Data Communications Company

SEC Modification Proposal, SECMP0268, DCC CR5407

Certificate Rotation Post Commissioning

Full Impact Assessment (FIA)

Version:	**0.2**
Date:	**22nd November 2024**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Contents

1 Executive Summary 3
2 Document History 4
2.1 Revision History 4
2.2 Associated Documents 4
2.3 Document Information 4
3 Context and Requirements 5
3.1 Current Arrangements 5
3.2 What is the Issue? 5
3.3 Impact of the Issue 6
3.4 Business Requirements 6
4 Description of Solution 9
4.1 DSP Technical Solution 9
4.2 Application Components 10
4.2.1 Technical Specifications 10
4.2.2 Key Management 10
4.2.3 Data Management 10
4.2.4 Infrastructure Impact 10
4.2.5 Other DSP Changes 10
4.3 Impacts on ECOS Provider (Accenture) 11
4.4 Data Science and Analytics Team 11
5 Implementation Timescales and Approach 12
5.1 DSP Pre-Integration Testing 12
5.2 System Integration Testing (SIT) 12
5.3 User Integration Testing (UIT) 13
5.4 Changes to DS&A Reporting 13
5.5 Transition to Operations 13
6 Costs and Charges 14
6.1 Changes to the Agreement 15
Appendix A: Glossary 16

1 Executive Summary

The Change Board are asked to approve the following:

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

Problem Statement

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

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

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

Modification Benefits

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

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

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

2 Document History

2.1 Revision History

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

2.2 Associated Documents

This document is associated with the following documents:

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

References are shown in this format, [1].

2.3 Document Information

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

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

The FIA was requested on 30th September 2024.

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

3 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by SECAS, the Proposer, and the Working Group, and have been validated by SSC and TABASC.

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

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

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

3.1 Current Arrangements

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

The Organisation Certificates contained within the first (and current) manufacturing pack will expire in 2026. SECMP0261 ‘Extending the Organisation Certificate Validity Period’ was implemented in February 2024, and allows the DCC to align the new Organisation Certificate with the existing Issuing Organisation Certification Authority (OCA) Certificate which has a Validity Period of 17 years and is set to expire in 2041 to prevent a new manufacturing pack being created prematurely. Once the 2024 manufacturing pack is made available by DCC, there will be Devices installed and commissioned that contain information from an Organisation Certificate that has a Validity Period of more than ten years. However, there is no explicit requirement in the SEC specifying the post-commissioning replacement of the Organisation Certificate information, for which the DCC is responsible. Furthermore, from 2026, there will be Devices installed that may have an expired or revoked Certificate in the Device Trust Anchor cell (due to them containing the original manufacturing pack Certificates). Currently there is no explicit requirement in the SEC to specify the duties on the DCC and Users when a Certificate on a Device has expired or been revoked.

3.2 What is the Issue?

The DCC issues a list of Certificates to Device Manufacturers for them to place into the Trust Anchor Cells on their Devices. This is known as the manufacturing pack. This ensures that those Devices can be initially communicated with during I&C. When a Device is installed, it will have Certificate information that assists in the I&C process. This is so that when the Devices are installed the Service Reference Variants (SRVs) can be sent to and received from the responsible Parties.

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

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

3.3 Impact of the Issue

Devices manufactured after the 2024 manufacturing pack release may contain information from an Organisation Certificate with a Validity Period exceeding ten years. The SMKI PMA approved the SECMP261 solution to allow for an extended Validity Period, provided that the information from that Organisation Certificate is replaced as soon as reasonably practicable following I&C. The information will be replaced with that of a Certificate with a ten-year Validity Period.

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

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

3.4 Business Requirements

The business requirements are as follows.

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

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

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

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

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

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

Requirement 2: The Proposed Solution must resolve the issue for three scenarios:

- **Change of Supplier (CoS) when the gaining Supplier cannot rectify the issue through manual intervention.**
- **When the previous Supplier has ceased to trade, and a Supplier of Last Resort (SoLR) has been nominated.**
- **When the Device does not support the process of Service Reference Variant (SRV) 6.24.2 ‘Retrieve Device Security Credentials (Device)’.**

The Proposer has highlighted the three most common scenarios that are impacted by Device certificate misalignment. In each scenario, the Supplier will only be able to send SRV 6.24.2 ‘Retrieve Device Security Credentials (Device)’ to the Device, meaning that the consumer will not benefit from smart functionality. Although these are the three most common scenarios, the Proposer has indicated that there may be other instances where Device certificate misalignment occurs.

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

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

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

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

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

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

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

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

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

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

DCC proposes that the reporting contains the following attributes:

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

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

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

4 Description of Solution

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

4.1 DSP Technical Solution

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

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

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

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

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

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

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

The “exclusion list” is a feature of the existing ACB certificate replacement capability, and was introduced to deal with the large proportion of PPMID devices do not properly support the ACB certificate replacement command and will always fail[1].

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

4.2 Application Components

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

4.2.1 Technical Specifications

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

4.2.2 Key Management

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

4.2.3 Data Management

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

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

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

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

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

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

4.2.4 Infrastructure Impact

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

4.2.5 Other DSP Changes

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

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

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

4.3 Impacts on ECOS Provider (Accenture)

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

Config File 1.0

- 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.

4.4 Data Science and Analytics Team

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

5 Implementation Timescales and Approach

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

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

5.1 DSP Pre-Integration Testing

The scope of this FIA includes activities required to:

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

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

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

5.2 System Integration Testing (SIT)

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

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

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

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

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

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

5.3 User Integration Testing (UIT)

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

5.4 Changes to DS&A Reporting

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

5.5 Transition to Operations

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

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

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

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

6 Costs and Charges

This section indicates the costs for all phases of application development for this Modification. Note these costs assume a release of just this SEC Modification without any other Modifications or Change Requests in the release, and without the regression testing required during the Integration Testing, which is not truly reflective of the post-PIT test costs. A separate estimate of these costs is provided by DCC.

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

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

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

6.1 Changes to the Agreement

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

- Schedule 2.1 (DCC Requirements): addition of new requirements for this change
- Schedule 3 (DCC Responsibilities): update to reflect the addition of new DCC Responsibilities
- Schedule 4.1 (DSP Solution): solution design documents
- Schedule 6.1 (Implementation Planning): addition of new milestones
- Schedule 7.1 (Charges and Payment): revisions to incorporate charges and payment

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

Other Service Providers are not impacted.

Appendix A: Glossary

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

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

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