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.

MP168 'CPL Security Improvements'

May 2022 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Elizabeth Woods	SECAS
Kev Duddy	SECAS
Adam Musgrave	SECAS
David Walsh	DCC
Emma Johnson	British Gas
Julie Geary	E.ON
Alex Hurcombe	EDF Energy
Daniel Davies	ESG Global
Martin Bell	EUA
Alastair Cobb	Landis+Gyr
Ralph Baxter	Octopus Energy
Mafs Rahman	Scottish Power
Matthew Alexander	SSE Networks
Shuba Khatun	SSE Networks
Audrey Smith-Keary	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 business requirements and the Proposed Solution.

Issue

- SEC Appendix Z 'CPL Requirements Document' details the requirements for Devices to be allowed on the Central Products List (CPL).
- Device Manufacturers are required to Digitally Sign the CPL Submission if it contains the Hash of a Manufacturer Image.

- DCC or Suppliers are required to provide those details to the Panel (via SECAS).
- The SEC Panel (via SECAS) authenticates the CPL submission originates from the person who created the Image and is endorsed by a Supplier.
- The SSC established this authentication of the manufacturer signing the CPL Submission is not sufficient.
- The Supplier or the DCC sends the confirmation via email.
- Therefore, neither a Supplier nor the SEC Panel can fully meet the SEC obligation.

Proposed Solution

- The DCC will become the Issuing Certificate Authority (CA) for x.509 certificates and issues Certificates to Device Manufacturers and Suppliers to use.
- Device Manufacturers digitally sign the CPL submission spreadsheet and pass to the Supplier (Devices) or DCC (Communications Hubs).
- The Supplier or DCC must then apply a secondary signature to the CPL submission.
- SECAS checks the validity of the Certificates against the Certificate Revocation List (CRL).

Business Requirements

1. The DCC shall publish the Infrastructure Key Infrastructure (IKI) Certificate Revocation List (CRL) on-line for a range of uses that require authentication via IKI (e.g. CPL submissions).
2. Any organisation that needs to authenticate IKI Certificates is given access to and is required to check the CRL when receiving requests authenticated with an IKI Certificate.
3. It shall be possible for non-SEC Parties (e.g. Device Manufacturers) to apply for Certificates.

Working Group Discussion

Proposed definitions

SECAS (KD) provided an overview of the issue, the Proposed Solution and the associated business requirements.

The DCC (DW) queried the acronyms used within the presentation, noting that Issuing Certificate Authority could be 'ICA'. SECAS resolved to confirm this, but suggested as there are a variety of Certificate types, that 'CA' was correct. SECAS has since confirmed that 'ICA' is specific to IKI Certificate Authority.

A Working Group member (AC) queried whether this modification sought to change the certificates on the CPL submission, or on the image. SECAS advised this is aimed at addressing the Certificates used to verify the CPL submissions. They also questioned whether the intent is that each Supplier that uses the product needs to provide a submission. SECAS confirmed that the intention is just one Supplier per submission for the CPL as the process stands currently.

Another Working Group member (AS) queried how the CRL would be made public. SECAS confirmed that it would need to be accessible via a standard internet browser to ensure any Party could access it.

One Working Group member (AC) questioned what the implementation timescales were for the modification. They noted that Device Manufacturers hold multi-year agreements with Issuing CAs and this would need to be considered when determining an implementation date. SECAS noted this and confirmed that the implementation date would be considered in full once the DCC Preliminary Assessment had been returned.

Next Steps

The following actions were recorded from the meeting:

- SECAS will engage Device Manufacturers directly to identify impacts; and
- SECAS will request the DCC Preliminary Assessment.