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.

Smart Energy Code

MP129

‘Allowing the use of CNSA variant for ECDSA’

Modification Report

Version 0.5

23 December 2020

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

1. Summary 3
2. Issue 3
3. Solution 4
4. Impacts 4
5. Costs 5
6. Implementation approach 6
7. Assessment of the proposal 6

Appendix 1: Progression timetable 8

Appendix 2: Glossary 9

Contact

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

Joe Hehir

020 7770 6874

Joe.hehir@gemserv.com

1. Summary

This proposal has been raised by David Rollason from the Data Communications Company (DCC).

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. It therefore 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.

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.

The Proposed Solution is to modify the GBCS so that's 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 implementation costs will be limited to the 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 2021 SEC Release.

2. Issue

What are the current arrangements?

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."

What is the issue?

The DSP considers itself to be a Remote Party in this context. It therefore interpreted the GBCS as mandating the GBCS variant of 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 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 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 for Service User buy in and to provide a clean migration path.

What is the impact this is having?

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

Impact on consumers

This issue does not impact consumers.

3. Solution

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.

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

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

This modification will not directly impact any Parties as the CNSA variant for Critical Command signing is already permitted. This modification only seeks make this explicitly clear in the GBCS.

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 9 of this report

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 'GB Companion Specification'
- Schedule 11 'TS Applicability Tables'

Technical specification versions

This modification will 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.

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

This modification will not incur any DCC costs.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. 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 not be associated with this modification.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **4 November 2021** (November 2021 SEC Release) if a decision to approve is received on or before 21 October 2021; or
- **30 June 2022** (June 2022 SEC Release) if a decision to approve is received after 21 October 2021 but on or before 16 June 2022.

This modification will impact the GBCS and, for efficiency, should be implemented in a scheduled SEC Release along with other GBCS changes, minimising SEC Party costs as well. This modification is non-DCC System impacting and will not impact Party systems and therefore will not require any lead-times for testing. This modification will be targeted for the November 2021 SEC Release as this is the next release uplifting the GBCS.

7. Assessment of the proposal

Observations on the issue

SMKI PMA views

The SMKI PMA believes 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 believes 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 variant 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 be 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 agreed and subsequently limited the scope of this modification to modify the GBCS to make it explicitly clear that the CNSA variant is permitted.

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.

Support for Change

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.

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

SECAS categorised this modification as a Low priority when applying its prioritisation criteria to it. The timeline below has been spaced out in line with this in reflection of the current number of open modifications. If steps are able to be completed earlier, SECAS will seek to do so.

SECAS are currently working with the Proposer to draft the legal text, after which a Refinement Consultation will be issued.

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
Update Panel	11 Sep 2020

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
DCC	Data Communications Company
DSP	Data Services Provider
ECDSA	Elliptic Curve Digital Signature Algorithm
GBCS	Great Britain Companion Specification
NIST	National Institute of Standards and Technology
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Technical Specifications
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
XML	Extensible Markup Language