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'

September 2020 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Joe Hehir	SECAS
Joey Manners	SECAS
Glenn Critchley	DCC
David Walsh	DCC
Robert Munro	DCC
Mari Toda	DCC
Simon Trivella	British Gas
Alex Hurcombe	EDF
Paul Saker	EDF
Rob Williams	E.ON
Alastair Cobb	Landis + Gyr
Elias Hanna	Landis + Gyr
John Noad	Npower
Mahfuzar Rahman	Scottish Power
Emslie Law	SSE/OVO
Matthew Alexander	SSEN
Rachel Norberg	Utilita
Gemma Slaney	WPD

Issue

SECAS explained the current GB Companion Specification (GBCS) requirements for cryptographic signing, specifically Section 4.3.3.2. This defines how a Smart Metering Entity should create a "Per-Message Secret Number 'k' with respect to Elliptic Curve Digital Signature Algorithm (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.

A Smart Metering Entity is defined as, *an entity that is either a Device or a Remote Party* and 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*.

The Data Services Provider (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 Commercial National Security Algorithm (CNSA) Suite variant, which is approved by the National Institute of Standards and Technology (NIST).

Party feedback

Smart Energy Code Administrator and Secretariat (SECAS) highlighted that the Department for Business, Energy and Industrial Strategy (BEIS) advised that this was a DSP interpretation which was overly restrictive and that it 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. The DCC noted that making the CNSA variant optional may lead to difficulties in the DCC developing a solution.

Solution options

SECAS presented two solution options:

1. A text only change to the GBCS permitting the use of the CNSA variant
2. DSP System change to facilitate the necessary system changes to use the CNSA variant (requirement a Preliminary Assessment)

SECAS advised that if this proposal were to be approved and give Parties the right to switch to the CNSA, the impact it has is at the discretion of each signing Party.

The DCC believes the overall DCC System impact to be low, although a move to the CNSA variant for the DCC will 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.

The Working Group had no other comments.

Next steps

The following actions were recorded from the meeting:

- SECAS will draft the GBCS legal text giving clarity that the CNSA variant is permitted.
- SECAS will request a DCC Preliminary Assessment for the DCC to make the necessary system changes for the DSP to use the CNSA variant.