

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.



DP222

‘CPL submission efficiency improvements’

Modification Report

Version 0.2

13 December 2022



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	6
Appendix 1: Progression timetable	7
Appendix 2: Glossary	7

Contact

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

Bradley Baker

020 7770 6597

bradley.baker@gemserv.com

1. Summary

This proposal has been raised by Martin Bell from the Energy and Utilities Alliance (EUA).

The Data Communications Company (DCC) uses the Central Products List (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.

At present, a Device Manufacturer can add a new Device to the CPL without any Supplier intervention. However as soon as the same Device requires a change to hardware or firmware, it must have Supplier endorsement before it can be updated on the CPL. Where there is no Supplier endorsement for a new Device hardware or firmware version, the Device Manufacturer cannot progress with the CPL submission. Hence a product that has gone through rigorous Certified Product Assurance (CPA) and other relevant assessments cannot be listed or used.

This modification does not intend to alter the processes for adding new Communications Hub Device Models to the CPL or associate these with a hash. This modification relates to Smart Metering Equipment Technical Specifications (SMETS) 2 Devices only.

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 Model is not listed on the CPL, a User cannot communicate with it other than to update the firmware to a Device Model version that is on the CPL. Only once a Device Model has met the requirements set out in the SEC Appendix Z 'CPL Requirements Document' can it be added to the CPL.

The CPL is a list of Device Models that are either:

- SMETS2 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 (for clarification this modification does not impact SMETS1 Devices)

Smart Energy Code (SEC) Section F 'Smart Metering System Requirements' defines the CPL and is supplemented by the CPL Requirements Document. Suppliers may use the information contained within the CPL to make efficient decisions when choosing products that may be available, which includes updated products. However, Suppliers are not obligated to use the CPL for this purpose.

Validating CPL entries

The CPL Requirements Document requires the Panel to check that a CPL submission is valid before being added to the CPL. Each time a new Device (whether it be a new hardware or firmware version) is added, a new version of the CPL entry is created. In practice this is carried out by the Smart Energy Code Administrator and Secretariat (SECAS) on behalf of the Panel.

SECAS validates whether the CPL submission has the required Assurance Certificates (CPA, ZigBee, Device Language Message Specification (DLMS) / Companion Specification for Energy Metering (COSEM)) and whether the Device Model details are unique.

Adding Device Models to an existing CPA certificate

Additional Device Models can be added to an existing CPA certificate: The DCC (for Communications Hubs) and the Supplier (for all other Devices) can notify the Panel in order to list these Device Models on the CPL (the Manufacturer is not able to do this). The DCC or the Supplier can only do this in accordance with the relevant CPA Assurance Maintenance Plan and must retain the evidence of having acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan. The Panel or the Authority can request this evidence.

Supplier testing of a Device

For any new or updated product that is intended for CPL inclusion, Manufacturers take the Device through intensive pre-defined CPA approval activities which demonstrate that the security functions of the Device meet the Security Characteristics as defined by the National Cyber Security Centre (NCSC) standards.

This differs from Supplier testing, which is geared more to ensuring the Device integrates into the Supplier's individual smart metering solution, for example when the Supplier runs its individual business processes and sends relevant Service Requests. To summarise, current Supplier testing of any metering Device is bespoke to the individual Supplier business requirements.

The CPL submission will then be submitted by the Manufacturer, supported by the Supplier's endorsement. SECAS will then process the submission and publish a new version of the CPL.

Once the new version has been added to the CPL, Suppliers are under no compulsion to take a new Device Model release if they have not tested it. Hence in reality there is no difference between a new or updated product being submitted to the CPL. However, having releases ready with fixes that the Manufacturer has already taken through CPA and other required CPL submission criteria (ZigBee / DLMS as required) will be beneficial to the efficient deployment of fixes, including operational and potentially security fixes by avoiding the challenge of delays in finding Supplier resource to do this.

Associating a Device Model with a hash

Currently, a Supplier must present the hash to SECAS for CPL submission; it cannot be the manufacturer.

A hash enables an updated firmware to be paired to the correct Device when an update is carried out.

Devices can apply the specific Hash function themselves. Upon receipt of a Manufacturer Image, the Device calculates the Hash. If the hash it calculates differs from that which is listed on the CPL, it is an indication that the firmware provided to the Device is not what the Supplier intended. Therefore, it will reject any installation commands.

Newly CPL-registered Device Models that may not initially contain a hash can be installed, commissioned, and used by the Supplier. When a Supplier chooses to update its Devices, the Device Model on the CPL that will feature the firmware upgrade will require a hash. The image hash is created by the Device Manufacturer.

What is the issue?

Supplier endorsement

Under current arrangements, a Device Manufacturer is not permitted to update an existing CPL-registered Device without the endorsement of a Supplier. Where there is no Supplier endorsement for a new Device hardware or firmware version, the Device Manufacturer cannot progress with the CPL submission, hence a product that has gone through rigorous CPA and other relevant assessments cannot be listed or used.

Furthermore, SEC Appendix Z (Section 5.2) refers to Suppliers following a CPA Assurance Maintenance Plan when a new firmware or hardware version is being submitted for CPL inclusion. However, Manufacturers manage this process, with the oversight of the SSC and the NCSC.

The Device Manufacturer compiles and keeps all relevant evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, should the Panel or the Authority request this. This obligation is the responsibility of the Supplier, however Suppliers fully devolve this responsibility of creating CPL updates in line with this process through the relevant Device Manufacturer.

Efficiencies identified with obtaining an image hash

The Proposer believes that as the Device Manufacturer creates the image hash for its Device, then provided the Device is CPA approved, there should be no reason why the Device Manufacturer cannot submit the hash for the CPL submission.

What is the impact this is having?

Not having a Supplier endorsement in place is stopping updated products coming to the GB Smart Metering market, hence unnecessarily delaying fixes (operational and potentially security) and potentially stifling competition, and procurer's choice. This is likely to increase as new initiatives and industry challenges arise. In theory, a Manufacturer could design a Device featuring new technology, however without a Supplier's endorsement, that Device is unlikely to be purchased and installed as it cannot be updated. As fuels change, for example with the introduction of hydrogen, new Devices will have to be built and installed.

During the Device lifecycle, Manufacturers must take products through operational fixes and issue resolutions. Suppliers may have other priorities which impacts ability to test these changes until the point they decide to use the changed Device. Such circumstances should not hold up CPL inclusion.

Furthermore, the inability to be able to immediately update existing in-stock Devices immediately post Installation and Commission, means that the original CPA listed Device is unlikely to be procured and used.

Impact on consumers

If Device updates cannot be added to the CPL, Suppliers may be left with Devices that are delivering sub-optimal performance and Manufacturers are restricted in their ability to communicate the availability of important fixes which could result ultimately in meter removal.

3. Assessment of the proposal

Areas for assessment

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC) and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums. The key points can be found below:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	The OPSG Chair has requested that updates are provided offline.
SMKI PMA	No anticipated SMKI impacts from this proposal.
SSC	Are there security implications from removing Supplier endorsements from CPL submissions? This will be investigated once the modification enters the Refinement Process.
TABASC	How will this proposal impact the smart metering technical and/or business architecture? This has been discussed with the TABASC Chair, and with the Proposed Solution likely to be a governance change, there will be no technical and/or business architecture changes. The TABASC Chair will be kept up to date as the modification progresses,

Observations on the issue

Views of the Change Sub-Committee

SECAS presented the Draft Proposal to the Change Sub-Committee (CSC) for initial comments in November 2022. A Manufacturer representative commented that an issue they experience is where it can take up to two weeks to get a Supplier to send their supporting statement to SECAS to allow the CPL inclusion to be processed. They added that this delay can cause major inconvenience if the update to the Device includes an urgent fix.

Initial SSC discussions

SECAS sought initial views from the SSC while in the Development Stage. The SSC commented that there is a difference between a new Device model and one that is already installed. It stated that Suppliers can choose to purchase the new Device model based on the results of the testing carried out prior to CPL inclusion, whereas the Supplier is not obliged to purchase a new firmware version for the installed Device.

SECAS informed the SSC that it would return to the Sub-Committee once solutions have been put forward and have been discussed with the Working Group.

Views from the SEC Panel

The Panel provided feedback on the Draft Proposal where a member, though supportive of the proposal, stated that it should be investigated to see if there is a viable solution that can be taken forward, rather than using up excess time and effort on a solution that is likely to be rejected. SECAS has informed the Proposer of this view.

Appendix 1: Progression timetable

SECAS has presented this proposal to the SEC Sub-Committees for initial comment and will return this to the Change Sub-Committee on 20 December 2022 under the recommendation that it proceeds to the Refinement Process. SECAS will then develop the business requirements and Proposed Solution. SECAS will then present the modification to the Working Group and the SSC.

Timetable	
Event/Action	Date
Draft Proposal raised	7 Nov 2022
Presented to CSC for initial comment	15 Nov 2022
Presented to Sub-Committees for initial comment	Nov – Dec 2022
CSC converts Draft Proposal to Modification Proposal	20 Dec 2022
<i>Business requirements developed with the Proposer</i>	Dec 2022
<i>Proposed Solution developed with the Proposer</i>	Dec 2022
<i>Legal text developed with the Proposer and SEC Lawyer</i>	Jan 2023
<i>Modification discussed with Working Group</i>	1 Feb 2023
<i>Modification discussed with the SSC</i>	22 Feb 2023
<i>Refinement Consultation</i>	27 Feb 2023 – 17 Mar 2023
<i>Modification Report approved by CSC</i>	18 Apr 2023
<i>Modification Report Consultation</i>	19 Apr – 10 May 2023
<i>Modification approved by Change Board</i>	31 May 2023

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
COSEM	Companion Specification for Energy Metering
CPA	Certified Product Assurance
CPL	Central Products List
CSC	Change Sub-Committee

Glossary	
Acronym	Full term
DCC	Data Communications Company
DLMS	Device Language Message Specification
EUA	Energy and Utilities Alliance
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	The 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
TABASC	Technical Architecture and Business Architecture Sub-Committee