

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<br>Network Parties<br>DCC | M      |
| 4                     | Under all reasonable steps, the Relevant Subscriber will replace a revoked Certificate                                                                                                                                                                                | Suppliers<br>Network Parties<br>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<br>Network Parties<br>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                                         |