This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP134B 'SMKI Certificates relating to a SoLR event – Part 2'

Business requirements – version 0.1

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 Communication 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**
1	A new User Role is created with roles as defined in Appendix AD 'DCC User Interface Specification' (DUIS)
2	Smart Energy Code (SEC) Parties acting in that User Role can subscribe for Extensible Markup Language (XML) Signing Certificates, but not Digital Signing Keys for signing Critical Commands
3	The new User Role will only be able to send Service Request 1.6 'Update Payment Mode'. The solution should be configurable to enable other Service Request to be added to the list of SRVs that this User Role is eligible to use.
4	Parties acting in this User Role must be able to create Authorised Responsible Officers (AROs) and Senior Responsible Officers (SROs) to enable submission of Anomaly Detection Threshold (ADT) files that will allow the new User Role to send Service Requests to Devices registered to a specific Supplier
5	The content of the Service Request (for SMETS1 Devices) and Signed Pre-Command (for SMETS2+ Devices) must be checked to only accept change Payment Mode to Credit
6	The default position will be that Users in this User Role will only be able to send the Service Requests listed in requirement 3 and will only be able to do so in the event of a Supplier failure and upon specific instruction from the Authority. Additional validation is set out in this requirement.
7	The DCC should remain able to send Alerts to the Supplier after the Supplier's Certificates have been revoked (noting that they will be routed to the failed Supplier's SRP).

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

2.1.1 Set up

A new SEC Role (e.g. SolrContingency) would be created for Shared Resource Providers (SRPs) to send Commands to Devices in the event of a Supplier failure (a SoLR situation). The User Role would identify the SRP acting in this capacity and limit its capabilities in that capacity.

Users in this Role could only subscribe for an XMLSigning Certificate (so that the associated Private Key could not be used to sign Critical Commands to Smart Metering Equipment Technical

Specifications (SMETS) (1 or 2+) Devices, but it could be used to sign certain XML format Service Request).

Under normal circumstances an SRP would subscribe to such Certificates, generate associated Keys and offer its Suppliers this service in case of a Supplier failure and revocation of Certificates. It could be a requirement on relevant Suppliers to put such arrangements in place.

2.1.2 Usage

For SMETS1 Devices:

The SRP would submit Service Requests to the DCC for any Meters that might be in Prepayment Mode, where:

- the Service Request has been signed with the SRP's XML Signing Certificate relating to the SolrContingency role.

The DCC would countersign the Service Request where:

- the range of checks to verify the XML is authentically from the SRP (e.g. signature etc) are met;
- the Notified Critical Supplier ID is for an identity which previously had SMKI Certificates in the Supplier Role; and
- for Service Request 1.6 (Update Payment Mode), the contents of the Service Request sets the Payment Mode to Credit (and will disallow any attempt to set to Prepayment).

For SMETS2+ Devices:

The SRP would submit Signed Pre-Commands to the DCC for any Meters that might be in Prepayment Mode, where:

- the GBCS Payload has been signed using the former Supplier's Great Britain Companion Specification (GBCS) Digital Signing Keys; and
- the Pre-Command has been signed with the SRP's XML Signing Certificate relating to the SolrContingency role.

The DCC would only add its Message Authentication Code (MAC) to such Commands where:

- The range of checks to verify the XML is authentically from the SRP (e.g. signature etc) are met;
- The Business Originator ID is for an identity which previously had SMKI Certificates in the Supplier Role; and
- For Service Request 1.6 (Update Payment Mode), the contents of the Service Request sets the Payment Mode to Credit (and will disallow any attempt to set to Prepayment).

2.2 Requirement 1: New 'SolrContingency' User Role

A new User Role is created as set up in SEC Appendix AD 'DCC User Interface Specification' (DUIS).

2.3 Requirement 2: New User Role eligible to subscribe for xmlSign Certificate

SEC Parties acting in this new User Role can subscribe for Organisation Certificates with the existing Remote Party Role of xmlSign, but not Digital Signing Keys for signing Critical Commands.

2.4 Requirement 3: Access Control restricts the new User Role's Use of Service Requests

The new User Role will be an eligible User of a limited set of Service Requests. The initial list will contain only Service Request 1.6 Update Payment Mode.

The list is to be confirmed through the modification process. The DCC's solution should also allow this list to be easily configured at any time.

2.5 Requirement 4: New User Role can create AROs & SROs to enable ADT submission

Parties acting in this new User Role must be able to create AROs and SROs to enable submission of ADT files that will allow the new User Role to send Service Requests to Devices registered to a specific Supplier.

2.6 Requirement 5: Service Request / Signed Pre-Command Content Checks

The content of Service Request 1.6 'Update Payment Mode' will be checked to ensure that only attempts to change the Payment Mode to Credit are further processed. Any attempt to change a meter's Payment Mode to Prepayment will be rejected (similar to it failing an Anomaly Detection Attribute (ADA) check).

For SMETS1 meters, this check will be performed on the Service Request from the SRP, acting in the User Role of SolrContingency.

For SMETS2+ meters, this check will be performed on the Signed Pre-Command from the SRP, acting in the User Role of SolrContingency.

2.7 Requirement 6: Limit circumstances when the new User Role can send Service Requests and for which Suppliers

The default position will be that Users in this User Role:

- will not be able to send Service Requests except those listed in Requirement 3, or subsequently updated through this or a future modification; and
- will only be able to do so upon specific instruction from the Authority (the source of this instruction to be confirmed), which may occur in the event of a Supplier's licence and Certificates being revoked.

In the normal course of events ADT values for the SolrContingency User Role will be set to zero for all Service Requests (meaning that Service Requests are not actioned). In the event of this process being required, the SRP will set the ADT values appropriately.

The DCC will validate the following:

Prior to processing ADT submissions that:

- It has received an instruction from [Ofgem] following notification of a SoLR to allow the SolrContingency SRP to set non-zero ADT values; and

Prior to countersigning any Service Requests for SMETS1 Devices that:

- the Service Request has been signed with the SRP's xmlSign Certificate relating to the SolrContingency role;
- the Supplier ID identified Service Request xml is for an identity which previously had SMKI Certificates in the Supplier Role (and are now revoked); and
- other existing checks (e.g. DUIS authentication and those set out in Requirement 5 are passed).

Prior to adding its Message Authentication Code (MAC) to any Commands for SMETS2+ Devices that:

- the Pre-Command has been signed with the SRP's xmlSign Certificate relating to the SolrContingency role;
- the Business Originator ID identified by the signed GBCS is for an identity which previously had SMKI Certificates in the Supplier Role (and are now revoked); and
- other existing checks (e.g. DUIS authentication and those set out in Requirement 5 are passed).

2.8 Requirement 7: Continue to Send Alerts

The DCC should remain able to send Alerts to the Supplier after the Supplier's Certificates have been revoked (noting that they will be routed to the failed Supplier's SRP).

After the Supplier's Certificates have been revoked the DCC should remain able to send Alerts using the failed Supplier's revoked Certificates, ensuring that safety critical Alerts can be actioned. The table below provides an initial list of safety critical Alerts.

Safety Critical Alerts	
Alert Code	**Alert Name**
0x8F1F	Low Battery Capacity
0x8F3F	Unauthorised Physical Access - Tamper Detect
0x8F73	Unauthorised Physical Access - Battery Cover Removed
0x8F74	Unauthorised Physical Access - Meter Cover Removed
0x8F75	Unauthorised Physical Access - Strong Magnetic field
0x8F76	Unauthorised Physical Access - Terminal Cover Removed
0x8F77	Unauthorised Physical Access - Second Terminal Cover Removed
0x8F78	Unauthorised Physical Access - Other
0x8F1D	GSME Power Supply Loss

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**
ADA	Anomaly Detection Attribute
ADT	Anomaly Detection Threshold
ARO	Authorised Responsible Officer
DCC	Data Communications Company
DUIS	DCC User Interface Specification
GBCS	Great Britain Companion Specification
ID	Identification
MAC	Message Authentication Code
SEC	Smart Energy Code
SMETS	Smart Metering Equipment Technical Specification
SMKI	Smart Meter Key Infrastructure
SoLR	Supplier of Last Resort
SRO	Senior Responsible Officer
SRV	Service Request Variant
SRP	Shared Resource Provider
XML	Extensible Markup Language