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 0.8

14 February 2022

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

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

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 latest full Data Communications Company (DCC) Preliminary Assessment response.

Contact

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

Mike Fenn

020 3314 1142

mike.fenn@gemserv.com

1. Summary

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

The Data Services 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.

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 standard 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. SECAS recommends this be a Self-Governance Modification and the targeted implementation date is the 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, CNSA Suite covers a suite of algorithms including ECDSA.

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

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 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, GBCS is not and 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 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 variant for Critical Command signing is permitted for use for Parties. The CNSA variant will be permitted for use along with the ECDSA, but it will not replace it.

This modification previously sought to facilitate the DSP System change needed for the DSP to switch from the ECDSA to the CNSA 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 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 amend the legal text and if the DSP wish to transition to the CNSA 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 Operators		Gas Network Operators
	Other SEC Parties	✓	DCC

Considering the CNSA variant is already permitted, the impact on a Party which chooses to switch to the CNSA variant will depend on its environment, technology, and cryptographic policy. The possible impacts of switching to the CNSA variant are drawn out in page 8 of this report.

Suppliers

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

Also, the DSP's ongoing service charge is expected to decrease if it uses the CNSA 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 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 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 will not require DSP System changes. As the switch to using the CNSA 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 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 Communications Hub changes. If the CSPs choose to switch to using the CNSA 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 and Principal Version of the GBCS. For efficiency this modification will be targeted for a SEC Release including other modifications which require an uplift of the GBCS.

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 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

Recommended implementation approach

SECAS is recommending 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 CNSA by Remote Parties. It believed the CNSA should be permitted, but not forced upon 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 ECDSA algorithm to the CNSA variant. A Change Sub-Committee (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 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 variant for Critical Command signing. The DCC believed the overall DCC System impact to be low, although a move to the CNSA 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 initially agreed and subsequently limited the scope of this modification to modify the GBCS to make it explicitly clear that the CNSA variant is permitted.

Later the DCC changed its mind and sought to facilitate the DCC System change via the modification. SECAS and the Working Group agreed for the DCC to carry out a Preliminary Assessment to understand the impacts on the DCC Systems and any associated implementation costs. Following the DCC's Preliminary Assessment and subsequent discussion with TABASC, the DCC again agreed to remove the DSP System change from the scope of the modification. MP129 is therefore a document-only modification and costs will be limited to SECAS time and effort to update the SEC.

The impact of switching to the CNSA variant

Considering the CNSA variant will not be mandated, the DCC noted the impact of switching to the CNSA 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 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 variant will require updates of appropriate documentation, including policies, design of calling and signing functions, and support definitions.
- A switch to the CNSA variant may involve updates to support contracts if it removes the need for special support arrangements for bespoke implementations that are currently in place.

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 business requirements and the Modification Report are 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 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 it had advised the DSP that a caveat will be required to ensure that the CNSA 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 and to report back to the TABASC.

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 future DSP, 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/DSP benefits will be required first. They 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 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.

Support for Change

SMKI PMA views

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

Solution benefits

The benefits of this modification are operational in nature. Moving to the standard CNSA 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 variant following implementation of MP129, 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 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)[1]

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

[1] To facilitate the efficient and transparent administration and implementation of this Code.

Industry views

Industry views will be gathered through the Refinement Consultation.

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.

Appendix 1: Progression timetable

Following the removal of DSP System changes from the modification scope, SECAS will issue a Refinement Consultation on 14 February 2022, which will close on 4 March 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	20 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

Glossary	
Acronym	**Full term**
GBCS	Great Britain Companion Specification
HSM	Hardware Security Module
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
TABASC	Technical Architecture and Business Architecture Sub-Committee
TCoS	Transitional Change of Supplier
XML	Extensible Markup Language