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'

December 2021 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Joe Hehir	SECAS
Khaleda Hussain	SECAS
Bradley Baker	SECAS
Joey Manners	SECAS
David Walsh	DCC
Eleanor Taylor	BEIS
Sarah-Jane Russell	British Gas
Lynne Hargrave	Calvin Capital
Steven Bull	DSP (CGI)
Mark Lenton	Haven Power
Julie Geary	E.ON
Alex Hurcombe	EDF Energy
Daniel Davis	ESG Global
Terry Jefferson	EUA
Carmen Strickland	Foresight Metering
Chris Brown	Haven Power
Alastair Cobb	Landis + Gyr
Stuart Blair	Northern Powergrid
Sharon Broadley	Scottish Power
Mafs Rahman	Scottish Power
John Heyburn	SGN
Jeff Studholme	Smart Meter Assets
Audrey Smith-Keary	OVO Energy
Christina Young	OVO Energy
Emslie Law	OVO Energy
Matthew Alexander	SSEN
Gemma Slaney	WPD
Kelly Kinsman	WPD

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue and the Proposed Solution identified in MP129 'Allowing the use of CNSA variant for ECDSA', and the Data Communications Company's (DCC's) Preliminary Assessment response.

Issue

- The Data Services Provider (DSP) has interpreted the 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 variant, which is approved by the National Institute of Standards and Technology (NIST).
- The Department for Business, Energy and Industrial Strategy (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 wording lacked clarity and would need to be updated to explicitly permit the use of CNSA Suite by Remote Parties, as well as the current bespoke GBCS variant.

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, but it will not replace it.

Working Group Discussion

Updated scope of MP129

SECAS provided an overview of the background to the modification, and a summary of the DCC's Preliminary Impact Assessment response. SECAS highlighted that since the Preliminary Assessment had been completed, it had been presented it to the Technical Architecture and Business Architecture Sub-Committee (TABASC) who questioned the business case. As a result, the DCC has since removed the DSP System change from the scope of the modification, with the DCC implementation costs consequently no longer applicable. SECAS noted this makes MP129 a document-only modification with the costs limited to SECAS time and effort to update the SEC.

SECAS provided a summary of the Preliminary Assessment for information but noted the DSP System change is no longer in scope, along with the associated costs. The DSP System change was quoted in the range of £0-£150,000 for Design, Build and Pre-Integration Testing (PIT). A Member (EL) felt the range was not helpful to assessing the business case given the wide range put forward.

A member (MR) questioned whether the DSP would be impacted if adapter providers used the CNSA Suite to sign their Critical Commands. The DSP (SB) advised that it is agnostic to the Critical Command signing method used by the sender and would not be affected if the sender used the CNSA Suite.

Members also questioned what the benefit was for the DSP using the CNSA Suite. The DCC (DW) noted that use of the CNSA Suite is expected to deliver performance improvement for the Smart Metering Key Infrastructure (SMKI) Recovery application amongst other DSP operations such as Enduring Change of Supplier (ECoS) and Hardware Security Modules (HSM) performance. The current version can process about 30 Certificates per second, whilst implementing the CNSA variant would be expected to accelerate this processing to between 300 and 500 Certificates/second. SECAS also noted the DSP would expect a reduction in ongoing maintenance effort and reduce DSP Operational Support charges. However, SECAS advised it had not received any feedback from Parties advising benefits for them. Considering this and the TABASC feedback, the DCC agreed there was no business case for implementing the DSP System change under MP129.

Working Group views against MP129

The Working Group agreed:

- The business case justifies the implementation costs (these costs being those for SECAS time and effort to update the SEC)
- The modification is ready to proceed to Refinement Consultation following the drafting of legal text

Benefits, objectives, and implementation approach

SECAS noted the following Party benefits:

- Provides reassurance that the CNSA Suit variant is permitted for Critical Command signing
- If the DSP chooses to use the CNSA variant, it is expected reduce ongoing maintenance effort and Operational Support charges
- Using the CNSA variant is also expected to deliver performance improvement for the SMKI Recovery application

SECAS noted there are no perceived consumer benefits or impacts and advised MP129 would better facilitate SEC Objective (g)[1] by making it explicitly clear that the GBCS permits the use of the CNSA variant for Critical Command signing. SECAS also highlighted the implementation approach which it will investigate with the DCC but is hoping to target for the November 2022 SEC Release, along with other GBCS impacting modifications. This is considering MP129 now being a document-only modification with a shorter lead-time as a result.

Next Steps

The following actions were recorded from the meeting:

- SECAS to draft the GBCS legal text (between December 2021 and January 2022)
- SECAS to issue a Refinement Consultation following the drafting of the legal text (targeted for February 2022)

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