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'

April 2022 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Kev Duddy	SECAS
Anik Abdullah	SECAS
Joey Manners	SECAS
Khaleda Hussain	SECAS
Mike Fenn	SECAS
Tom Mudryk	SECAS
Rainer Lischetzki	SECAS
Elizabeth Woods	SECAS
David Walsh	DCC
David Rollason	DCC
Emma Johnson	British Gas
Alex Hurcombe	EDF Energy
Daniel Davies	ESG Global
Alastair Cobb	Landis+Gyr
Ralph Baxter	Octopus Energy
Mafs Rahman	Scottish Power
Gordon Hextall	Security Sub-Committee (SSC)
Matt Alexander	SSE Networks
Shuba Khatun	SSE Networks
Audrey Smith-Keary	SSE - OVO
Emslie Law	SSE - OVO
Robert Johnstone	Utilita
Kelly Kinsman	WPD

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue identified, the Proposed Solution, the legal text and the implementation approach.

Issue

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.

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.

Legal Text

The legal text change required to deliver this modification is an addition in Smart Energy Code (SEC) Schedule 8 'Great Britain Companion Specification (GBCS)' section 4.3.3.2 which clarifies that the CNSA Suite variant may be used as well as the GBCS variant.

Implementation approach

SECAS recommended 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.

Working Group Discussion

Legal Text

SECAS (MF) advised that the document cited in the GBCS as defining the method for using the CNSA Suite variant has been superseded by another document. The correct reference is being investigated by the Technical Specification Issue Resolution Subgroup (TSIRS) and, once confirmed, will be incorporated into the legal text.

A Working Group member (AA) queried if it was correct to say that this modification will not require DCC System changes. SECAS (MF) clarified that the modification is not mandating that any Party uses the CNSA Suite variant, only providing clarity to Parties that they may use the variant if they wish to. If the DSP or any other Party chooses to switch to using the CNSA Suite variant any system

changes required would be outside of the modification process and the cost would be borne by the Party making the changes, not socialised to industry.

The Working Group agreed that, subject to the confirmation of the legal text, MP129 was ready to proceed to the Report Phase. The Working Group agreed that this modification better facilitated SEC Objective (g)[1], and agreed with the recommended implementation approach.

Next Steps

The following actions were recorded from the meeting:

- SECAS to confirm the correct document reference with TSIRS and amend the legal text accordingly.
- SECAS to present MP129 to the Change Sub-Committee (CSC) for progression to Report Phase.
- SECAS to issue a Modification Report Consultation.

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