliant with each of its obligations under Sections G3 to G6 in each of its User Roles.

G8.17 A **"Verification User Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider in respect of a User to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User.

G8.18 A **"User Security Self-Assessment"** shall be an assessment carried out by a User, the outcome of which is reviewed by the User Independent Security Assurance Service Provider, to identify any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a User Security Assessment was carried out in respect of that User.

G8.19 A **"Follow-up Security Assessment"** shall be an assessment carried out by the User Independent Security Assurance Service Provider, following a User Security Assessment, in accordance with the provisions of Section G8.29.

G8.20 For the purposes of Sections G8.17 and G8.18, a Verification Security Assessment and User Security Self-Assessment shall each be assessments carried out in respect of a User having regard in particular to:

- (a) any changes made to any System, Data, functionality or process falling within the scope of Section G5.14 (Information Security: Obligations on Users);
- (b) where the User is a Supplier Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Responsible Supplier; and
- (c) where the User is a Network Party, any increase in the number of Enrolled Smart Metering Systems for which it is the Electricity Distributor or the Gas Transporter.

User Security Assessments: General Procedure

User Security Assessment Methodology

G8.21 Each User Security Assessment carried out by the User Independent Security Assurance Service Provider shall be carried out in accordance with the User Security Assessment Methodology applicable to the relevant category of assessment.

The User Security Assessment Report

G8.22 Following the completion of a User Security Assessment, the User Independent Security Assurance Service Provider shall, in discussion with the User to which the assessment relates, produce a written report (a **"User Security Assessment Report"**) which shall:

- (a) set out the findings of the User Independent Security Assurance Service Provider on all the matters within the scope of the User Security Assessment;
- (b) in the case of a Full User Security Assessment:
 - (i) specify any instances of actual or potential non-compliance of the User with its obligations under Sections G3 to G6 which have been identified by the User Independent Security Assurance Service Provider; and
 - (ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified; and
- (c) in the case of a Verification User Security Assessment:
 - (i) specify any material increase in the security risk relating to that User which the User Independent Security Assurance Service Provider has identified since the last occasion on which a Full User Security Assessment was carried out in respect of that User; and
 - (ii) set out the evidence which, in the opinion of the User Independent Security Assurance Service Provider, establishes the increase in security risk which it has identified.

G8.23 The User Independent Security Assurance Service Provider shall submit a copy of each User Security Assessment Report to the Security Sub-Committee and to the User to which that report relates.

The User Security Assessment Response

G8.24 Following the receipt by any User of a User Security Assessment Report which relates to it, the User shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

- (a) produce a written response to that report (a "**User Security Assessment Response**") which addresses the findings set out in the report; and
- (b) submit a copy of that response to the Security Sub-Committee and the User Independent Security Assurance Service Provider.

G8.25 Where a User Security Assessment Report:

- (a) following a Full User Security Assessment, specifies any instance of actual or potential non-compliance of a User with its obligations under Sections G3 to G6; or
- (b) following a Verification User Security Assessment, specifies any material increase in the security risk relating to a User since the last occasion on which a Full User Security Assessment was carried out in respect of that User,

the User shall ensure that its User Security Assessment Response includes the matters referred to in Section G8.26.

G8.26 The matters referred to in this Section are that the User Security Assessment Response:

- (a) indicates whether the User accepts the relevant findings of the User Independent Security Assurance Service Provider and, where it does not, explains why this is the case;
- (b) sets out any steps that the User has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the User Security Assessment Report; and
- (c) identifies a timetable within which the User proposes to take any such steps that have not already been taken.

G8.27 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), the Security Sub-Committee (having considered the advice of the User Independent Security Assurance Service Provider) shall review that response and either:

- (a) notify the User that it accepts that the steps that the User proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the User Security Assessment Report; or
- (b) seek to agree with the User such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G8.28 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User shall:

- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) report to the Security Sub-Committee on:
 - (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;
 - (ii) the completion of those steps in accordance with the timetable; and
 - (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G8.29 Where a User Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G8.26(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G8.27, the User Independent Security

Assurance Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the relevant User to:

- (a) identify the extent to which the User has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) assess any other matters related to the User Security Assessment Response that are specified by the Security Sub-Committee.

User Security Assessments: Further Provisions

G8.30 The User Independent Security Assurance Service Provider:

- (a) may in its discretion, and shall where directed to do so by the Security Sub-Committee:
 - (i) in relation to a User which acts in more than one User Role, determine that a single User Security Assessment may be carried out in relation to that User in respect of any two or more such User Roles; and
 - (ii) in carrying out any User Security Assessment, take into account any relevant security accreditation or certification held by the relevant User; and
- (b) shall, where any Shared Resources which have not been provided by a Shared Resource Provider form part of the User Systems of more than one User, have regard to information obtained in relation to such Shared Resources in the User Security Assessment of one such User when carrying out a User Security Assessment of any other such User.

Initial Full User Security Assessment: User Entry Process

G8.31 Sections G8.33 to G8.39 set out the applicable security requirements referred to in Section H1.10(c) (User Entry Process Requirements).

G8.32 For the purposes of Sections G8.33 to G8.39, any reference in Sections G3 to G6 or the preceding provisions of this Section G8 to a 'User' (or to any related expression which applies to Users), shall be read as including a reference (or otherwise applying) to any Party seeking to become a User by completing the User Entry Process for any User Role.

Initial Full User Security Assessment

G8.33 For the purpose of completing the User Entry Process for a User Role, a Party wishing to act as a User in that User Role shall be subject to a Full User Security Assessment in respect of the User Role.

Panel: Setting the Assurance Status

G8.34 Following the completion of that initial Full User Security Assessment, the Security Sub-Committee shall ensure that copies of both the User Security Assessment Report and User Security Assessment Response are provided to the Panel.

G8.35 Following the receipt by it of the User Security Assessment Report and User Security Assessment Response, the Panel shall promptly consider both documents and (having regard to any advice of the Security Sub-Committee) set the assurance status of the Party, in relation to its compliance with each of its obligations under Sections G3 to G6 in the relevant User Role, in accordance with Section G8.36.

G8.36 The Panel shall set the assurance status of the Party as one of the following:

- (a) approved;
- (b) approved, subject to the Party:
 - (i) taking such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or
 - (ii) both taking such steps and being subject to a Follow-up Security Assessment by such date as the Panel may specify,
- (c) deferred and:
 - (i) the Party having first taken such steps as it proposes to take in its User Security Assessment Response in accordance with Section G8.26(b) and been subject to a Follow-up Security Assessment; and
 - (ii) the Panel having determined that it is satisfied, on the evidence of the Follow-up Security Assessment, that such steps have been taken; or
- (d) rejected and:
 - (i) the Party shall have a second Full User Security Assessment to address any issues identified by the Panel as being, in the opinion of the Panel, not adequately addressed in that response as submitted to the Security Sub-Committee; and
 - (ii) upon completion of the second Full User Security Assessment the Panel will reconsider the assurance status in accordance with Section G8.35.

Approval

G8.37 For the purposes of Sections H1.10(c) and H1.11 (User Entry Process Requirements):

- (a) a Party shall be considered to have successfully demonstrated that it meets the applicable security requirements of this Section G8 when:
 - (i) the Panel has set its assurance status to 'approved' in accordance with either Section G8.36(a) or (b); or

- (ii) the Panel has set its assurance status to 'deferred' in accordance with Section G8.36(c) and the requirements specified in that Section have been met; and
- (b) the Panel shall notify the Code Administrator as soon as reasonably practicable after the completion of either event described in paragraph (a)(i) or (ii).

Obligations on an Approved Party

G8.38 Where the Panel has set the assurance status of a Party to 'approved subject to' specified in Section G8.36(b), the Party shall take the steps to which that approval is subject in accordance with that section.

Disagreement with Panel Decisions

G8.39 Where a Party disagrees with any decision made by the Panel in relation to it under Section G8.36, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Security Assurance Assessments: Post-User Entry Process

G8.40 Within 12 months after completion of the User's initial Full User Security Assessment (or after the Follow-up Security Assessment where there was one), for the purposes of the User Entry Process, a User shall schedule a User Security Assessment with the User Independent Security Assurance Provider in accordance with the provisions of Sections G8.41 to G8.47. The initial Full User Security Assessment will be deemed complete when the Panel set an assurance status of:

- (a) approved; or
- (b) approved, subject to the User:
 - (i) taking such steps as the User proposes to take in its User Security Assessment Response in accordance with Section G8.26(b); or
 - (ii) both taking the steps referred to in (i) above and being subject to a Follow-up Security Assessment by such date as the Panel may specify.

Supplier Parties

G8.41 Where a User is a Supplier Party and either:

- (a) the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 250,000; or
- (b) the number of Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier exceeds 50,000; or
- (c) $(5N) + D > 250,000$

Where N is the number of Non-Domestic Premises and D is the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier,

the User Security Assessment required by Section G8.40 shall be a Full User Security Assessment and the User shall schedule a further Full User Security Assessment within 12 months after each Full User Security Assessment.

G8.42 Where a User is a Supplier Party of electricity and/or gas to Domestic Premises and/or Non-Domestic Premises through one or more Smart Metering Systems for which it is the Responsible Supplier but does not meet any of the criteria specified under Section G8.41, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

- (a) within 12 months after each Verification User Security Assessment schedule a User Security Self-Assessment; and
- (b) within 12 months after each User Security Self-Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and
- (c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.43 In assessing for the purposes of Sections G8.41 and G8.42 the number of Domestic Premises and Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Responsible Supplier, that number shall, where any Shared Resources which are not provided by a Shared Resource Provider form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises or Non-Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Responsible Supplier.

Network Parties

G8.44 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter exceeds 250,000, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

- (a) within 12 months after previous Verification User Security Assessment, schedule a second Verification User Security Assessment with the User Independent Security Assurance Provider;
- (b) within 12 months after each second successive Verification User Security Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and

- (c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.45 Where a User is a Network Party and the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter is equal to or less than 250,000, the User Security Assessment required by Section G8.40 shall be a Verification User Security Assessment and the User shall:

- (a) within 12 months after each Verification User Security Assessment, schedule a User Security Self-Assessment;
- (b) within 12 months after each User Security Self-Assessment, schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and
- (c) within 12 months after each Full User Security Assessment, schedule a Verification User Security Assessment with the User Independent Security Assurance Service Provider.

G8.46 In assessing for the purposes of Sections G8.44 and G8.45 the number of Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which a User is the Electricity Distributor and/or the Gas Transporter, that number shall, where any Shared Resources form part of both its User Systems and the User Systems of another User, be deemed to include any Domestic Premises supplied with electricity and/or gas through one or more Smart Metering Systems for which that other User is the Electricity Distributor and/or the Gas Transporter.

Other Users

G8.47 Where a User is neither a Supplier Party nor a Network Party, Section G8.40 requires the User to schedule a User Security Verification Assessment and the User shall:

- (a) within 12 months after the previous User Security Verification Assessment, schedule a User Security Self-Assessment;
- (b) within 12 months after the User Security Self-Assessment schedule a Full User Security Assessment with the User Independent Security Assurance Service Provider; and
- (c) within 12 months after each Full User Security Assessment, schedule a User Security Verification Assessment.

Interpretation

G8.48 Section G8.49 applies where:

- (a) pursuant to Sections G8.41 to G8.43, it is necessary to determine, in relation to any Supplier Party, the number of Domestic Premises and Non-Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Responsible Supplier; or

Managed by

- (b) pursuant to Sections G8.44 to G8.46, it is necessary to determine, in relation to any Network Party, the number of Domestic Premises that are supplied with electricity and/or gas through one or more Smart Metering Systems for which it is the Electricity Distributor and/or the Gas Transporter.

G8.49 Where this Section applies:

- (a) the determination referred to in Section G8.48 shall be made at the time at which the nature of each annual security assurance assessment for the relevant User falls to be ascertained; and
- (b) the DCC shall provide all reasonable assistance that may be requested by that User or the Security Sub-Committee for the purposes of making that determination.

User Security Self-Assessment

G8.50 Where, in accordance with the requirements of this Section G8, a User is subject to a User Security Self-Assessment in any year, that User shall:

- (a) carry out the User Security Self-Assessment during in accordance with the User Security Assessment Methodology that is applicable to User Security Self-Assessments; and
- (b) ensure that the outcome of the User Security Self-Assessment is documented and is submitted to the User Independent Security Assurance Service Provider for review by no later than the date which is 12 months after the date of the completion of the previous User Security Assessment or (if more recent) User Security Self-Assessment.

Users: Obligation to Pay Explicit Charges

G8.51 Each User shall pay to the DCC all applicable Charges in respect of:

- (a) all User Security Assessments and Follow-up Security Assessments carried out in relation to it by the User Independent Security Assurance Service Provider;
- (b) the production by the User Independent Security Assurance Service Provider of any User Security Assessment Reports following such assessments; and
- (c) all related activities of the User Independent Security Assurance Service Provider in respect of that User in accordance with this Section G8.

G8.52 Expenditure incurred in relation to Users in respect of the matters described in Section G8.51 shall be treated as Recoverable Costs in accordance with Section C8 (Panel Costs and Budgets).

G8.53 For the purposes of Section G8.51 the Panel shall, at such times and in respect of such periods as it may (following consultation with the DCC) consider appropriate, notify the DCC of:

- (a) the expenditure incurred in respect of the matters described in Section G8.51 that is attributable to individual Users, in order to facilitate Explicit Charges designed to

pass-through the expenditure to such Users pursuant to Section K7 (Determining Explicit Charges); and

- (b) any expenditure incurred in respect of the matters described in Section G8.51 which cannot reasonably be attributed to an individual User.

Events of Default

G8.54 In relation to an Event of Default which consists of a material breach by a User of any of its obligations under Sections G3 to G6, the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G8.55 to G8.60.

G8.55 Where in accordance with Section M8.2 the Panel receives notification that a User is in material breach of any requirements of Sections G3 to G6, it shall refer the matter to the Security Sub-Committee.

G8.56 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “Security Sub-Committee”.

G8.57 Where the Security Sub-Committee has:

- (a) carried out an investigation in accordance with Section M8.3; or
- (b) received a report from the User Independent Security Assurance Service Provider, following a User Security Assessment, concluding that a User is in actual or potential non-compliance with any of its obligations under Sections G3 to G6,

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any obligations under Sections G3 to G6 has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G8.58 Where the Panel determines that an Event of Default has occurred, it shall:

- (a) notify the relevant User and any other Party it considers may have been affected by the Event of Default; and
- (b) determine the appropriate steps to take in accordance with Section M8.4.

G8.59 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G8.60 Where the Panel determines that a User is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

Shared Resource Providers

G8.61 Section G8.62 applies where:

- (a) Shared Resources are provided to a User by a Shared Resource Provider; and

- (b) any User Security Assessment is carried out in respect of that Shared Resource Provider.

G8.62 Where this Section applies:

- (a) the outcome of the User Security Assessment (including for these purposes any actions or decisions described at Sections G8.22 to G8.29) shall be treated as applying to the User, in respect of the Shared Resources, in the same manner as it is applicable to the Shared Resource Provider; and
- (b) in any User Security Assessment which takes place in respect of the User, the User Independent Security Assessment Service Provider shall, with regard to matters relating to the Shared Resources, rely on the outcome of the most recent User Security Assessment in respect of the Shared Resource Provider and shall not be required to repeat that assessment.

G8.63 For the purposes of Section G8.40, where a Shared Resource Provider provides Shared Resources to Users which are:

- (a) Supplier Parties, the provisions of Sections G8.41 and G8.42 shall apply to the Shared Resource Provider as if it was a Supplier Party and the Smart Metering Systems for which those Supplier Parties are the Responsible Suppliers were Smart Metering Systems for which it is the Responsible Supplier;
- (b) Network Parties, the provisions of Sections G8.44 to G8.46 shall apply to the Shared Resource Provider as if it was a Network Party and the Smart Metering Systems for which those Network Parties are the Electricity Distributor and/or Gas Transporter were Smart Metering Systems for which it is the Electricity Distributor and/or Gas Transporter;
- (c) Other Users, the provisions of Section G8.47 shall apply to the Shared Resource Provider as if it was an Other User.

CPA Certificate Remedial Plan Preparation

G8.64 Where a User is a Supplier Party, the User shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

Add Section G9.2 as follows:

G9. DCC SECURITY ASSURANCE

The DCC Independent Security Assessment Arrangements

G9.1 The DCC shall establish, give effect to, maintain and comply with arrangements, to be known as the "**DCC Independent Security Assessment Arrangements**", which shall procure the services of a DCC Independent Security Assessment Service Provider to undertake security assessment services.

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 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.

G9.3 The actions specified in this Section G9.3 shall be actions taken by the DCC to:

- (a) procure the provision of security assessment services by the DCC Independent Security Assessment Service Provider (as further described in Section G9.4);
- (b) ensure that the DCC Independent Security Assessment Service Provider carries out Security Assessments for the purpose specified in Section G9.2:
 - (i) annually;
 - (ii) on any material change to the DCC Total System; and
 - (iii) at any other time specified by the Security Sub-Committee or the Panel;
- (c) comply with the arrangements set out by the Security Sub-Committee in a Security Controls Framework;
- (d) in line with the methodology and processes set out in the Security Controls Framework:
 - (i) procure that the DCC Independent Security Assessment Service Provider produces a DCC Security Assessment Report following each such assessment that has been carried out;
 - (ii) ensure that the DCC Independent Security Assessment Service Provider provides the Security Sub-Committee with a copy of each such DCC Security Assessment Report;
 - (iii) produce a DCC Security Assessment Response in relation to each such report; and
 - (iv) provide to the Panel and the Security Sub-Committee a copy of each DCC Security Assessment Response and, as soon as reasonably practicable thereafter, a report on its implementation of any action plan that is required by the Security Sub-Committee.

The DCC Independent Security Assessment Service Provider

G9.4 For the purposes of Section G9.3, the "**DCC Independent Security Assessment Service Provider**" shall be a person who is appointed by the DCC to provide security assessment services:

- (a) of the scope specified in Section G9.2;
- (b) from a person who:

- (i) is suitably qualified in accordance with Section G9.5;
- (ii) is suitably independent in accordance with Section G9.8.

Suitably Qualified Service Provider

G9.5 The DCC Independent Security Assessment Service Provider shall be treated as suitably qualified in accordance with this Section G9.5 only if it satisfies:

- (a) the requirements specified in Section G9.6; and
- (b) the requirement specified in Section G9.7.

G9.6 The requirements specified in this Section G9.6 are that the DCC Independent Security Assessment Service Provider:

- (a) is accredited by UKAS as meeting the requirements for providing audit and certification of information security management systems in accordance with ISO/IEC 27001:2017 Information Technology – Security Techniques – Information Security Management Systems) or any equivalent to that standard which updates or replaces it from time to time; and/or
- (b) holds another membership, accreditation, approval or form of professional validation that is in the opinion of the Security Sub-Committee substantially equivalent in status and effect to the arrangements described in paragraph (a).

G9.7 The requirement specified in this Section G9.7 is that the DCC Independent Security Assessment Service Provider:

- (a) employs consultants who are assured under an official cyber security qualification scheme recognised by NCSC or the UK Cyber Security Council or UKAS and which is approved by the Security Sub-Committee at levels equivalent to 'Chartered', 'Principal', 'Lead' or 'Senior Practitioner' in either 'Security and Information Risk Advisor' or 'Information Assurance Auditor' roles; and
- (b) engages those individuals as its lead auditors for the purposes of carrying out all security assessments in accordance with this Section G7.

Independence Requirement

G9.8 The DCC Independent Security Assurance Service Provider shall be treated as suitably independent in accordance with this Section G9.8 only if it satisfies:

- (a) the requirements specified in Section G9.9; and
- (b) the requirement specified in Section G9.10.

G9.9 For the purposes of Sections G9.9 and G9.10:

- (a) the DCC must be independent from the DCC Independent Security Assessment Service Provider in carrying out functions under this Section G9; and

- (b) all of the DCC's Service Providers must be independent from the DCC Independent Security Assessment Service Provider in carrying out its functions to assess the DCC's compliance with its obligations as the DCC under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.10 The requirements specified in this Section G9.10 are that:

- (a) neither the DCC or any of its subsidiaries, and no DCC Service Provider or any of its subsidiaries, holds or acquires any investment by way of shares, securities or other financial rights or interests in the DCC Independent Security Assessment Service Provider;
- (b) no director of the DCC and no director of any DCC Service Provider, is or becomes a director or employee of, or holds or acquires any investment by way of shares, securities or other financial rights or interests in, the DCC Independent Security Assessment Service Provider; and
- (c) the DCC Independent Security Assessment Service Provider does not hold or acquire a participating interest (as defined in section 421A of the Financial Services and Markets Act 2000) in the DCC or any of the DCC's Service Providers, (for these purposes references to the DCC's Service Providers shall not include the DCC Independent Security Assessment Service Provider where it acts in that capacity).

G9.11 The requirement specified in this Section G9.11 is that the DCC Independent Security Assessment Service Provider is able to demonstrate to the satisfaction of the Security Sub-Committee that it has in place arrangements to ensure that it will at all times act independently of any commercial relationship that it has, has had, or may in future have with the DCC or the DCC's Service Providers (and for these purpose a 'commercial relationship' shall include a relationship established by virtue of the DCC Independent Security Assessment Service Provider itself being a DCC Service Provider to the DCC).

Compliance of the DCC Independent Security Assessment Service Provider

G9.12 The Security Sub-Committee shall advise the DCC of any performance failures or non-compliance with the SEC obligations on the part of the DCC Independent Security Assessment Service Provider to enable the DCC to ensure that the DCC Independent Security Assessment Service Provider carries out its functions in accordance with the provisions of this Section G12.

DCC: Duty to Cooperate in Assessment

G9.13 The DCC shall do all such things as may be reasonably requested by the Security Sub-Committee, or by any person acting on behalf of or at the request of the Security Sub-Committee (including in particular the DCC Independent Security Assessment Service Provider), for the purposes of facilitating an assessment of the DCC's compliance with its obligations under Sections G2 and G4 to G6 or DCC Licence Condition 8 (Security Controls for the Authorised Business) or SEC Appendix Z Sections 6 and 7 and any CPA Certificate Remedial Plan.

G9.14 For the purposes of Section G9.13, the DCC shall provide the DCC Independent Security Assessment Service Provider with:

- (a) all such Data as may reasonably be requested, within such times and in such format as may reasonably be specified;
- (b) all such other forms of cooperation as may reasonably be requested, including in particular:
 - (i) access at all reasonable times to such parts of the premises of the DCC or its Service Providers as are used for, and such persons engaged by the DCC as carry out or are authorised to carry out, any activities related to its compliance with its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7; and
 - (ii) such cooperation as may reasonably be requested by the DCC Independent Security Assessment Services Provider for the purposes of carrying out any security assurance assessment in accordance with this Section G9.

Categories of DCC Security Assessment

G9.15 For the purposes of this Section G9, there shall be the following two categories of security assessment:

- (a) a Full DCC Security Assessment (as further described in Section G9.16);
- (b) a Follow-up DCC Security Assessment (as further described in Section G9.17).

G9.16 A **"Full DCC Security Assessment"** shall be an assessment carried out by the DCC Independent Security Assessment Service Provider in respect of the DCC and its Service Providers to identify the extent to which the DCC is compliant with each of its obligations under Sections G2 and G4 to G6 and DCC Licence Condition 8 (Security Controls for the Authorised Business) and SEC Appendix Z Sections 6 and 7.

G9.17 A **"Follow-up DCC Security Assessment"** shall be an assessment carried out by the DCC Independent Security Assessment Service Provider, following a DCC Security Assessment, in accordance with the provisions of Section G9.25.

DCC Security Assessments: General Procedure

DCC Security Assessment Methodology

G9.18 Each DCC Security Assessment carried out by the DCC Independent Security Assessment Service Provider shall be carried out in accordance with the Security Controls Framework developed as defined in G7.19(a).

The DCC Security Assessment Report

G9.19 Following the completion of a DCC Security Assessment, the DCC Independent Security Assessment Service Provider shall, in discussion with the DCC, produce a written report (a **"DCC Security Assessment Report"**) which shall:

- (a) set out the findings of the DCC Independent Security Assessment Service Provider on all the matters within the scope of the DCC Security Assessment;
- (b) specify any instances of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 which have been identified by the DCC Independent Security Assessment Service Provider;
- (c) specify any instances of actual or potential non-compliance of the DCC with its obligations under DCC Licence Condition 8 (Security Controls for the Authorised Business);
- (d) specify any instances of actual or potential non-compliance of the DCC with its obligations under SEC Appendix Z, Sections 6 and 7; and
- (e) set out the evidence which, in the opinion of the DCC Independent Security Assessment Service Provider, establishes each of the instances of actual or potential non-compliance which it has identified.

G9.20 The DCC Independent Security Assessment Service Provider shall submit a copy of each DCC Security Assessment Report to the Security Sub-Committee and to the DCC.

The DCC Security Assessment Response

G9.21 Following the receipt by the DCC of a DCC Security Assessment Report which relates to it, the DCC shall as soon as reasonably practicable, and in any event by no later than such date as the Security Sub-Committee may specify:

- (a) produce a written response to that report (a "**DCC Security Assessment Response**") which addresses the findings set out in the report; and
- (b) submit a copy of that response to the Security Sub-Committee and the DCC Independent Security Assessment Service Provider.

G9.22 Where a DCC Security Assessment Report following a Full DCC Security Assessment, specifies any instance of actual or potential non-compliance of the DCC with its obligations under Sections G2 and G4 to G6 and/or with DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or with SEC Appendix Z, Sections 6 and 7, the DCC shall ensure that its DCC Security Assessment response includes the matters referred to in Section G9.23.

G9.23 The matters referred to in this Section are that the DCC Security Assessment Response:

- (a) indicates whether the DCC accepts the relevant findings of the DCC Independent Security Assessment Service Provider and, where it does not, explains why this is the case;
- (b) sets out any steps that the DCC has taken or proposes to take in order to remedy and/or mitigate the actual or potential non-compliance or the increase in security risk (as the case may be) specified in the DCC Security Assessment Report; and

- (c) identifies a timetable within which the DCC proposes to take any such steps that have not already been taken.

G9.24 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), the Security Sub-Committee (having considered the advice of the DCC Independent Security Assessment Service Provider) shall review that response and either:

- (a) notify the DCC that it accepts that the steps that the DCC proposes to take, and the timetable within which it proposes to take them, are appropriate to remedy and/or mitigate the actual or potential non-compliance or increase in security risk (as the case may be) specified in the DCC Security Assessment Report; or
- (b) seek to agree with the DCC such alternative steps and/or timetable as would, in the opinion of the Security Sub-Committee, be more appropriate for that purpose.

G9.25 Where a DCC Security Assessment Response sets out any steps that the DCC proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the DCC in accordance with Section G9.24(b), the DCC shall:

- (a) take the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) report to the Security Sub-Committee on:
 - (i) its progress in taking those steps, at any such intervals or by any such dates as the Security Sub-Committee may specify;
 - (ii) the completion of those steps in accordance with the timetable; and
 - (iii) any failure to complete any of those steps in accordance with the timetable, specifying the reasons for that failure.

Follow-up Security Assessment

G9.26 Where a DCC Security Assessment Response sets out any steps that the User proposes to take in accordance with Section G9.23(b), and where those steps and the timetable within which it proposes to take them are accepted by the Security Sub-Committee, or alternative steps and/or an alternative timetable are agreed between it and the User in accordance with Section G9.24(b), the DCC Independent Security Assessment Service Provider shall, at the request of the Security Sub-Committee (and by such date as it may specify), carry out a Follow-up Security Assessment of the DCC to:

- (a) identify the extent to which the DCC has taken the steps that have been accepted or agreed (as the case may be) within the timetable that has been accepted or agreed (as the case may be); and
- (b) assess any other matters related to the DCC Security Assessment Response that are specified by the Security Sub-Committee.

DCC Security Assessments: Further Provisions

G9.27 The DCC Independent Security Assessment Service Provider may, in carrying out any DCC Security Assessment, take into account any relevant security accreditation or certification held by the DCC.

Setting the Compliance Status

G9.28 Following the completion of a Full DCC Security Assessment, the Security Sub-Committee shall consider the DCC Security Assessment Report and the DCC Security Assessment Response.

G9.29 The Security Sub-Committee shall identify whether any remaining non-compliances that exist with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7 and shall, where appropriate:

- (a) note and record that there are no non-compliances; or
- (b) note and record the specific non-compliances that need to be addressed.

G9.30 Where the Security Sub-Committee identifies remaining non-compliances that exist with Section G2 and G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z Sections 6 and 7, it shall:

- (a) require the DCC to take the steps set out in Section G9.24: or
- (b) require a Follow-up Security Assessment as set out in Section G9.26.

G9.31 Where the Security Sub-Committee identifies any remaining non-compliances with Section G2 or G4 to G6 and/or the DCC Licence Condition 8 (Security Controls for the Authorised Business) and/or SEC Appendix Z, Sections 6 and 7, it shall notify the Panel as required by G9.37(b).

CPA Certificate Remedial Plan Preparation

G9.32 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans. The DCC Independent Security Assessment Service Provider will assess the DCC's compliance with Appendix Z Section 6 and Section 7.

Disagreement with Security Sub-Committee Decisions

G9.33 Where the DCC disagrees with any decision made by the Security Sub-Committee in relation to it under Section G9.28 to G9.31, it may appeal that decision to the Panel. If the DCC disagrees with any decision made by the Panel, it may appeal that decision to the Authority and the determination of the Authority shall be final and binding for the purposes of the Code.

Events of Default

G9.34 In relation to an Event of Default which consists of a material breach by the DCC of any of the obligations referred to at Section G9.2(c), the provisions of Sections M8.2 to M8.4 shall apply subject to the provisions of Sections G9.35 to G9.41.

G9.35 For the purposes of Sections M8.2 to M8.4 as they apply pursuant to Section G9.34, an Event of Default shall (notwithstanding the ordinary definition thereof) be deemed to have occurred in respect of the DCC where it is in material breach of any of the obligations referred to at Section G9.2(d) (provided that Sections M8.4(e), (f) and (g) shall never apply to the DCC).

G9.36 Where in accordance with Section M8.2 the Panel receives notification that the DCC is in material breach of any of the obligations referred to at Section G9.2(d), it shall refer the matter to the Security Sub-Committee.

G9.37 On any such referral the Security Sub-Committee may investigate the matter in accordance with Section M8.3 as if the references in that Section to the “Panel” were to the “Security Sub-Committee”.

G9.38 Where the Security Sub-Committee has:

- (a) carried out an investigation in accordance with Section M8.3; or
- (b) received a DCC Security Assessment Report concluding that the DCC is in actual or potential non-compliance with any of the obligations referred to at Section G9.2(c),

the Security Sub-Committee shall consider the information available to it and, where it considers that actual non-compliance with any of the obligations referred to at Section G9.2(c) has occurred, shall refer the matter to the Panel for it to determine whether that non-compliance constitutes an Event of Default.

G9.39 Where the Panel determines that an Event of Default has occurred, it shall:

- (a) notify the DCC and any other Party it considers may have been affected by the Event of Default; and
- (b) determine the appropriate steps to take in accordance with Section M8.4.

G9.40 Where the Panel is considering what steps to take in accordance with Section M8.4, it may request and consider the advice of the Security Sub-Committee.

G9.41 Where the Panel determines that the DCC is required to give effect to a remedial action plan in accordance with Section M8.4(d) that plan must be approved by the Panel (having regard to any advice of the Security Sub-Committee).

CPA Certificate Remedial Plan Preparation

G9.42 The DCC shall ensure that it has in place (and periodically reviews) a policy for creating and managing compliance with CPA Certificate Remedial Plans.

Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

These changes have been redlined against Appendix AC version 7.0.

Add Section 5.19 as follows:

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

- 5.1 This Clause 5 applies only to SMETS2+ Devices.
- 5.2 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, the DCC shall ensure that:
- (a) the Communications Hub Function re-generates its Private Keys, and that Device Certificates containing the associated new Public Keys are stored on the Device; and
 - (b) the information from at least one of the Organisation Certificates that comprise the Communications Hub Function's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate).
- 5.3 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Smart Meter, a Standalone Auxiliary Proportional Controller or a Gas Proxy Function, the Responsible Supplier shall, in relation to each such Device, ensure that:
- (a) the Device Security Credentials which pertain to the Network Parties are:
 - (i) in the case of those which pertain to the Electricity Network Party, those of the Electricity Distributor; and
 - (ii) in the case of those which pertain to the Gas Network Party, those of the Gas Transporter (or, if they are not available in the SMKI Repository, the Device Security Credentials which pertain to the Gas Network Party shall be populated with information from the Organisation Certificates Issued to the DCC and referred to in Sections L3.23(f) (the DCC (access-Control-Broker) – digitalSignature Certificate) and L3.23(g) (the DCC (access-Control-Broker) – keyAgreement Certificate));
 - (b) the Device re-generates its Private Keys, and that the Device Certificates containing the associated new Public Keys are stored on the Device; and
 - (c) in the case of a Smart Meter and a Standalone Auxiliary Proportional Controller, information from at least one of the Organisation Certificates that comprise the Device's Device Security Credentials is replaced (provided that for such purposes the information from an Organisation Certificate may be replaced with that from the same Organisation Certificate).
- 5.4 As soon as reasonably practicable (and in any event within 7 days) following the Commissioning of a Communications Hub Function, Gas Proxy Function, Standalone

Managed by

Auxiliary Proportional Controller or Smart Meter, the DCC shall interrogate the Device to ascertain whether the Device's recovery Trust Anchor Cell is populated with Device Security Credentials that pertain to a DCC Recovery Certificate. For Devices Commissioned before Service Release 1.3 (or such later date as may be directed by the SofS for the purposes of this Clause 5.4), the reference to the period of 7 days following Commissioning shall apply as 7 days following Service Release 1.3 (or 7 days following any later date directed by the SofS).

- 5.5 The DCC shall monitor Commands sent to Devices and the associated Responses from Devices and, based on the information available to it, record the information set out in Clause 5.8 in relation to each Device identified in Clause 5.7 (the **"Post Commissioning Information"**).
- 5.6 The DCC shall ensure that the Post Commissioning Information is updated on a daily basis to reflect the most accurate and up-to-date information available to the DCC at the time of the update.
- 5.7 For the purposes of Clause 5.5, the relevant Devices include any Communications Hub Function, Gas Proxy Function, a Standalone Auxiliary Proportional Controller or Smart Meter which has an SMI Status of 'commissioned', has been Commissioned for a period of 7 days or more, and in relation to which one or both of the following applies:
 - (a) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.4; and/or
 - (b) the DCC has successfully carried out the interrogation of the Device pursuant to Clause 5.4 and has identified that the Device's recovery Trust Anchor Cell is not populated with Device Security Credentials that pertain to a DCC Recovery Certificate.
- 5.8 For the purposes of Clause 5.5, the Post Commissioning Information to be recorded in relation to each relevant Device shall include:
 - (a) the Device ID and Device Type;
 - (b) the date upon which the Device was Commissioned;
 - (c) which of Clauses 5.7 (a) and/or (b) applies;
 - (d) other than in the case of Communications Hub Functions, the Responsible Supplier at the time the Post Commissioning Information for the Device was most recently updated;
 - (e) other than in the case of Communications Hub Functions, the Supplier Party that sent the Service Request that resulted in the Commissioning of the Device; and
 - (f) the date on which the Post Commissioning Information for the Device was most recently updated.
- 5.9 As soon as reasonably practicable following the end of each month, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that month, compile and provide (in an electronic format) to the Panel, the Security Sub-Committee and the Authority a report which includes the following information:

- (a) the month to which the report relates;
- (b) for each Party that is the Responsible Supplier for any Smart Meter or Gas Proxy Function that is listed in the Post Commissioning Information for that month (or was listed in the information for the previous month):
 - (i) the total number of Devices of each Device Type listed in the Post Commissioning Information for that month for which that Party is the Responsible Supplier;
 - (ii) the number of such Devices of each Device Type that have been added since the last monthly report;
 - (iii) the number of such Devices of each Device Type that have been removed since the last monthly report;
 - (iv) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates;
 - (v) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and
 - (vi) the number of such Devices of each Device Type that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates; and
- (c) in respect of Communications Hub Functions:
 - (i) the total number of Communications Hub Functions listed in the Post Commissioning Information;
 - (ii) the number of Communications Hub Functions that have been added since the last monthly report;
 - (iii) the number of Communications Hub Functions that have been removed since the last monthly report;
 - (iv) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous month and remain listed in the information for the month to which the report relates;
 - (v) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous three months and remain listed in the information for the month to which the report relates; and
 - (vi) the number of Communications Hub Functions that were listed in the Post Commissioning Information for the previous six months and remain listed in the information for the month to which the report relates.

5.10 As soon as reasonably practicable following the end of each day, the DCC shall, based upon the Post Commissioning Information prevailing at the end of that day, compile and

make available to each Supplier Party (via a secure electronic means for a period of at least 30 days following the day to which the report relates) a report which includes the following information in relation to Devices (other than Communications Hub Functions) listed in the Post Commissioning Information for which that Supplier Party was the Responsible Supplier on that day:

- (a) the Device ID and Device Type of each such Device;
- (b) the date on which the Post Commissioning Information for each such Device was most recently updated;
- (c) the date upon which each such Device was Commissioned; and
- (d) which of Clause 5.7 (a) and/or (b) applies in relation to each such Device.

5.11 Where requested by the Panel or the Authority, the DCC shall, as soon as reasonably practicable following any such request, provide to the Panel and/or the Authority (in an electronic format) copies of the reports referred to in Clause 5.10. Where requested by the Panel or the Authority, DCC shall additionally include in any such report the information referred to in Clause 5.8(e) in relation to each Device included in any such report.

5.12 The DCC shall ensure that each report provided under Clause 5.9, 5.10 or 5.11 is clearly marked as being “confidential”.

5.13 Where the DCC is aware that:

- (a) either or both of the steps in Clauses 5.2 (a) and/or (b) have not been carried out within 7 days following the Commissioning of a Communications Hub Function; and/or
- (b) either of Clause 5.7(a) or (b) applies in relation to a Communications Hub Function,

then the DCC shall raise an Incident in accordance with the Incident Management Policy.

5.14 Where, in relation to a Gas Proxy Function, Standalone Auxiliary Proportional Controller or a Smart Meter, a Supplier Party is aware that:

- (a) either or both of the steps in Clauses 5.3 (b) and/or (in the case of Smart Meters and Standalone Auxiliary Proportional Controllers only) 5.3(c) have not been carried out within 7 days following the Commissioning of the Device; and/or
- (b) the DCC has failed successfully to carry out the interrogation of the Device pursuant to Clause 5.4, and the Supplier has (within a period of 14 days following the Commissioning of the Device) also failed to successfully carry out the relevant interrogation,

then the Supplier Party shall not send Service Requests requesting that the DCC sends communications to that Device other than for the purposes of: (i) completing those steps; (ii) replacing the Device Security Credentials held on the Device in response to a change of supplier; or (iii) maintaining an energy supply to the relevant premises.

5.15 Where the Responsible Supplier for a Gas Proxy Function, Standalone Auxiliary Proportional Controller or Smart Meter becomes aware that the Device does not have a

recovery Trust Anchor Cell that is populated with Device Security Credentials that pertain to a DCC Recovery Certificate, then that Responsible Supplier shall (subject to Clause 5.17), as soon as reasonably practicable thereafter: other than in the case of a Gas Proxy Function, replace the Device; or, in the case of a Gas Proxy Function, replace the Communications Hub of which that Gas Proxy Function forms part.

5.16 Where a Communications Hub is returned to the DCC:

- (a) following its replacement pursuant to Clause 5.13 or 5.15; or
- (b) a Communications Hub is returned following replacement because it was not possible to interrogate the Gas Proxy Function pursuant to Clause 5.14(b),

then the Supplier Party returning the Communications Hub may (under and subject to Section F9 (Categories of Communications Hub Responsibility)) specify the reason for return as being a CH Defect.

5.17 A Responsible Supplier shall not replace a Device under Clause 5.15 where the reason that the relevant steps cannot be completed is an inability to communicate with a Device as a result of the SM WAN being unavailable.

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 48 hours 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

Managed by

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 and Expired Certificates Preliminary Impact Assessment (PIA)

Version:	0.21
Date:	24th July 2024
Author:	DCC
Classification:	DCC PUBLIC

Contents

1	Executive Summary	4
2	Document History	5
2.1	Revision History	5
2.2	Associated Documents	5
2.3	Document Information.....	5
3	Context and Requirements	6
3.1	Current Arrangements.....	6
3.2	What is the Issue?	6
3.3	Impact of the Issue	7
3.4	Business Requirements	7
4	Description of Solution	10
4.1	DSP Background	10
4.2	Impacts on DSP	10
4.3	Impacts on ECOS Provider (Accenture).....	11
5	Impact on DCC Systems, Processes and People	12
5.1	Service User Impact.....	12
5.2	Security Impact, DSP and ECOS.....	12
5.3	Technical Specifications	12
5.4	DSP Component Impact	12
5.5	Infrastructure Impact	12
5.6	Transition into Service	12
5.7	Service Impact	12
5.8	Data Science and Analytics Team	13
6	Implementation Timescales and Approach.....	14
6.1	Implementation Approach.....	14
6.2	Testing and Acceptance.....	14
6.2.1	DSP Pre-Integration Testing (PIT).....	14
6.2.2	DSP System Integration Testing (SIT).....	14
6.2.3	DSP User Integration Testing.....	15
6.2.4	ECOS Change Testing.....	15
7	Costs and Charges.....	16
7.1	Design, Build and Testing Cost Impact.....	16
7.2	Contract and Schedule Impacts.....	16
8	Risk, Assumptions, Issues, and Dependencies	17



8.1	Risks.....	17
8.2	Assumptions.....	17
Appendix A: Glossary		18

1 Executive Summary

The Change Board are asked to approve the following:

- Cost to complete the Full Impact Assessment of **£17,636**.
- The timescales to complete the Full Impact Assessment of 40 Working Days.
- ROM costs for SECMP0268, up to the end of Pre-Integration Testing (PIT) of £10,000 to £160,000.
- The Data Service Provider (DSP), ECOS Service Provider, and DCC DS&A team are impacted by this Modification.

Problem Statement

Currently the obligations to rotate ACB and 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 Access Control Broker (ACB) rotation, but this has been managed informally with the Service Provider. 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.

Modification Benefits

The first aim of this Modification is to ensure devices do not hold extended life manufacturing pack certificates delivered as part of the manufacturing pack programme for an extended period of time.

This change will mandate post-commissioning obligations of DCC Service Providers and enable full DCC reporting around Service Provider performance.

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
19/07/2024	0.1	Initial version, for DCC internal review
24/07/2024	0.21	DCC internal review completed

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.	Annex A - MP268 Business Requirements v0.4	SECAS	02/07/2024

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 26th March, 2024.

The technical solution for this Modification is often referred to as "Post Commissioning Obligation on Access Control Broker (ACB) and Enduring Change of Supplier (ECOS) Providers," but the Modification has been retained for continuity.

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 I&C.

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 Installation and Commissioning (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.

Commented [WD(1)]: Should this be 2051? 2026 +25?

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 Q4 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 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 comprised 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

This solution will be applied to SMETS2+ Devices. Further detail for each requirement follows.

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: 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 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.

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

4.1 DSP Background

Currently, the DSP can replace ACB certificates on devices when “convenient” with respect to other operational considerations. This Modification mandates replacement between 2 and 23 days after the commissioning of a device, and with the intended solution the DSP shall be able to:

1. rotate the ACB certificates on a newly commissioned device away from the manufacturing ACB certificates to a set of Operational ACB certificates;
2. rotate the ACB certificates no sooner than 48 hours after the device is commissioned; and
3. for cases where rotation has failed, attempt to rotate the ACB certificates for up to 23 days after the device is commissioned.

4.2 Impacts on DSP

The DSP solution already provides a capability to “manually” rotate ACB certificates on devices. This capability has been used successfully to move part of the device estate away from manufacturing ACB certificates to operational (aka Business as Usual) ACB certificates, but is not suitable in the current state to deal with the large number of devices impacted by this Modification.

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

- automatically initiate ACB certificate replacement as a scheduled daily task;
- select devices which currently hold a manufacturing ACB certificate for which 48 hours has passed since the device became commissioned;
- replace the manufacturing ACB certificate on these devices with a specified operational ACB certificate; and
- if unsuccessful, continue to attempt ACB certificate replacement every seven days for up to three re-attempts (21 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 days);
- maximum retry attempts (set to three retries); and
- maximum ACB rotations per day (a default value will be agreed as part of the design stage)

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 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); and
- 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.

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

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. This is called config file 2.0:

Config File 1.0

- 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 this config file will not be implemented at any stage.
- Failed migrated devices will be covered by no-comms projects.

Config File 1.5

- 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.

Config File 2.0

- 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.

5 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0268 solution on DCC Services and Interfaces that impact Users and/or Parties.

5.1 Service User Impact

The only very low risk impact is the impact to an Install & Commission SR6.21 handover of DCC device happening at the same time as ACB swap out. There is no impact on COS as the ECOS provider can use registration data to ensure COS swap out is not delivered at the same time as an ECOS migration or rotation.

5.2 Security Impact, DSP and ECOS

Changes to the timing of message processing do not have a security impact. Further, there are no interface changes to the solution and no new infrastructure is being introduced in support of the solution. As such, there is no perceived need for penetration testing nor any Protective Monitoring changes. The security impact of this Modification should be limited to security assurance throughout the implementation phase. This assurance includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

A more detailed assessment of Security impact will be carried out as part of the Full Impact Assessment.

5.3 Technical Specifications

No changes to any technical specifications required for this modification. This is not a design change.

5.4 DSP Component Impact

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

5.5 Infrastructure Impact

There will be no change to the infrastructure design because of this Modification. Additional processing and storage will be required. However, they are not sufficiently large to warrant the procurement of additional compute power or storage.

This Modification does not impact the DSP resilience or DR implementation.

5.6 Transition into Service

It is assumed that the activities required for the DSP Transition to Operations (TTO) will be minimal.

Configuration changes to ECOS will be part of this phase but also will be small.

5.7 Service Impact

While the SEC currently lays out no obligation on the replacement of ACB certificates, the DSP Application Management Services (AMS) team has implemented a capability to perform rotation on ACB certificates. The DSP have proposed changes to the tools used to perform the rotation on ACB certificates.

The Modification will not have a material impact on system performance and as such, the indicative price for the scope of supply as set out in this document does not include any performance testing.

5.8 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. Details will be established as part of the FIA. Current data reports align to MP268, they simply become mandatory.

6 Implementation Timescales and Approach

This Modification will be implemented in a future SEC Release. Design, Build, and PIT is expected to take approximately three months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Implementation Approach

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

6.2 Testing and Acceptance

For each SEC System Release, there is a Post-PIT Change Request that provides the SIT and UIT response for the SEC Release as a whole, covering the testing of individual changes in the scope of the release, as well as activities that are common to all changes in the scope (e.g. test plans, system regression testing, test management and governance).

6.2.1 DSP Pre-Integration Testing (PIT)

The System Test Team will create a System Test to check the selection of devices for ACB replacement with recently installed devices being prioritised. The System Test Team will also regression test other parts of ACB replacement to ensure there are no unintended consequences. The Modification will be subject to Factory Acceptance Testing to demonstrate the implementation to the DCC in accordance with established SEC System Release processes. The outcome of PIT phase testing shall be documented in the form of a Test Completion Report.

6.2.2 DSP System Integration Testing (SIT)

The Modification will be delivered as part of a SEC System Release. The SIT scope of this Modification comprises:

- for each set, Install and Commission of an ESME, GSME and PPMID;
- verifying, at the time configured from commissioning each device, that a script is executed to initiate the certificate rotation;
- verifying that the certificates are rotated successfully through submission of a Service Request and querying the Smart Metering Inventory; and
- decommissioning.

To carry out the scope of testing, a device set for each CSP (three) is required. This comprises:

- a Toshiba (CSP South and Central) Comms Hub with ESME, GSME and PPMID;
- an EDM I (CSP North) Comms Hub, with ESME, GSME and PPMID; and
- a 4G Toshiba (NEWAN) Comms Hub with ESME, GSME and PPMID.

It is anticipated that one test scenario and script will need to be created to test this Modification, with approximately 133 tests to be executed to verify. DCC will challenge this assessment as part of the FIA.

Note that SIT costs are not included in the PIA costs and effort calculations.

6.2.3 DSP User Integration Testing

The UIT scope of this Modification comprises:

- for each set, Install and Commission an ESME, GSME, and PPMID;
- verifying, at the time configured from commissioning each device, a script is executed to initiate the certificate rotation;
- verifying that the certificates are rotated successfully through submission of a Service Request and querying the Smart Metering Inventory; and
- decommissioning.

To carry out the scope of testing, a device set for each CSP is required. This comprises:

- a Toshiba (CSP South and Central) Comms Hub with ESME, GSME and PPMID;
- an EDM I (CSP North) Comms Hub, with ESME, GSME and PPMID; and
- a 4G Toshiba (NEWAN) Comms Hub with ESME, GSME and PPMID.

It is estimated that for this Modification, approximately 100 tests will be executed within the UIT scope to verify. While the UIT team will aim to use the UIT Automation Framework where possible, some tests required to verify the Modification will need to be carried out manually. DCC will challenge these estimates as part of the FIA.

Note that UIT costs are not included in the PIA costs and effort calculations.

6.2.4 ECOS Change Testing

This solution is already tested by DCC, with no impact on PIT, SIT, or UIT. The configuration change would be implemented in the production environment via a maintenance window.

7 Costs and Charges

The scope of supply under this PIA includes design, development (build), system testing, and performance testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional and non-functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change. As a result, the final offer price may result in a variation.

7.1 Design, Build and Testing Cost Impact

The table below details the cost of delivering the changes and Services required by all impacted Service Providers to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

£	Design, Build and PIT
SECMP0268	£ 10,000 to £160,000

Although not included in this PIA, it is expected that there will be integration testing costs associated with this Modification. If the targeted SEC Release date includes another Modification or Change Request with regression testing, that cost will be shared equally between the two (or more) changes, and the cost of Integration Testing will come down.

Given the low-cost to the ECOS provider, it is likely that a formal FIA assessment will not be required or requested.

Based on the existing requirements, the total fixed price cost for a Full Impact Assessment by the DSP and the DCC DS&A team is **£17,636** and would be expected to be completed in 40 Working Days.

7.2 Contract and Schedule Impacts

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

Updates to the DSP Design Baseline (Schedule 4.1) and Payment milestones (Schedules 6.1 and 7.1) are anticipated.

8 Risk, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified.

8.1 Risks

Ref.	Risk and Impact
MP268-DR1	the impact to Install & Commissioning SR6.21 handover of DCC device happening at the same time as ACB swap out

8.2 Assumptions

Ref.	Assumption
MP268-AA1	As the ECoS (Accenture) solution is tested in SIT and UIT, it is ready to implement in production as soon as DCC Operations are happy reporting is in place in monitor ECOS auto rotations via config file 2.0.
MP268-AD2	The replacement obligation will not apply where communication with a device is not possible.
MP268-AD3	This Modification will be required for SIT and UIT testing after the CH&N has been delivered into Production, and therefore SIT and UIT scope must also include a 4G Comms Hub

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
DUIS	DCC User Interface Specification
ECOS, ECoS	Enduring Change of Supplier
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
GSME	Gas Smart Metering Equipment
GUID	Global Unique Identifier
I&C	Install and Commission
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
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	-