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.

Paper Reference:	**TABASC_65_0605_10**
Action:	**For Information**

MP134B Business Requirements

1. Purpose

The purpose of this document is for the Technical Architecture and Business Architecture Sub Committee (TABASC) to assess and agree that the business requirements for MP134B 'Use of SMKI Certificates relating to a SoLR event – Part 2' are clear and unambiguous and that this modification is suitable to proceed to Preliminary Assessment.

2. Overview of MP134B

Issue

When a Supplier fails, the Authority can use its Supplier of Last Resort (SoLR) powers to revoke a licence and select and appoint a SoLR where a trade sale or commercial solution is not possible. Once the Authority revokes the failed Supplier's Licence, the DCC is currently obliged to revoke the Supplier's SMKI Certificates. Only the failed Supplier (or its agent) will hold the Smart Metering Key Infrastructure (SMKI) Private Keys that enable Critical Commands to be sent that will be actioned by the meter, until the new Supplier can replace the Certificates. This can take anywhere between two and four weeks.

Consumers with prepayment meters will continue to run down credit during a SoLR process whilst the new Supplier onboards the consumers (knowing enough information about the consumers to populate systems and service them). During a 'disorderly exit' by a failed Supplier there is a risk that a consumer could lose energy supply. It may take a significant amount of time before the new Supplier can issue Critical Commands, such as Emergency Credit, to recommence supply.

MP134 was raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC) to resolve the issues around use of SMKI Certificates during this time.

Proposed Solution

The solution will apply to small Suppliers who use Shared Resource Providers (SRPs). In these cases, the SRP uses the Suppliers SMKI Certificates on behalf of the Supplier to service the estate. In the event of a 'disorderly exit' the Proposed Solution is to have a new User Role ('SoLRContingency') which will be requested by the failed Supplier's SRP. This Role will have limited capability to allow the SRP to subscribe for XML Certificates and allow certain agreed Service Requests (currently suggested SR1.6 'Update Payment Mode) to continue to be issued by the SRP.

This will ensure the affected consumers can remain on supply until the SoLR is able to onboard those consumers.

3. Business requirements

Following discussion at a requirements workshop, a set of business requirements has been developed with input from the Data Service Provider (DSP).

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).

The full details of the business requirements can be found in Appendix A.

4. Questions for the TABASC

At this stage of the modification's progression, we seek the TABASC's views on the following question:

- Are the business requirements suitable to proceed to Preliminary Assessment?

5. Next steps

The business requirements will be reviewed by both the TABASC and the Working Group, and any comments made will be incorporated.

Once the TABASC and the Working Group are content that the business requirements are satisfactory, MP134B will be submitted to the DCC for Preliminary Assessment.

6. Recommendations

The TABASC is requested to **AGREE** the MP134B business requirements are clear and unambiguous and that MP134B is suitable to be progressed to Preliminary Assessment.

Ali Beard

SECAS Team

29 April 2021

Attachments:

- **Appendix A:** MP134B Business Requirements v0.1