SEC
Smart Energy Code

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'

Modification Report

Version 1.0

19 April 2022

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

This document also has three annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** contains the Data Communications Company (DCC) Preliminary Assessment response[1].

Contact

If you have any questions on this modification, please contact:

Mike Fenn

020 3314 1142

mike.fenn@gemserv.com

[1] The implementation timescale and costs in the DCC Preliminary Assessment response are no longer valid as the modification scope has changed. For full details see the section titled 'Solution Development'.

1. Summary

This proposal has been raised by David Rollason from the DCC.

The Data Service Provider (DSP) interpreted SEC Schedule 8 'GB Companion Specification' (GBCS) as mandating the GBCS variant of the Elliptic Curve Digital Signature Algorithm (ECDSA) for all Device Critical Command signing operations, rather than the more common Commercial National Security Algorithm (CNSA) Suite standard variant.

The Department for Business, Energy and Industrial Strategy (BEIS) advised that the DSP could have used the CNSA Suite standard and remained compliant. The Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA) agreed that the GBCS wording in Section 4.3.3.2 lacked clarity and would need to be updated to explicitly permit the use of CNSA Suite by Remote Parties.

The Proposed Solution is to modify the GBCS so that it clearly shows the CNSA Suite variant is permitted for use as well as the GBCS variant of the ECDSA.

This modification will not directly impact any Parties as it is not changing any obligations and only seeks to make the GBCS clearer. There are no DCC System costs so the cost to implement will be limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort to update the SEC. This is being progressed as a Self-Governance Modification and the targeted implementation date is 3 November 2022 (November 2022 SEC Release).

2. Issue

What are the current arrangements?

Critical Command signing

The ECDSA is a cryptographic algorithm used for signing Critical Commands. It can be used with differing key lengths and can be implemented in different ways, known as variants. One example is the approach published in the GBCS which makes use of message characteristics to ensure that a signature of a given Command will differ every time it is signed, thus protecting against cryptographic analysis. Another is the approach documented within the CNSA Suite which uses random number entropy for the same purpose. As its title implies, the CNSA Suite covers a suite of algorithms including the ECDSA.

The CNSA Suite replaced the older National Security Agency (NSA) Suite-B as published by the United States (US) National Security Agency.

GBCS rules for the ECDSA

GBCS Section 4.3.3.2 defines how a Smart Metering Entity should create a "Per-Message Secret Number 'k' with respect to 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." The DSP and Supplier Parties

are both Remote Parties and carry out Critical Command signing activities. The Communication Service Providers (CSPs) could also be considered Remote Parties.

What is the issue?

The DSP has interpreted the GBCS as mandating the GBCS variant of the ECDSA for all Device Critical Command signing operations, rather than the more common CNSA Suite variant, which is approved by the National Institute of Standards and Technology (NIST).

BEIS advised that this was a DSP interpretation which was overly restrictive and advised that the DSP could have used the CNSA Suite variant and remained compliant.

The SMKI PMA agreed that the GBCS Section 4.3.3.2 wording lacked clarity and would need to be updated to explicitly permit the use of CNSA Suite variant by Remote Parties. The SMKI PMA noted the clear distinction that this should permit its use, but not require its use, i.e. Remote Parties should be allowed to continue to use GBCS variant if they choose. This is critical to the continuity of Service Users' processes and to provide a clean Certificate migration pathway.

What is the impact this is having?

The CNSA Suite variant is easier for Users to implement and makes the process more efficient. However, the GBCS wording is unclear on whether the more common CNSA Suite variant is permitted.

The GBCS variant of the ECDSA is bespoke and designed to suit the characteristics of meters. The GBCS variant requires bespoke code, whereas the CNSA Suite is a widely adopted commercial standard supported by most Hardware Security Models (HSMs). The CNSA implementation is maintained by the HSM vendors; the GBCS is not and instead is a UK Sovereign implementation.

The Proposer notes the following factors supporting the use of the CNSA Suite variant:

- GBCS bespoke code is subject to less validation and any issues are less likely to be identified.
- Issues are more easily escalated with the HSM vendors when associated with a commercial standard as they are incentivised to fix by having large numbers of their user base complaining about the same issue.
- Upgrades and improvements to CNSA implementation come free with HSM upgrades.
- GBCS bespoke code requires bespoke support arrangements and this is only supported by two HSM vendors at present. CNSA Suite variant is supported on most western commercial HSMs.
- The GBCS variant of the ECDSA is far less efficient that the CNSA Suite variant where the Device has access to an appropriate Random Number Generator.

Impact on consumers

This issue does not impact consumers.

3. Solution

Proposed Solution

The Proposed Solution will modify Section 4.3.3.2 of the GBCS so that it clearly shows that the CNSA Suite variant for Critical Command signing is permitted for use for Parties. The CNSA Suite variant will be permitted for use along with the GBCS variant, but it will not replace it.

This modification previously sought to facilitate the DSP System change needed for the DSP to switch from the GBCS variant to the CNSA Suite variant for Critical Command signing, which it intends to do if MP129 is approved. The costs of this System change would have been borne by industry. Following the DCC's Preliminary Assessment and subsequent discussion with the Technical Architecture and Business Architecture Sub-Committee (TABASC), the DCC agreed to remove the DSP System change from the scope of the modification. This means that this modification will only amend the legal text; if the DSP wishes to transition to the CNSA Suite variant it can, but the cost will not be levied through the Modification Process.

There will be no Device impacts as result of this modification, and it will not impact the way Devices receive Critical Commands.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Parties	✓	Gas Network Parties
	Other SEC Parties	✓	DCC

Considering use of the CNSA Suite variant will not be mandated, the DCC noted the impact of switching to the CNSA Suite variant is at the discretion of each signing Party. Any change in implementation by any given Party should logically be transparent to Devices. The DCC added that the impact on a Party which chooses to switch to the CNSA Suite variant will depend on its environment, technology, and cryptographic policy. However, it considered the following points:

- A switch in variant will require reconfiguration of a Party's application which requests a digital signature.
- Although this may impact on the signing function itself, it would be moving from a bespoke approach to an industry standard approach, so this is unlikely to be an issue for most Parties.
- A switch to the CNSA Suite variant will require updates of appropriate documentation, including policies, design of calling and signing functions, and support definitions.

- A switch to the CNSA Suite variant may involve updates to support contracts if it removes the need for special support arrangements for bespoke implementations that are currently in place.

Suppliers

Suppliers routinely carry out Critical Command signing and they could significantly benefit from this modification, should they choose to use the CNSA Suite variant.

Also, the DSP's ongoing service charge is expected to decrease if it uses the CNSA Suite variant, which would benefit Suppliers.

Network Parties

Network Parties are able to carry out Critical Command signing and they could significantly benefit from this modification, should they choose to use the CNSA Suite variant.

Also, the DSP's ongoing service charge is expected to decrease if it uses the CNSA Suite variant, which would benefit Suppliers.

DCC

The DSP

The DSP would benefit from this modification. If the DSP chooses to move to the standard CNSA Suite variant for Critical Command signing, it is expected to improve the performance of its HSMs and reduce ongoing maintenance effort and Operational Support charges. There would also be a corresponding reduction in the DSP ongoing service charge.

If the DSP intends to switch to using the CNSA Suite variant for Critical Command signing, it would also be required to carry out Systems Integration Testing (SIT). However, SIT is not included in this modification as it is a text-only change and does not mandate DSP System changes. As the switch to using the CNSA Suite variant is optional, any DSP costs would have to be justified to the Authority through the DCC's annual price control process.

The CSPs

Whilst the CSPs could implement the CNSA Suite variant, the number of Critical Commands sent to Communications Hubs is low. As such, performance gains would be minimal, and the reduction in memory on the Devices would have a negative effect and would most likely require Communications Hub changes. If the CSPs choose to switch to using the CNSA Suite variant the costs would have to be justified to the Authority through the DCC's annual price control process.

DCC System

This modification will not impact the DCC Systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Schedule 8 'Great Britain Companion Specification'
- Schedule 11 'Technical Specification Applicability Tables'

Technical specification versions

This modification is expected to be implemented within a new Sub-Version of the GBCS (v4.n). For efficiency this modification will be targeted for a SEC Release including other modifications which require an uplift of the GBCS. SECAS is recommending implementing MP129 in the November 2022 SEC Release, which is expected to uplift the GBCS to version 4.2.

This modification will have no impact on Devices and therefore no impact on the Smart Metering Equipment Technical Specifications (SMETS).

The TABASC will ultimately approve the technical specification versions for the given release, taking into account all the modifications included within that release.

Consumers

This modification does not have any consumer impacts.

Other industry Codes

This modification does not impact any other Codes.

Greenhouse gas emissions

This modification does not impact greenhouse gas emissions.

5. Costs

DCC costs

There will be no DCC costs to implement this modification.

SECAS costs

The estimated SECAS implementation costs to implement this modification is one day of effort, amounting to approximately £600. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

This modification will not incur any SEC Party costs.

Parties can already use the CNSA Suite variant at their own discretion. Switching to this variant may incur a cost. However, this cost would be at the expense of the individual SEC Party.

6. Implementation approach

Approved implementation approach

The Change Sub-Committee (CSC) has agreed an implementation date of:

- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received on or before 20 October 2022; or
- **29 June 2023** (June 2023 SEC Release) if a decision to approve is received after 20 October 2022 but on or before 15 June 2023.

This modification will impact the GBCS and, for efficiency, should be implemented in a scheduled SEC Release along with other GBCS changes, also minimising SEC Party cost.

7. Assessment of the proposal

Observations on the issue

SMKI PMA views

The SMKI PMA believed that the GBCS section 4.3.3.2 wording lacks clarity and would need to be updated to explicitly permit the use of the CNSA Suite variant by Remote Parties. It believed the CNSA Suite variant should be permitted but not forced on Parties, and therefore remain optional.

Change Sub-Committee views

SECAS advised that DCC System changes would be needed if the DSP were to switch from the GBCS variant of the ECDSA to the CNSA Suite variant. A CSC member noted that Parties should understand the issue and remain cautious when making changes to the DSP Systems as there are already issues regarding duplicate identifiers (IDs) and messages.

Solution development

Scope of the modification

Initially the DCC sought to use this modification to cover any DCC System impacts and implementation costs for switching to the CNSA Suite variant for Critical Command signing. The DCC believed the overall DCC System impact to be low, although a move to the CNSA Suite variant for the

DCC would impact the DSP and require appropriate testing. This is given the fact that a switch in variant has not been proven not to impact any Devices.

However, SECAS advised that Parties should not incur the cost for the DCC switching to this variant when it is already permitted.

The DCC carried out a Preliminary Assessment to understand the impacts on the DCC Systems and any associated implementation costs before deciding how to proceed. Following the outcome of the Preliminary Assessment and subsequent discussion with the TABASC (see below), the DCC agreed to limit the scope of this modification to amending the GBCS to make it explicitly clear that the CNSA Suite variant is permitted.

The DSP System change has been removed from the scope of the modification, and MP129 is therefore a document-only modification. Costs will be limited to SECAS time and effort to update the SEC. The DCC's Preliminary Assessment response is provided in Annex C for reference.

Business requirements workshop

The business requirements were discussed at a business requirements workshop in April 2021, attended by the DCC and its Service Providers as well as the SMKI PMA Chair.

SECAS highlighted an extract from DCC User Interface Specification (DUIS) v4.0, Page 72, section 3.3: '*All these DUIS signing activities shall be performed using the Elliptic Curve Digital Signature Algorithm (ECDSA)…*'. The DSP advised that this text is related to Extensible Markup Language (XML) Signing, not GBCS Critical Command signing, and it does not impact the issue highlighted in this proposal.

The DSP noted that the business requirements and the Modification Report had been initially written in the context that this only impacts the DSP. However, Suppliers routinely carry out Critical Command signing and they could significantly benefit from this modification as well, should they choose to use the CNSA Suite variant.

SECAS agreed to update the business requirements so that they show a benefit to all Remote Parties, not just the DSP.

The SMKI PMA Chair highlighted that upon previously looking at this proposal they had advised the DSP that a caveat will be required to ensure that the CNSA Suite variant is subject to appropriate implementation of a Federal Information Processing Standards (FIPS)-approved random number generator. SECAS agreed to reflect this in the business requirements.

TABASC review of the Preliminary Assessment

SECAS presented the TABASC with an update on the outputs from the DCC's Preliminary Assessment.

The TABASC noted that some Service User benefits are clear, particularly regarding the proposed investments in HSMs. SECAS also highlighted that there would be a reduction in the DSP charge. However, the Preliminary Assessment did not state how much this decrease could be.

The TABASC Chair referenced the impact on the DSP's HSMs and questioned whether the DSP or the Service User would be the beneficiary. The TABASC noted that the DSP could be the beneficiary whilst the financial burden fell on the Service User. SECAS agreed to investigate the business case further with the DCC.

The TABASC advised SECAS to seek a clear view of the User benefits and whether this will be seen prior to the end of the existing DSP contract. The Chair also presented the argument for implementing MP129 as part of the DSP re-procurement, with the benefit that the functionality could be utilised from day one, with the potential for this to be less costly than introducing this into the current DSP.

The TABASC advised that whilst there is some support for MP129 moving forward to Impact Assessment, further analysis of the User and DSP benefits will be required first. It agreed that the Proposed Solution would not have a negative impact on the technical and/or business architecture of either the DCC Systems or Users' systems.

SMKI PMA review of the Preliminary Assessment

SECAS presented the SMKI PMA with an update on the outputs from the DCC's Preliminary Assessment.

A SMKI PMA member questioned whether there would be any impacts on Devices. Members advised there would not be impacts on Devices, with the Devices "oblivious" as to which Critical Command signing variant is used.

SECAS noted the TABASC's comments that more investigation on the business case is required. A member advised that there would be a need for less HSMs as well as faster SMKI recovery times, which would provide a positive business case.

The SMKI PMA agreed the Proposed Solution would not compromise the SMKI arrangements.

8. Case for change

Business case

The benefits of this modification are operational in nature. Moving to the standard CNSA Suite variant for Critical Command signing is expected to improve the performance of the HSMs and reduce ongoing maintenance effort and Operational Support charges. If the DSP switches to the CNSA Suite variant following implementation of MP129, there is expected to be a corresponding reduction in the DSP ongoing service charge.

Using the CNSA Suite variant is also expected to deliver performance improvement for the SMKI Recovery application. The current version can process about 30 Certificates per second, while implementing the CNSA Suite variant is expected to accelerate this processing to between 300 and 500 Certificates per second. This will benefit large scale Certificate replacement activities such as Transitional Change of Supplier (TCoS) to Enduring Change of Supplier (ECoS) migration, and also any use of the SMKI Recovery application to replace compromised Certificates.

Views against the General SEC Objectives

Proposer's views

Objective (g)[2]

The Proposer believes this modification would better facilitate SEC Objective (g) by making it explicitly clear that the GBCS permits the use of the CNSA Suite variant for Critical Command signing.

Industry views

The Refinement Consultation returned no responses from industry. The Working Group were supportive of the change as it provides clarity on the permissible use of the CNSA Suite variant, and agreed that it would better facilitate SEC Objective (g).

The Chair of the SMKI PMA and Security Sub-Committee (SSC) expressed their support for the modification, citing the efficiency and cost benefits of the DSP switching to the CNSA Suite variant.

Views against the consumer areas

Improved safety and reliability

This modification will be neutral against this consumer benefit area.

Lower bills than would otherwise be the case

This modification will be neutral against this consumer benefit area.

Reduced environmental damage

This modification will be neutral against this consumer benefit area.

Improved quality of service

This modification will be neutral against this consumer benefit area.

Benefits for society as a whole

This modification will be neutral against this consumer benefit area.

[2] Facilitate the efficient and transparent administration and implementation of this Code.

Appendix 1: Progression timetable

On 19 April 2022 the CSC approved the Modification Report for progression to the Report Phase. SECAS will issue a Modification Report Consultation ahead of the Change Board vote under Self-Governance on 25 May 2022.

Timetable	
Event/Action	**Date**
Draft Proposal raised	12 May 2020
Presented to SMKI PMA for initial comment	19 May 2020
Presented to CSC for initial comment	26 May 2020
Panel converts Draft Proposal to Modification Proposal	19 Jun 2020
Business requirements developed with Proposer and DCC	Aug 2020
Modification discussed with Working Group	2 Sep 2020
Business requirements workshop	19 Apr 2021
DCC Preliminary Assessment	9 Jul 2021 – 25 Aug 2021
Modification discussed with the TABASC	4 Nov 2021
Modification discussed with the SMKI PMA	10 Nov 2021
Refinement Consultation	14 Feb – 4 Mar 2022
Modification discussed with Working Group	6 Apr 2022
Modification Report approved by CSC	19 Apr 2022
Modification Report Consultation	19 Apr – 11 May 2022
Change Board Vote	25 May 2022

Appendix 2: 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 of Business, Energy and Industrial Strategy
CNSA	Commercial National Security Algorithm
CSC	Change Sub-Committee
CSP	Communication Service Providers
DCC	Data Communications Company
DSP	Data Services Provider
DUIS	DCC User Interface Specification
ECDSA	Elliptic Curve Digital Signature Algorithm
ECoS	Enduring Change of Supplier
FIPS	Federal Information Processing Standards
GBCS	Great Britain Companion Specification
HSM	Hardware Security Module
ID	Identifier
NIST	National Institute of Standards and Technology
NSA	National Security Agency
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TCoS	Transitional Change of Supplier
US	United States
XML	Extensible Markup Language

MP129 'Allowing the use of CNSA variant for ECDSA'

Annex B

Legal text – version 1.0

About this document

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

Schedule 8 'Great Britain 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)*'~~ *FIPS 186-4*, 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 6.3 and Appendix B.5 of FIPS 186-4.

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.

Data Communications Company

SEC Modification Proposal, SECMP0129, DCC CR4386

Allowing the use case of CNSA Variant for ECDSA

Preliminary Impact Assessment (PIA)

Version:	**0.4**
Date:	**22nd September, 2021**
Author:	**DCC**
Classification:	**DCC Public**

Data Communications Company

Contents

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to complete the Full Impact Assessment of £19,787
- The timescales to complete the Full Impact Assessment of 30 days
- ROM costs for SECMP0129, up to the end of Pre-Integration Testing (PIT) of between £0 and £150,000

Problem Statement and Solution

Cryptographic signing is an important element in the securing and transmission of Critical Commands. However, the Great Britain Companion Specification (GBCS) only refers to the Elliptic Curve Digital Signature Algorithm (ECDSA) cryptographic algorithm for Critical Command signing. The Commercial National Security Algorithm (CNSA) variant is recognised as a more cost-effective and more widely used variant than the ECDSA variant.

The 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.

Modification Benefit

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

Moving to the standard CNSA variant for ECDSA signing is expected to improve the performance of the Hardware Security Modules, reduce ongoing maintenance effort, and reduce DSP Operational Support charges. A corresponding reduction in the DSP ongoing service charge is anticipated.

DCC notes that related, specific DSP certificate-based functions such as SMKI Recovery, Transitional Change of Supplier (TCoS) to Enduring Change of Supplier (ECoS) migration, and Hardware Security Module performance would show significant performance improvements. The current version can process about 30 certificates per second, while implementing the CNSA variant is expected to accelerate this processing to between 300 and 500 certificates/second.

DCC notes that the legal text should be changed to permit the use of the CNSA variant, but must remain optional.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
23/08/2021	0.1	Initial DCC Review with Service Providers
25/08/2021	0.3	Internal review
22/09/2021	0.4	Amended following SECAS feedback

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP129 Modification Report v0.5	SECAS	23/12/2020
2	MP129 Business Requirements v0.1	SECAS	12/07/2021

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is David Rollason of Smart DCC.

The Preliminary Impact Assessment was requested of DCC on 12th July 2021, and accepted on the 16th July 2021.

3 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by SECAS, the Proposer, and the Working Group.

3.1 Context

The 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, the DSP are both Remote Parties and carry out Critical Command signing activities. The Communication Service Providers (CSPs) could also be considered Remote Parties.

3.2 Problem Statement

The Data Services Provider (DSP) considers itself to be a ‘Remote Party’ in the context of Smart Energy Code (SEC) Schedule 8 ‘GB Companion Specification’ (GBCS) Section 4.3.3.2. The DSP interpreted the GBCS as mandating the GBCS variant of Elliptic Curve Digital Signature Algorithm (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 CNSA variant is recognised as a more cost-effective and more widely used variant for cryptographic signing than the ECDSA. However, the GBCS only refers to the ECDSA for Critical Command signing.

The Department for Business, Energy and Industrial Strategy (BEIS) advised that the DSP could have used the CNSA variant and remained compliant. The Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) agreed that the GBCS wording in Section 4.3.3.2 lacked clarity and would need to be updated to explicitly permit the use of CNSA by Remote Parties.

In terms of current issues, the main concern is that the GBCS wording is unclear whether the more common CNSA Suite variant is permitted. It should be noted that the CNSA Suite variant is easier for Users to implement and makes the process more efficient, and has very clear performance improvements associated with its use.

3.3 Business Requirement

There is one Requirement for this Modification.

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 also 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 implemented with a Federal Information Processing Standard (FIPS)-approved random number generator. This increases processing requirements, but has a higher level of security associated with the full implementation.

3.4 Proposed Solution

The Proposed Solution is to modify the GBCS so it clearly shows the CNSA variant is permitted for use as well as the ECDSA variant. This modification will not directly impact any Parties as it is not changing any obligations and only seeks to make the GBCS clearer. The legal text implementation costs will be limited to the Smart Energy Code Administrator and Secretariat (SECAS) time and effort.

System changes would be required by the DSP and any other Service Provider that wishes to adopt the CNSA variant.

As directed by SECAS, this solution should be applied to Smart Metering Equipment Technical Specifications (SMETS)1 and SMETS2 Devices. However SMETS1 does not use Critical Commands and the benefits would be minimal in applying this solution, such that SMETS1 usage has been discounted in this document.

4 Description of Technical Solution

Changes to the DSP are required for implementing the CNSA Variant solution. It should be noted that while the Communications Service Providers could implement the CNSA variant, the number of Critical commands sent to Communications Hubs is low, performance gains would be minimal, and the reduction in memory on the devices would have a negative effect and would most likely require Comms Hub changes.

4.1 DSP Solution

The existing GBCS variant of ECDSA is supported in the DSP using a custom library (named Phase2 API) provided by the Hardware Security Module (HSM) vendor, Thales. The solution would change this to the standard CNSA variant for ECDSA signing for (Access Control Broker) ACB and Recovery operations. Moving to the standard CNSA variant for ECDSA signing is expected to improve the performance of the HSMs and reduce ongoing maintenance effort. It is also expected to deliver performance improvement for the Recovery application.

It shall be noted that TCoS signing will continue to use the existing ECDSA variant, as TCoS will eventually be replaced by the ECoS service.

To change to the standard CNSA variant for ECDSA signing, DSP would make the following changes.

1. Modify the DSP implementation to use the standard ECDSA signing mechanism rather than using the Thales Phase2 API.
2. Modify the DSP implementation to support JCE/PKCS[1]11 keys, which are usable outside of the SEE (Secure Execution Engine) of HSMs.
3. Copy the existing digital signature keys and convert the copies to be usable by JCE such that the certificates in the Devices can remain unchanged. This will require DSP to upgrade the HSM client software.
4. Remove the SEE machines that are no longer required. The SEE machines are used to hold the existing keys. The associated Access Control Lists (ACL) shall also be removed.

The revised application code that supports the use of Standard CNSA shall be subject to a feature switch to allow for phased deployment and provide fail back if required. Item 4 above (Removal of the SEE machines) will only occur after the feature switch has been activated in each environment and successful operation has been confirmed.

It should also be noted that the recovery application is a special case function that is not updated via standard release processes as it is not network connected to core DSP in normal state. Its update will need to be subject to manual code deployment and specific testing.

[1] JCE is the Java Cryptography Extension, PKCS relates to Public-Key Cryptography Standards

5 Impact on Systems, Processes and People

This section describes the impact of SECMP0129 on Services and Interfaces that impact Users and/or Parties.

5.1 Security Impact

The implementation will be security assured throughout. This assurance includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

The DSP Security Team will be involved with each aspect of this change and activities will include, but are not limited to, development team support, key conversion, regression testing, reconfiguration of HSM for each environment and update of all security documentation reflecting the new Design. The Security Team will also be directly involved in supporting testing of the recovery function.

A more detailed Security impact will be carried out as part of the Full Impact Assessment.

The Security libraries will need to be modified to use the standard CNSA variant for ECDSA signing as described above.

5.2 Hardware Security Module

The SEE machines that are no longer required shall be removed from the HSMs. It shall be noted that a minimum of one SEE per environment is needed for supporting the Certificate Signing Request (CSR) for GMAC (Galois Message Authentication Code).

5.3 Infrastructure Impact

There will be no change to the infrastructure design as a result of this change. Additional processing and storage will be required; however, they are not sufficiently large to warrant the procurement of additional compute power or storage. The change does not impact the DSP resilience or DR implementation.

5.4 Service Impact

It is not thought that the change in behaviour of the DSP system from this Modification will have a material ongoing service impact. No changes to SLAs or reporting are expected as a result of this change. However, a more detailed service impact will be completed as part of the FIA.

5.5 Solution Benefits

The benefits of this Modification are operational in nature.

Moving to the standard CNSA variant for signing is expected to improve the performance of the HSMs and reduce ongoing maintenance effort and Operational Support charges. When implemented, there is expected to be a corresponding reduction in the DSP ongoing service charge.

Using the CNSA variant is also expected to deliver performance improvement for the SMKI Recovery application. The current version can process about 30 certificates per second, while implementing the CNSA variant is expected to accelerate this processing to between 300 and 500 certificates/second. This will benefit large scale certificate replacement activities

such as TCoS to ECoS Migration, and also any use of the SMKI Recovery application to replace compromised certificates.

6 Implementation Timescales and Approach

This change is expected to be included in a future SEC Release. Design, Build, and PIT is expected to take about three months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA. As noted in section 4.1, the HSM client software upgrade could be carried out as part of the DSP Technical Refresh activity. Since this version upgrade is a prerequisite for implementing this Modification, this Modification could be part of a release that includes the Tech Refresh activity or a later major release.

It is likely that the testing and deployment of updates to the recovery function will be aligned to extant recovery function activities (the regular (annual) SMKI Recovery testing that takes place) in order to minimise costs. However, this would act as a major timeline dependency for the delivery of this Modification and alternative plans might be developed in the FIA.

6.1 Testing and Acceptance

There will be an impact to Systems Integration Testing (SIT) as a result of this change. SIT activities will include test preparation, execution and reporting as required, as well as Service Request Variant (SRV) testing to verify the use of critical commands on selected devices.

The System Integrator will be required to manage the testing. It should be noted that the additional costs for SIT are likely to be similar to Design, Build, and PIT costs, and the scale of the costs is due to testing certificates with the HSM. These costs will be included in the Full Impact Assessment (FIA).

There is no perceived requirement to test this Modification in User Integration Testing (UIT).

7 Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional requirements. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result the final offer price may result in a variation.

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

	Design, Build and PIT	Days to Create FIA	Cost to Create FIA
DSP	£0 to £150,000	30	£19,787

Table 2: SECMP0129 Standalone Cost

The phases included are as follows.

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.

Based on the existing requirements, the fixed price cost for a Full Impact Assessment is **£19,787** and would be expected to be completed in 30 days.

7.1 Legal Text Changes

For the legal text change, SECAS recommends this be a Self Governance Modification.

Legal text implementation costs will be limited to the Smart Energy Code Administrator and Secretariat (SECAS) time and effort.

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
ACB	Access Control Broker
ACL	Access Control List
CAN	Contract Amendment Note
CNSA	Commercial National Security Algorithm
CR	DCC Change Request
CSP	Communication Service Provider
CSR	Certificate Signing Request
DCC	Data Communications Company
DSP	Data Service Provider
ECDSA	Elliptic Curve Digital Signature Algorithm
ECoS	Enduring Change of Supplier
FIA	Full Impact Assessment
FIPS	Federal Information Processing Standard
GBCS	Great Britain Companion Specification
GMAC	Galois Message Authentication Code
HSM	Hardware Security Module
JCE	Java Cryptography Extension
NIST	National Institute of Standards and Technology
PIA	Preliminary Impact Assessment
PKCS	Public-Key Cryptography Standards
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SEE	Secure Execution Engine
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SMKI	Smart Meter Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SRV	Service Request Variant
TCoS	Transitional Change of Supplier
UIT	User Integration Testing

Appendix B: Risks, Assumptions, Issues, and Dependencies

The tables below provide a summary of any Risks, Assumptions, Issues, and Dependencies (RAID) observed during the production of this PIA. Scope exclusions are also noted.

Assumptions

Ref	Description	Status/Mitigation
MP129-DA1	To avoid incurring additional charges for SMKI Recovery testing, there is a dependency on the delivery of this Modification being scheduled at a suitable date to allow the Annual SMKI Recovery Testing to take place	Open
MP129-DA2	TCoS signing will continue to use the existing ECDSA variant, as TCoS will eventually be replaced by the ECoS service. It is assumed that the current HSM setup can achieve the required processing rates for ECoS migration	Open
MP129-DA3	It is assumed that there will be a requirement for Performance testing and benchmarking of the Recovery application before and after the implementation of this CR4386	Open

Dependencies

Ref	Description	Status/Mitigation
MP129-DD1	To avoid incurring additional charges for SMKI Recovery testing, there is a dependency on the delivery of this CR4386 being scheduled at a suitable date to allow the Annual SMKI Recovery Testing to take place	Open

Scope Exclusions

TCoS is excluded from the scope of this Modification on the basis that it is soon to be replaced and in order to keep charges as low as possible.

The Install & Commission (I&C) of new devices is not required for this change and is therefore excluded, on the basis that SIT testing will be undertaken against existing device sets.