

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