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'

Annex B

Legal text – version 0.1

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Schedule 8 'GB Companion Specification'

These changes have been redlined against Schedule 8 version 4.1.

These changes will be applied to version 4.n.

Amend Section 4.3.3.2 as follows:

4.3.3 Cryptographic primitives and their usage

In relation to any Remote Party Message, Smart Metering Entities shall:

- use SHA-256, as specified in FIPS 180-41, as the Hash function;
- use the AES-128 cipher, as specified in FIPS 1972, as the block cipher primitive;
- use the Galois Counter Mode (GCM) mode of operation as specified in NIST Special Publication 800-38D3 ;
- use the GMAC technique, based on the use of AES-128, for the calculation of Message Authentication Codes (MACs), as specified in NIST Special Publication 800-38D (see above);
- use, as the Digital Signature technique, ECDSA (as specified in FIPS PUB 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at section D1.2.3) and SHA-256 as the Hash function. Within Messages, Signatures shall be in the Plain Format;
- use, to calculate the Shared Secret Z, the Static Unified Model, C(0e, 2s, ECC CDH) Key Agreement technique (as specified in NIST Special Publication 800-56Ar24 save for the requirement to zeroize the Shared Secret) with:
  - the Single-step Key Derivation Function (KDF) based on SHA-256, as specified in NIST Special Publication 800-56Ar2; and
  - the P-256 curve for the elliptic curve operations.

Resulting DerivedKeyingMaterial (with its meaning in *NIST Special Publication 800-56Ar2*) shall only ever be used in relation to one Message instance. Any Shared Secret that is not 'zeroized' shall be stored and used with the same security protections as Private Keys.

4.3.3.1 Scope of Cryptographic Protections

The fields that shall always contribute to MAC and Digital Signature are detailed in Section 7.2. Fields that vary across Messages are specified in Section 6, and in the relevant Use Cases. For clarity, a Message instance may transit through multiple Smart Metering Entities before delivery to its target Device, and more than one Smart Metering Entity may be required to apply a Cryptographic Protection to that Message instance. Thus, the scope of protection can only be across fields in the Message instance as constructed at the point the protection is applied.

[1] http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[2] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[3] http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf
[4] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

Where a Message has multiple Cryptographic Protections, the order in which the Smart Metering Entities apply these Cryptographic Protections is specified in this GBCS.

A Device verifying the Cryptographic Protections in such Messages shall undertake such verifications in the reverse sequence to that in which the Cryptographic Protections were applied. This order is also specified in this GBCS.

4.3.3.2 ECDSA per message secret number

When generating a Digital Signature, the Smart Metering Entity shall calculate the DSA Per-Message Secret Number 'k' with respect to ECDSA (with the meaning in section 6.3 of *FIPS 186-4*) to be the SHA-256 hash of the concatenation of:

- the parts of the Message to be signed, as defined in Section 7.2.7; and
- the Private Key that the Smart Metering Entity will use in the Digital Signature generation.

If the value of k so calculated is zero or greater than n -1, or results in an 'r' or 's' value of 0, where r and s have the meanings in the NSA's '*Suite B Implementer's Guide to FIPS 186-3 (ECDSA)*', then a new value for k shall be calculated to be the SHA-256 hash of the concatenation of:

- the parts of the Message to be signed, as defined in Section 7.2.7;
- the Private Key that the Smart Metering Entity will use in the Digital Signature generation; and
- 0x00.

The addition of 0x00 to the concatenation shall be repeated until a value of k is generated that does not result in k being zero or greater than n -1, or an 'r' or 's' value of 0.

As an alternative to the above, a Remote Party may choose to derive 'k' using the method defined in Section 3.3 and Appendix A.2 of NSA's 'Suite B Implementer's Guide to FIPS 186-3 (ECDSA)'.

4.3.3.3 Calculating unique Shared Secret Keys for a Remote Party Message Instance

Where a Smart Metering Entity executes the KDF in relation to a Message instance, the *OtherInfo* field, with the meaning in *NIST Special Publication 800-56Ar2*, shall be populated using the value of information provided in, or to be placed in, the originator-system-title, recipient-system-title and transaction-id fields of the Grouping Header, as per the requirements of Section 7.2.7.

The *OtherInfo* shall be in the Concatenation Format as defined in section 5.8.1.2.1 of NIST Special Publication 800-56Ar2 and shall be the concatenation:

AlgorithmID || value of originator-system-title || length of transaction-id || value of transaction-id || value of recipient-system-title

where:

- AlgorithmID is that for AES-GCM-128 and so has a value 0x60857406080300, as specified by section 9.2.3.4.6.5 of the Green Book; and
- length of transaction-id has the value 0x09.

4.3.3.4 Calculating the Initialization Vector for GCM and GMAC

In relation to Remote Party Messages, Smart Metering Entities shall use a 96 bit Initialization Vector (IV) for the GCM and GMAC algorithms as defined in *NIST Special Publication 800-38D*. The IV shall be the concatenation:

FixedField || *InvocationField*

where:

- FixedField shall always have the same value as the Business Originator ID in the Grouping Header part of the Message being processed (see Section 7.2.7); and
- InvocationField = 0x00000000.

The DLMS COSEM Authentication Key (AK), as defined in the Green Book, shall be a zero length string.

4.3.3.4.1 Other input parameters to MAC and Encryption / Decryption operations – informative

Other input parameters for MAC, Encryption and Decryption are not specified in this Section 4.3.3 because they vary dependent on a number of factors. These other input parameters are listed in tables of the same format as Table 4.3.3.4.1 and their values are specified in each part of the GBCS where such an operation is specified.

The template for such tables is the Table 4.3.3.4.1. Please note that this table does not contain any values as it is a template only.

Input Parameter	Value	Note
To calculate the Shared Secret ('*Z*') input to the KDF:		
Private Key Agreement Key		
Public Key Agreement Key		
The other input to the KDF ('*OtherInfo*') shall be calculated according to the requirements of Section 4.3.3.3.		
As input to the GMAC function, the IV shall be constructed according to the requirements of Section 4.3.3.4, the Plaintext shall be empty and:		
Additional Authenticated Data shall be the concatenation:		

Table 4.3.3.4.1: Template for other input parameters

4.3.3.4.2 Size of MAC

The bit length of the MAC shall be 96 except for the MAC contained in the WrappedApexContingencyKey extension within root Certificates, where the bit length of the MAC shall be 128.