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.

MP129 'Allowing the use of CNSA variant for ECDSA'

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 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	Parties shall be permitted to use the Commercial National Security Algorithm (CNSA) variant for Critical Command signing.

2. Considerations and assumptions

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

2.1 General

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.

This solution will be applied to Smart Metering Equipment Technical Specifications (SMETS)1 and SMETS2 Devices.

2.2 Requirement 1: Parties shall be permitted to use the CNSA variant for Critical Command signing

The CNSA variant is recognised as a more cost-effective and more widely used variant for cryptographic signing than the ECDSA variant. However, the GBCS only refers to the ECDSA variant for Critical Command signing.

The GBCS and any other SEC Technical Specifications shall be updated so that they clearly permit the use of the CNSA variant, but must remain optional and not replace the ECDSA variant.

Suppliers as well as the DSP, routinely carry out Critical Command Signing and they could significantly benefit from this modification, should they choose to use the CNSA variant.

The CNSA variant must be subject to appropriate implementation of a Federal Information Processing Standard (FIPS)-approved random number generator.

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**
BEIS	Department for Business, Energy and Industrial Strategy
CNSA	Commercial National Security Algorithm
DCC	Data Communications Company
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standard
NIST	National Institute of Standards and Technology
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority