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'

July 2021 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Holly Burton	SECAS
Bradley Baker	SECAS
Joe Hehir	SECAS
Kev Duddy	SECAS
Piers Garton	SECAS
Joey Manners	SECAS
Mike Fenn	SECAS
Khaleda Hussain	SECAS
Anik Abdullah	SECAS
Remi Oluwabamise	DCC
Robin Seaby	DCC
David Walsh	DCC
Abhijit Pal	DCC
Graeme Liggett	DCC
Sarah-Jane Russell	British Gas
Lynne Hargrave	Calvin Capital
Julie Geary	E.ON
Robert Williams	E.ON
Alex Hurcombe	EDF Energy
Daniel Davies	ESG Global
Terry Jefferson	EUA
Alastair Cobb	Landis + Gyr
Alan Creighton	Northern Power Grid
Ralph Baxter	Octopus Energy
Andy McFaul	Ofgem
Emslie Law	OVO Energy
Mafs Rahman	Scottish Power
Elias Hanna	Smart ADSL
Matthew Alexander	SSE
Simon Willcox	Stark
Naeem Saleem	UK Power Networks

Rachel Norberg	Utilita
Gemma Slaney	WPD
Kelly Kinsman	WPD

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue identified, the current business requirements and proposed next steps.

Issue

The Data Services Provider (DSP) has interpreted the GB Companion Specification (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, which is approved by the National Institute of Standards and Technology (NIST).

The Department of 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 variant and remained compliant.

The Smart Metering Key Infrastructure Policy Management Authority (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.

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.

Working Group Discussion

A Working Group member sought clarity on the issue. SECAS (JHe) confirmed that this is in relation to the critical command signing. There is another variant which is more frequently used and DSP has advised is more efficient. However, it is not permitted for use in the GBCS. SECAS highlighted that the proposal is for the CNSA variant to be permitted alongside the ECDSA variant, not to replace it. Therefore, it will be optional which variant Parties use.

This raised questions around how costs would be picked up for those Parties that do choose to switch to the CNSA variant, given it is not being enforced.

The Technical Architecture and Business Architecture Sub-Committee (TABASC) Chair (JH) added that the modification would only impact those Parties looking to switch algorithms and that it should

improve efficiency. Therefore, over the long-term, cost savings should be achieved. They added that the DSP has advised it should be a low-cost change.

A Working Group member (EL) question this modification would incur the cost for any Parties that were looking to switch variant. A Working Group member (GS) questioned if this would only be a legal text change and why a Preliminary Assessment is being carried out. SECAS (JHe) advised it would request a Preliminary Assessment to gain a clearer understanding of the implementation costs.

A Working Group member (EH) added that any comment on the DSP change or implementation costs would be an assumption until a Preliminary Assessment was carried out.

A Working Group member (RB) questioned why the CNSA variant needs to be permitted in the SEC. They advised that if we have been living with ECDSA variant, why are we being asked for money to make this change. SECAS agreed that this is a question that needs answering and that the costs need to be determined before any further steps are taken.

SECAS (AB) added that there have been discussions internally with the DCC about who is responsible for any costs needed to switch variant. The legal text change to the SEC is to confirm the CNSA variant is permitted alongside the ECDSA variant and it was expected that this would not have any direct DCC or SEC Party System impacts.

There was an agreement to request a Preliminary assessment, and define the costs moving forward. The Preliminary Assessment will then be discussed at the Working Group alongside any business case.

Next Steps

The following actions were recorded from the meeting:

- SECAS (PG) will request a Preliminary Assessment from the DCC to determine any implementation costs.