

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.



DP211

‘Aligning the SMI with the CPL’

Modification Report

Version 0.2

9 August 2022

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
3. Assessment of the proposal	4
Appendix 1: Progression timetable	5
Appendix 2: Glossary	6

Contact

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

Kev Duddy

020 3574 8863

kev.duddy@gemserv.com

1. Summary

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

The policy intent is that the Data Communications Company (DCC) should only communicate with Devices that have their Device Model listed on the Central Products List (CPL). Once the Device Model is marked as removed on the CPL, then the DCC has an obligation to suspend any Device within the Smart Metering Inventory (SMI) that has that Device Model.

The intended security objective is for the Smart Energy Code (SEC) to cater for Devices that do not have a matching Device Model on the CPL to be prevented from communicating with the DCC. However, at present the SEC only caters for Devices being suspended if the Device Model is marked as removed on the CPL. The SEC doesn't explicitly cater for preventing a Device that isn't already on the CPL from communicating with the DCC.

2. Issue

What are the current arrangements?

Central Products List

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.

Only once a Device Model has met the requirements set out in SEC Appendix Z 'CPL Requirements Document' can it be added to the CPL.

If a Device Model has an Assurance Certificate withdrawn, cancelled or expire, then the Panel shall mark that Device Model as removed on the CPL. In the case of expiry of Commercial Product Assurance (CPA) Certificates, this removal would be up to the discretion of the SSC in line with SEC Appendix Z, section 6.

Once the Device Model is removed from the CPL, then the DCC has an obligation to suspend any Device within the SMI that has that Device Model.

At present, the SEC only caters for Devices being suspended if the corresponding Device Model has been **removed** from the CPL. It does not explicitly cater for Devices where the Device Model has never been placed on the CPL.

DCC System validation

The DCC uses the CPL to manage the Devices it should communicate with. For Devices to be added initially to the Smart Metering System they must be pre-notified by the Supplier to the DCC. This pre-notification is validated by the DCC to ensure that the Device Model appears on the CPL. The DCC

can then add these Devices to the SMI if it passes the validation. If a Device Model is not listed on the CPL, it should not be added to the SMI and therefore should not be communicated with.

A similar process exists when a Supplier wishes to update the firmware on a Device. The firmware is sent by the Supplier via Service Request Variant (SRV) 11.1 'Update Firmware' and then activated using a follow up SRV 11.3 'Activate Firmware'. Both SRVs validate the firmware version against the CPL in the same way.

What is the issue?

The policy intent is that any Device Model that is not on the CPL should not be added to the SMI and any Devices that have been removed from the CPL should be suspended. However, SEC Section H 'DCC Services' defines the DCC's responsibilities, and SEC Section H6.10 only states the Device should be suspended if the Device Model has been removed from the CPL:

H6.10 Where a Device's Device Model is removed from the Central Products List, that Device shall be Suspended and the DCC shall set the SMI Status of the Device to 'suspended'.

A scenario has been identified that does allow a firmware version that is not on the CPL to be live on the SMI. For security reasons, the SSC does not wish to disclose the detail of how this can occur but does wish the SEC wording to be clarified to prevent the scenario from re-occurring in future.

What is the impact this is having?

There is potential for Suppliers to be responsible for Devices that are operating with unauthorised firmware on the CPL. This also increases a security risk that Devices could introduce security vulnerabilities if the Device model does not appear on the CPL.

Impact on consumers

Whilst this issue does not directly impact Consumers, there is an increased security risk that a consumer's Device could be operated with an incorrect or unauthorised firmware.

3. Assessment of the proposal

Areas for assessment

Sub-Committee input

As part of the modification assessment, the Smart Energy Code Administrator and Secretariat (SECAS) engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the SSC and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums.

SECAS believes the following Sub-Committees will need to input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	None – No impact on operational processes
SMKI PMA	None – No impacts on the SMKI document set
SSC	SSC will manage this modification outside of approvals
TABASC	None – TABASC Chair attends SSC to provide view on architecture

Due to the confidentiality of the security risk, SECAS recommends that the SSC acts as the Working Group for this modification and provides recommendations for the Change Sub-Committee and Change Board with regards to approvals.

Observations on the issue

How many Devices could be affected?

The initial scenario presented to SECAS is a symptom of the problem. The issue is that the security loophole needs to be closed. There is a potential risk to Critical National Infrastructure (CNI) which could require hundreds of thousands of Devices needing to be replaced if this issue is not addressed. This would be very costly and incur reputational damage for Suppliers and the Smart Metering Programme. The SSC has carried out an assessment and believes this risk needs to be addressed.

Appendix 1: Progression timetable

This proposal will be presented to the Change Sub-Committee (CSC) on 16 August 2022 for final comment on the issue. SECAS recommends it is converted to a Modification Proposal. SECAS and the SSC will then develop the business requirements for the DCC to conduct the Preliminary Assessment against.

Timetable	
Event/Action	Date
Draft Proposal raised	12 Jul 2022
Presented to CSC for initial comment	19 Jul 2022
SECAS to work with DCC & the SSC to determine scale of issue & possible system impacts	Late Jul 2022
CSC converts Draft Proposal to Modification Proposal	16 Aug 2022
Business requirements developed with SSC	Aug 2022
Preliminary Assessment requested	29 Aug 2022
Preliminary Assessment returned	7 Oct 2022
Modification discussed with SSC	26 Oct 2022
Refinement Consultation	31 Oct – 18 Nov 2022
Modification discussed with SSC	26 Oct 2022
Impact Assessment costs approved by Change Board	21 Dec 2022

Timetable	
Event/Action	Date
<i>Impact Assessment requested</i>	21 Dec 2022
<i>Impact Assessment returned</i>	3 Mar 2023
<i>Modification discussed with SSC</i>	22 Mar 2023
<i>Modification Report approved by CSC</i>	18 Apr 2023
<i>Modification Report Consultation</i>	19 Apr – 10 May 2023
<i>Change Board Vote</i>	31 May 2023

Italics denote planned events that could be subject to change

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
CNI	Critical National Infrastructure
CPA	Commercial Product Assurance
CPL	Central Products List
CSC	Change Sub-Committee
DCC	Data Communications Company
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specifications
SMI	Smart Metering Inventory
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SRV	Service Request Variant
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee