

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.



DP168 'CPL Security Improvements'

Modification Report

Version 0.1

11 June 2021

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

| | |
|---|---|
| 1. Summary..... | 3 |
| 2. Issue..... | 3 |
| Appendix 1: Progression timetable | 5 |
| Appendix 2: Glossary | 5 |

Contact

If you have any questions on this modification, please contact:

Joe Hehir

020 7770 6874

joe.hehir@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC).

Smart Energy Code (SEC) Appendix Z 'CPL Requirements Document' requires the Panel to check that a communication requesting a firmware Image to be associated with a Device Model on the Central Products List (CPL) originates from the person who created the Image and is endorsed by a Supplier. At present, the nature of the signatures used by manufacturers do not enable cryptographic authentication that the communication originates from a specific manufacturer beyond reasonable doubt. Neither a Supplier nor the Panel can therefore suitably verify the authenticity of the communication and therefore fully meet the SEC obligation.

The SSC considers that there are readily available commercially effective solutions that can be adopted by the Data Communications Company (DCC) as an extension to the Infrastructure Key Infrastructure (IKI) service. Therefore, the SSC, with support from the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA), wishes to address the current SEC compliance issue and improve the security controls.

2. Issue

What are the current arrangements?

What is the Central Products List?

The DCC uses the CPL to manage the Devices it can communicate with. If a Device is not listed on the CPL, a User cannot communicate with it other than to update the firmware to a version that is on the CPL. Only once a Device has met the requirements set out in the CPL Requirements Document can it be added to the CPL. The CPL is a list of Device Models that are either:

- Smart Metering Equipment Technical Specifications (SMETS) 2 Devices which have received all relevant Assurance Certificates; or
- SMETS1 Devices which have been notified by the DCC and have been included as entries on the SMETS1 Eligible Products Combination list.

SEC Section F 'Smart Metering System Requirements' (section 2) defines the CPL and is supplemented by SEC Appendix Z.

Validating CPL entries

SEC Appendix Z sections 4.1 and 4.3 require the SEC Panel to check that a communication requesting a firmware Image to be associated with a Device Model on the CPL originates from the person who created the Image and is endorsed by a Supplier. In practice this is carried out via SECAS on behalf of the Panel.

Relevant extract from Appendix Z

The following is an extract from version 2.0 of SEC Appendix Z setting out the obligations for associating a Hash (in relation to a firmware Image) with a Device Model on the CPL:

4. Association of Hashes with Device Models on the CPL

- 4.1 *Where the DCC or a Supplier Party wishes the Panel to associate the Hash of a Manufacturer Image with a Device Model on the Central Products List, that Party shall provide the Hash and the identity of the person who created the Manufacturer Image in a communication to the Panel which has been Digitally Signed by the person who created the Manufacturer Image in a manner that reasonably enables the Panel to check that the communication originates from the person who created the Manufacturer Image.*
- 4.2 *The Panel may specify the format which the communication referred to in Clause 4.1 must take (in which case Parties sending such communications must use such format). The Panel shall notify the relevant Parties of any such required format and of any changes to such required format that the Panel may make from time to time.*
- 4.3 *The Panel shall only associate a Hash provided under Clause 4.1 with a Device Model on the Central Products List where:*
 - (a) *the Panel has successfully confirmed that the Digital Signature referred to in Clause 4.1 is that of the person who created the Manufacturer Image (validated as necessary by reference to a trusted party);*
 - (b) *there is no Hash currently associated with the Device Model; provided that, if there is a Hash currently associated with the Device Model, the Panel shall investigate the matter with the relevant Parties to identify whether it is appropriate to replace the associated Hash (and shall, where it is appropriate to do so, update the Central Products List accordingly); and*
 - (c) *if the Device Model is a SMETS1 Device Model, the communication to the Panel referred to in Clause 4.1 is from the DCC.*

What is the issue?

At present, the nature of the signatures used by manufacturers do not enable cryptographic authentication that the communication originates from a specific manufacturer beyond reasonable doubt. Neither a Supplier nor the SEC Panel can therefore suitably verify the authenticity of the communication. The SEC Panel therefore cannot fully meet the SEC obligation. SEC Appendix Z section 4.2 allows the SEC Panel to specify the format which the communication referred to in section 4.1 must take.

The SSC has considered the security implications and considers that there are commercially available solutions that are readily available that can be adopted by the DCC as an extension to the IKI service. Therefore, the SSC, with support from the SMKI PMA, wishes to address the current SEC compliance issue and improve the security controls.

What is the impact this is having?

If this issue is not resolved, the Panel will not be able to fully authenticate communications requesting a firmware Image to be associated with a Device Model on the CPL originates from the person who created the Image and is endorsed by a Supplier.

Impact on consumers

Although there are controls in place to prevent this, if this issue is not resolved, it may increase an easily avoidable risk of consumer smart metering Devices receiving improperly authorised or, in the worst case, malicious firmware.

Appendix 1: Progression timetable

This proposal will be presented to Change Sub-Committee (CSC) for initial comment on 29 June 2021.

| Timetable | |
|--------------------------------------|-------------|
| Event/Action | Date |
| Draft Proposal raised | 11 Jun 2021 |
| Presented to CSC for initial comment | 29 Jun 2021 |

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

| Glossary | |
|----------|---|
| Acronym | Full term |
| CPL | Central Products List |
| CSC | Change Sub-Committee |
| DCC | Data Communications Company |
| IKI | Infrastructure Key Infrastructure |
| SEC | Smart Energy Code |
| SECAS | Smart Energy Code Administrator and Secretariat |
| SMETS | Smart Metering Equipment Technical Specifications |
| SMKI PMA | Smart Metering Key Infrastructure Policy Management Authority |
| SSC | Security Sub-Committee |