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_67_0107_08**
Action:	**For Information**

MP129 Business Requirements

Purpose

This paper presents the business requirements for Modification Proposal MP129 'Allowing the use of CNSA variant for ECDSA'. We seek the Technical Architecture and Business Architecture Sub-Committee's (TABASC) views on whether the solution options are suitable for Preliminary Assessment and whether the business requirements are clear and unambiguous.

- If the business requirements are clear and unambiguous?
- If the solution is suitable to proceed to Preliminary Assessment?

Summary of MP129

This section summarises the key points of this Modification Proposal. More information is available in the draft Modification Report in Appendix A.

What is the issue?

GB Companion Specification (GBCS) Section 4.3.3.2 defines how a Smart Metering Entity should create a "Per-Message Secret Number 'k' with respect to Elliptic Curve Digital Signature Algorithm (ECDSA)" when applying Digital Signatures to meter communications. The 'k' is a random number generator used in the algorithm to create a unique Digital Signature.

Smart Metering Entities are defined as, "An entity that is either a Device or a Remote Party". A Remote Party is defined as "An entity which is remote from a Device and is able to either send Messages to or receive Messages from a Device, whether directly or via a third party."

Suppliers Parties as well as the Data Services Provider (DSP) are both Remote Parties and carry out Critical Command signing activities. The GBCS can be interpreted as mandating the GBCS variant of ECDSA for all Device critical command signing operations, rather than the more common Commercial National Security Algorithm (CNSA) Suite variant, which is approved by the National Institute of Standards and Technology (NIST).

The Department for Business, Energy and Industrial Strategy (BEIS) and the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA) have both since advised the CNSA variant should be permitted for use.

Proposed Solution

The Proposed Solution will modify the relevant sections of the GBCS so that it clearly shows that the CNSA variant for Critical Command signing is permitted for use for Parties. This solution will apply to Smart Metering Equipment Technical Specifications (SMETS)1 and SMETS2 Devices.

The CNSA variant will be permitted for use along with the ECDSA variant, but it will not replace it.

Business requirements

Following discussion at a requirements workshop, a set of business requirements has been developed with input from the DCC, the DSP and the SMKI PMA Chair.

Ref.	Requirement
1	Parties shall be permitted to use the CNSA variant for Critical Command signing.

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

Questions for the TABASC

We seek the TABASC's views on the following questions to feed into the business requirements before we request a Preliminary Assessment:

- Is the solution suitable to proceed to Preliminary Assessment?
- Are the business requirements clear and unambiguous?

Next steps

We will also be seeking comments from the Working Group and we will incorporate the comments received from the TABASC and Working Group into the draft business requirements before requesting the Preliminary Assessment.

Recommendations

The TABASC is requested to **PROVIDE** views on the suitability of the business requirements to deliver the Proposed Solution.

Piers Garton

SECAS Team

24 June 2021

Attachments:

- **Appendix A:** MP129 Business Requirements v0.1