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.

DP129

'Allowing the use of CNSA variant for ECDSA'

Modification Report

Version 0.1

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, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

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 Data Communications Company (DCC).

The Data Services Provider (DSP) considers itself to be a Remote Party in the context of SEC Schedule 8 'GB Companion Specification' (GBCS) Section 4.3.3.2. It therefore interpreted the GBCS as mandating the GCBS 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 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) also agreed that the above GBCS wording lacked clarity and would need to be updated to explicitly permit the use of CNSA by Remote Parties.

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 GCBS as mandating the GCBS variant of ECDSA for all device critical command signing operations, rather than the more common CNSA Suite variant, which is approved by the NIST.

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

The SMKI PMA also 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 GCBS 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 currently precludes the use of the more common CNSA Suite variant. However, the CNSA Suite variant is easier for users to implement and makes the process more efficient.

Appendix 1: Progression timetable

SECAS will ask for the SMKI PMA's views on this Draft Proposal before taking initial comments from the Change Sub-Committee.

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

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**
CNSA	Commercial National Security Algorithm
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
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority