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.

MP107 ‘SMETS1 Validation of SRV 6.15.1’

Annex A

Business requirement – version 0.3

About this document

This document contains the business requirements that support the Proposers solution for this Modification. It sets out the requirements along with any assumptions and considerations. The DCC 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	Network Operators must be able to change their Certificates that have been incorrectly placed on SMETS1 Devices that are not in their region
2	(Optional) DCC to undertake corrective action to fix the incorrect Network Operator's certificate(s) as one-off activity on the SMETS1 Device's virtual anchor slots.

2. Considerations and assumptions

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

2.1 Requirement 1: Network Operators must be able to change their Certificates that have been incorrectly placed on SMETS1 Devices that are not in their region

Critical Commands sent to Smart Metering Equipment Technical Specifications 1 (SMETS1) Devices are validated against the Registration Data Provider (RDP) data and Device Certificates. Due to this, if a device is updated with Certificates for the incorrect Network Operator, that Network Operator cannot use Service Request Variant (SRV) 6.15.1 'Update Security Credentials (KRP) to correct those Certificates.

Validation of either Critical Commands (or possibly just SR 6.15.1) must be changed to allow incorrect Certificates to be updated on SMETS1 Devices in such scenarios.

2.2 Requirement 2: (Optional) DCC to undertake corrective action to fix the incorrect Network Operator's certificate(s) as one-off activity on the SMETS1 Device's virtual anchor slots.

DCC voluntarily included an optional requirement to resolve the incorrect certificate data issues on LIVE environment should the impacted Parties wishes to.

This means, DCC to undertake corrective action to fix the incorrect' Network Operator's certificate(s) as one-off activity on the SMETS1 Device's virtual anchor slots (database at S1SP systems) in LIVE environment following the deployment of Requirement 1 if the impacted Parties deem it worthwhile to do so given the numbers of devices involved.

The rationale behind voluntarily including this optional requirement are:

- following the delivery of Requirement 1, 'incorrect' Network Operator need to place the 'correct' Network Operator certificates on SMETS1 device's virtual anchor slots. This approach is similar to SMETS2 and can be considered as enduring solution to fix any future incorrect Network Operator certificate issue. However, resolving the current incorrect certificate data issue requires signification effort and coordination among Network Operators.

- considering the numbers of impacted SMETS1 devices in LIVE environment, Network Operators may consider DCC managed single solution to fix all the current incorrect certificate data issue on behalf of all Network Operators.

3. Solution options

This section outlines potential options for this modification's solution. It sets out the rationale for the potential variants and any further information that can be provided to help assess this change.

3.1 General

The DCC and its Service Providers are requested to assess the requirements and devise a solution, whilst considering the Proposers suggestion below.

The Proposer suggests a possibility of removing the RDP data validation in order to allow a DCC User to update an incorrect Certificate on a SMETS1 Device where they are not the owner of the MPAN. This would mean that the validation of Critical Commands on a SMETS1 Device would act in a similar fashion to validation of SMETS2 Devices.