

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.

Smart Energy Code

# MP222

## ‘CPL submission efficiency improvements’

### Modification Report

Version 1.0

19 April 2023

Corporate member of  
Plain English Campaign  
Committed to clearer  
communication

592



## About this document

---

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

## Contents

---

1. Summary.....	3
2. Issue.....	3
3. Solution .....	6
4. Impacts.....	7
5. Costs .....	8
6. Implementation approach .....	9
7. Assessment of the proposal .....	9
8. Case for change.....	10
Appendix 1: Progression timetable .....	11
Appendix 2: Glossary .....	12

This document also has three annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** contains the full responses received to the Refinement Consultation.

## Contact

---

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

**Bradley Baker**

020 7770 6597

[bradley.baker@gemserv.com](mailto: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 proposes to remove the requirement for Supplier Parties to have to endorse hardware or firmware revisions to pre-existing CPL-listed Device Models. It will also allow Manufacturers to submit Hash Images directly as part of the CPL submission.

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 Image. This modification relates to Smart Metering Equipment Technical Specifications (SMETS) 2 Devices only.

This is a Self-Governance modification and will impact Suppliers and Device Manufacturers. There are no DCC-associated implementation costs. Implementation is targeted for the June 2023 SEC Release (29 June 2023).

## 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 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)

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 to be installed in consumers' premises, 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)), the required Companion Specification for Energy Metering (COSEM), and whether the Device Model details are unique (to avoid duplicated entries).

### **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 focused more on 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 obligation 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 or 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 Image**

Currently, a Supplier must present the Hash Image to SECAS for CPL submission; it cannot be the Manufacturer. A hash enables an updated firmware version to be paired to the correct Device when an update is carried out. Upon receipt of a Manufacturer Image, the Device calculates the hash. If the Hash Image 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 the update firmware activation 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 Hash Image is created by the Device Manufacturer.

## What is the issue?

### Supplier endorsement

At present, a Device Manufacturer can add a new Device to the CPL without any Supplier endorsement. However, 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, in practice, Manufacturers manage this process, with the oversight of the Security Sub-Committee (SSC) and the NCSC, not Suppliers.

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 a Hash Image

The Proposer believes that as the Device Manufacturer creates the Hash Image for its Device, and provided the Device is CPA approved, there should be no reason why the Device Manufacturer cannot submit the Hash Image for the CPL submission as it is responsible for the necessary regulatory approvals to achieve this. Whilst initially it was envisaged that the Supplier would monitor Manufacturers' CPA Assurance Maintenance Plans, the reality is that Suppliers have fully devolved this to Manufacturers and hence this proposal is ensuring that processes are aligned.

## What is the impact this is having?

Not having a Supplier endorsement in place is stopping updated products coming to the Smart Metering market of Great Britain. This unnecessarily delays fixes (operational and potentially security fixes), and potentially stifles competition as well as 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.

During the Device lifecycle, Manufacturers must take products through operational fixes and issue resolutions. Suppliers may have other priorities which impact their ability to test these changes until

the point they decide to use the changed Device. The Proposer believes that such circumstances should not hold up CPL submissions.

Furthermore, the inability to be able to immediately update existing in-stock Devices 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. Solution**

---

### **Proposed Solution**

The Proposed Solution is to remove the requirement for a Supplier Party to provide endorsement or approval for a firmware or hardware revision to a SMETS2 Device that is currently listed on the CPL. This will result in a more efficient process when making updates available to pre-existing CPL-listed Devices.

By removing the Supplier endorsement from a Manufacturer's CPL submission, the Manufacturer is solely responsible for the CPA Assurance Maintenance Plan. They will provide the documentation to the CPL submission process directly and fulfil any questions that might arise without unnecessary delay. For clarity, this does not force the Supplier to deploy the update but is designed to enable a Supplier to do this more quickly and take advantage of available certified firmware without undue delay. This modification will not impact the current CPA certification process.

The Proposed Solution will also enable the Manufacturer (provided it is a SEC Party) to submit the Hash Image, without it having to be submitted via a Supplier Party as currently required.

This is a proposed governance change and will not impact DCC Systems.

For clarity, SEC Appendix Z 'CPL Requirements Document' will be amended to state that Supplier Parties and Manufacturers who are SEC Parties can submit CPL submissions, but that if a Manufacturer creates a submission, the Supplier Party endorsement will not be required. If the Manufacturer is not a SEC Party, it will have to abide by the current obligations and seek the Supplier's endorsement.

The business requirements for this solution can be found in Annex A.

### **MP168 'CPL Security Improvements'**

SECAS has investigated the potential link that MP222 will have with [MP168 'CPL Security Improvements'](#). MP168 seeks to add a further level of security to CPL submissions by validating that the correct individual has signed the CPL submission using the DCC Infrastructure Key Infrastructure (IKI) token. This will be validated against the Certificate Revocation List (CRL).

If MP222 is approved, the Supplier Party representative will no longer be required to endorse a Manufacturer's CPL submission and would not be required to sign the submission. When developing the Proposed Solution with the SSC, it was agreed that Supplier Parties will still be able to submit CPL submissions. This means that if both modifications are implemented, Supplier Parties and Manufacturers will require DCC IKI tokens to sign CPL submissions that include Hash Images. The SSC approved of this additional security check. To clarify, if MP168 is not approved, Manufacturers will have to sign submissions containing Hash Images via a trusted Certification Authority.

## 4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

### SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
	Electricity Network Operators		Gas Network Operators
✓	Other SEC Parties		DCC

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
✓	Device Manufacturers		Flexibility Providers

Device Manufacturers will be impacted by this change as they will be responsible for submitting firmware and or hardware revisions for pre-existing CPL-listed SMETS2 Devices directly to SECAS without Supplier endorsement.

Supplier Parties will be impacted by this change as they may no longer need to be involved in submitting SMETS2 CPL submissions.

The DCC will experience no impact as, once completed, the updated CPL is uploaded into its system using the existing business as usual (BAU) process.

### DCC System

This modification will have no impact on the DCC System.

### SECAS

This modification will not result in further work for SECAS, however the team that process CPL submissions will need to be aware that the modification has been implemented.



## SEC and subsidiary documents

The following parts of the SEC will be impacted:

- SEC Section F 'Smart Metering System Requirements' (housekeeping change)
- Appendix Z 'CPL Requirements Document'

The changes to the SEC required to deliver the proposed solution can be found in Annex B.

## Consumers

This modification will have a positive impact on consumers as updates that include fixes to installed Devices will be made available more quickly than the current process allows.

## Other industry Codes

This modification will have no impact on other industry Codes.

## Greenhouse gas emissions

This modification may result in new technologies being implemented into the smart infrastructure that will allow consumers to better manage their energy usage and therefore reduce greenhouse gas emissions.

# 5. Costs

---

## DCC costs

This modification has no associated DCC costs.

## SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

## SEC Party costs

SECAS received two responses to the Refinement Consultation from a Network Party, who are not impacted by this change, with therefore no associated costs, and a Large Supplier. The Large Supplier stated that no significant cost will be incurred or saved because of the change as their overall testing process for new firmware will not be heavily impacted. They advised that the main impact they will see is the Manufacturer not having to wait for the Supplier to complete their own internal testing before being able to list the new firmware on the CPL.

Managed by



## 6. Implementation approach

---

### Approved implementation approach

The Change Sub-Committee (CSC) has agreed an implementation date of:

- **29 June 2023** (June 2023 SEC Release) if a decision to approve is received on or before 15 June 2023; or
- **2 November 2023** (November 2023 SEC Release) if a decision to approve is received after 15 June 2023 but on or before 19 October 2023.

This is a document only change and therefore the next SEC Release this could be implemented in is the June 2023 SEC Release. There should be minimal or no impact on SEC Parties and therefore this modification can be implemented in the June 2023 SEC Release.

## 7. Assessment of the proposal

---

### Observations on the issue

#### Views of the Change Sub-Committee

A Manufacturer representative commented that it can take up to two weeks to get a Supplier to send its 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

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. When SECAS returned to the SSC to present the Proposed Solution, it was met with approval.

### Solution development

#### Support from a Large Supplier party

When presented at the SEC Working Group, a Large Supplier representative acknowledged the issue and approved of the Proposed Solution. A Device Manufacturer representative also commented that they experience liaising with many Suppliers as part of BAU CPL submissions, and was also supportive of the Proposed Solution. During the Working Group discussion, a member asked whether

the modification had any DCC System impacts. SECAS confirmed that this modification will not result in any DCC System impacts as MP222 is a governance change. The Proposer added that they believed that the Proposed Solution will not negatively impact Parties, as the process will become more direct and efficient.

### **Security enhancements**

SECAS presented the straw man solution to the SSC to understand if there was any security compromise. The SSC noted the issue and business requirements that the Proposed Solution must adhere to. It suggested that CPL submissions should be limited to Supplier Parties and Device Manufacturers, and the legal text was amended accordingly. This will bolster security as this will limit who can submit new Devices to the CPL. Furthermore, the SSC added that provided MP168 is implemented, the two modifications will complement each other and will provide greater security to smart metering. The SSC approved of the Proposed Solution. The Proposer and SECAS have since restricted the new change further to Device Manufacturers that are SEC Parties.

## **8. Case for change**

---

### **Business case**

This modification will result in a more efficient CPL submission process. Enabling Manufacturers to be able to submit firmware and hardware revisions to existing Devices, without Supplier Party endorsement, will allow for additional functionality and fixes to be made available in a more time efficient manner. This will reduce the time for fixes and improvements to be available for deployment with operational, security and consumer benefits and allow Suppliers to focus on testing activities.

### **Views against the General SEC Objectives**

#### **Proposer's views**

The Proposer believes that this modification better facilitates SEC Objective (a)<sup>1</sup>, as the efficiency improvements to the CPL submission process will provide improvements to the provision, operation and interoperability of smart metering systems.

The Proposer also believes that this modification will better facilitate SEC Objective (c)<sup>2</sup>, as the Proposed Solution will enable fixes and enhancements to consumers' smart meters that will enable them to better manage their energy usage.

Furthermore, the Proposer believes that this modification will better facilitate SEC Objective (d)<sup>3</sup>, as the proposed CPL submission efficiencies will mean that Manufacturers that are not affiliated with a Supplier will be able to provide firmware and hardware revisions to their Devices.

---

<sup>1</sup> Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

<sup>2</sup> Facilitate energy consumers' management of their use of electricity and gas through the provision of appropriate information via smart metering systems.

<sup>3</sup> Facilitate effective competition between persons engaged in, or in commercial activities connected with, the supply of energy.

### **Industry views**

The Refinement Consultation respondents agreed with the Proposer, stating that the modification will better facilitate SEC Objectives (a), (c) and (d).

### **Views against the consumer areas**

#### **Improved safety and reliability**

This modification will offer improvements to the reliability of Devices, as firmware updates that include fixes to issues will be able to be implemented in a more efficient manner than the current process allows.

#### **Lower bills than would otherwise be the case**

This modification will have a neutral impact on the cost of consumers' energy bills.

#### **Reduced environmental damage**

This modification will have a positive impact on the reduction of environmental damage, as the Proposed Solution will allow Manufacturers who are not currently endorsed by a Supplier to update their Devices. This will mitigate against the potential removal of these Devices.

#### **Improved quality of service**

This modification will facilitate and improve quality of service as firmware updates will be made available more quickly, which Suppliers will then be able to roll out to their customers.

#### **Benefits for society as a whole**

This modification will have a positive impact on society as the efficiencies to the CPL submission process will enable updates to Devices including fixes and additional functionality to be made available in a timelier manner.

## **Appendix 1: Progression timetable**

---

SECAS will present the modification to the CSC on 18 April 2023 with the recommendation that MP222 enters the Report Phase. SECAS will then issue the Modification Report Consultation before proceeding to Change Board vote. This modification will be progressed as a Self-Governance modification.

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
Business requirements developed with the Proposer	Dec 2022
Proposed Solution developed with the Proposer	Dec 2022
Legal text developed with the Proposer and SEC Lawyer	Jan 2023
Modification discussed with Working Group	1 Feb 2023
Modification discussed with the SSC	22 Feb 2023
Refinement Consultation	15 Mar 2023 – 5 Apr 2023
<i>Modification Report approved by CSC</i>	<i>18 Apr 2023</i>
<i>Modification Report Consultation</i>	<i>19 Apr – 12 May 2023</i>
<i>Modification approved by Change Board</i>	<i>24 May 2023</i>

## 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
BAU	business as usual
COSEM	Companion Specification for Energy Metering
CPA	Certified Product Assurance
CPL	Central Products List
CRL	Certificate Revocation List
CSC	Change Sub-Committee
DCC	Data Communications Company
DLMS	Device Language Message Specification
EUA	Energy and Utilities Alliance
IKI	Infrastructure Key Infrastructure
NCSC	National Cyber Security Centre
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

Glossary	
Acronym	Full term
TABASC	Technical Architecture and Business Architecture Sub-Committee

# MP222 ‘CPL submission efficiency improvements’

## Annex A

### Business requirements – version 0.1

#### About this document

---

This document contains the business requirements that support the solution(s) for this Modification Proposal. It sets out the requirements along with any assumptions and considerations. The Data Communications Company (DCC) will use this information to provide an assessment of the requirements that help shape the complete solution.

## 1. Business requirements

---

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	Requirement
1	Firmware and / or hardware revisions for Devices currently listed on the Central Products List (CPL) are to be submitted in a more efficient manner.
2	A Manufacturer can submit a Hash Image for firmware and / or hardware revisions for Devices currently listed on the CPL following CPA approval without the additional support of a Supplier Party.
3	CPL submission efficiencies will not compromise security and will not force the Supplier Party to deploy the firmware and / or hardware revision.



## 2. Considerations and assumptions

---

This section contains the considerations and assumptions for each business requirement.

### 2.1 General

This solution will be applied to Smart Metering Equipment Technical Specifications (SMETS)2 Devices only.

### 2.2 Requirement 1: Firmware and / or hardware revisions for Devices currently listed on the Central Products List (CPL) are to be submitted in a more efficient manner.

The Proposer has suggested that in order to make CPL submissions that relate to firmware and / or hardware revisions of pre-existing CPL-listed Devices more efficient, the requirement to obtain a Supplier Party endorsement should be removed. The rationale behind this is that the modification will allow updated products to enter the GB Smart Metering market, providing important fixes (operational and potentially security) and new technologies in a more efficient manner. This will allow for a more open marketplace, with new Manufacturers and technologies no longer facing hurdles to provide their products. This is likely to increase as new initiatives and industry challenges arise. An example of this is the design and build of new Devices in order to facilitate the introduction of hydrogen.

### 2.3 Requirement 2: A Manufacturer can submit a Hash Image for firmware and / or hardware revisions for Devices currently listed on the CPL following CPA approval without the additional support of a Supplier Party.

Currently, if present, a Supplier must present the Hash Image to Smart Energy Code Administrator and Secretariat (SECAS) for CPL submission; it cannot be the manufacturer. This is despite the Manufacturer creating the Hash Image. The Proposer has stated that it would be more efficient to allow the Manufacturer to present the Hash Image that it created as part of the CPL submission.

### 2.4 Requirement 3: CPL submission efficiencies will not compromise security and will not force the Supplier Party to deploy the firmware and / or hardware revision.

It is the intention of this modification to make the process of submitting new entries to the CPL that are providing either hardware or firmware updates to existing Devices more efficient, however the Proposed Solution should not reduce the current security requirements in place. SECAS and the Proposer will discuss the Proposed Solution with the Security Sub-Committee (SSC). The firmware and / or hardware revisions will also not be mandatory.

### 3. Solution development

---

This section contains a must-have, should-have, could-have, won't-have (MoSCoW) analysis for the different requirement components to be considered as part of the solution.

MoSCoW Analysis		
Requirement Ref.	Description	MoSCoW
1	Any proposed CPL submission solutions put forward under MP222 must be more efficient than what is currently in place.	M
2	Allowing the Manufacturer to submit the Hash Image that it has created will be an efficiency improvement.	S
3	The Proposed Solution must not compromise the smart metering security infrastructure.	M

#### Key

- M = Must have
- S = Should have
- C = Could have
- W = Won't have

## 4. 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
DCC	Data Communications Company
SECAS	Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specifications
SSC	Security Sub-Committee

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.

# MP222 ‘CPL submission efficiency improvements’

## Annex B

### Legal text – version 1.0

#### About this document

---

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

This document contains the changes required to deliver the Proposed Solution.

## **Appendix Z ‘CPL Requirements Document’**

---

These changes have been redlined against Appendix Z version 6.0.

**Amend Appendix Z as follows:**

## APPENDIX Z

### CPL Requirements Document

## 1. **Overview**

- 1.1 This Appendix supplements Section F2 (Central Products List).

## 2. **Central Products List Contents**

- 2.1 The Panel shall ensure that the Central Products List identifies each Device Model by Physical Device Type, and lists the following matters in respect of each Device Model:
- (a) Manufacturer and model;
  - (b) hardware version;
  - (c) firmware version;
  - (d) for SMETS2+ Device Models, the version of the SMETS or CHTS (as applicable) and (in each case) the GBCS version for which the Device Model has one or more Assurance Certificates;
  - (e) for SMETS1 Device Models, Version 1.2 of SMETS;
  - (f) for SMETS2+ Device Models, the identification numbers for each of the Device Model's Assurance Certificates (including the version of the relevant standard against which each Assurance Certificate was issued);
  - (g) where the Device Model is required to have an associated CPA Certificate, the expiry or renewal date of the Device Model's CPA Certificate and the associated version of the Security Characteristics (as defined in the relevant Technical Specification); and
  - (h) where there is an associated Manufacturer Image:
    - (i) the relevant identity of the person who created the Manufacturer Image;
    - (ii) a descriptor of the Manufacturer Image; and
    - (iii) the Hash of the Manufacturer Image (to be provided pursuant to Clause 4).

## 3. **Addition of Device Models to the List**

- 3.1 For SMETS2+ Device Models, the Panel shall only add Device Models to the Central Products List once the Panel has received all the Assurance Certificates required (under the Technical Specifications) to be obtained in respect of Device Models of the relevant Physical Device Type (which Assurance Certificates may be provided to the Panel by a Party or any other person).
- 3.2 For SMETS1 Device Models, the Panel shall only add a Device Model to the Central Products List once the Panel has received a notification from the DCC or, subject to Clause 3.5, from a Supplier Party. [Clauses 3.3 to 3.13 \(inclusive\) set out the process for adding SMETS1 Device Models to the Central Products List.](#)
- 3.3 The DCC shall only send a notification to the Panel in respect of a SMETS1 Device Model (as referred to in Clause 3.2) once the Device Model has been included as part of at least one entry on the SMETS1 Eligible Products Combinations list.
- 3.4 A Supplier Party may only send a notification to the Panel in respect of a SMETS1 Device Model (as referred to in Clause 3.2) if:
- (a) that SMETS1 Device Model has not been included as part of at least one entry on the SMETS1 Eligible Product Combinations list; and



- (b) that Supplier Party reasonably believes that the addition of the SMETS1 Device Model to the Central Products List is required in order to facilitate the urgent resolution of a material security vulnerability relating to Commissioned Devices for which it is the Responsible Supplier.
- 3.5 As soon as reasonably practicable after sending a notification to the Panel in accordance with Clause 3.2, the relevant Supplier Party shall notify the DCC via the Notification Interface that it has sent such a notification to the Panel and, in doing so, shall inform the DCC of the Device Model notified to the Panel.
- 3.6 The Panel shall only accept and process a notification from a Supplier Party under Clause 3.2 if the notification has been made in accordance with the requirements of the Supplier Party CPL Notification Procedures and where the Panel has successfully confirmed that the notification was from a Supplier Party and has not been modified since its creation.
- 3.7 For the purposes of Clause 3.6, the Supplier Party CPL Notification Procedures are procedures that provide for a Device Model to be notified to the Panel by a Supplier Party in a manner that allows the Panel to confirm that:
- (a) any such notification has originated from a Supplier Party; and
  - (b) any such notification from a Supplier Party has not been modified since its creation.
- 3.8 The Panel shall develop the Supplier Party CPL Notification Procedures and any subsequent modification to them in consultation with the Security Sub-Committee and publish the Supplier Party CPL Notification Procedures on the Website.
- 3.9 Where the DCC has received a notification via the Notification Interface from a Supplier Party pursuant to Clause 3.5, the DCC shall, as soon as reasonably practical after uploading into the DCC Systems a revised version of the Central Products List that additionally includes the Device Model notified to the Panel by the Supplier Party, inform that Supplier Party via the Notification Interface that the upload has taken place.
- 3.10 For the purposes of Clauses 3.5 and 3.9, the Notification Interface is an appropriately secure interface, the identity of which the DCC shall communicate to Supplier Parties, for the purposes of making the notifications between Supplier Parties and the DCC referred to in those Clauses.
- 3.11 After the addition of a Non-EPCL Device Model to the Central Products List, the Supplier Party that notified the Non-EPCL Device Model to the Panel shall take all reasonable steps to ensure that each Device Model Combination:
- (a) of which any Commissioned Device of that Non-EPCL Device Model forms part; and
  - (b) for which Commissioned Device it is the Responsible Supplier,
- is added to the SMETS1 Eligible Product Combinations List as soon as reasonably practicable.
- 3.12 After the Commissioning of a Device that is of a Non-EPCL Device Model, the Responsible Supplier for that Device shall take all reasonable steps to ensure that that the Device Model Combination of which that Device forms part is added to the SMETS1 Eligible Product Combinations List as soon as reasonably practicable.
- 3.13 Where a PPMID of a particular type is capable of forming part of either a SMETS1 Smart Metering System or a SMETS2+ Smart Metering System, any Device Model added to the Central Products List shall:
- (a) insofar as it relates to PPMIDs of that type forming part of SMETS2+ Smart Metering Systems, be the Manufacturer of the PPMID, its model, its hardware version and its firmware version; and
  - (b) insofar as it relates to PPMIDs of that type forming part of SMETS1 Smart Metering Systems, be the Manufacturer of the PPMID, its model, its hardware version and a value representing its firmware version that is different to the firmware version of the PPMID of that type that forms part of a SMETS2+ Smart Metering System.

#### 4. Association of Hashes with Device Models on the CPL

- 4.1 Where the DCC ~~or~~, a Supplier Party or a Manufacturer which is a 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.

#### 5. Adding Device Models to CPA Certificates

- 5.1 An existing CPA Certificate for a Device Model may allow one or more additional Device Models to be added under that existing CPA Certificate, provided that any additional Device Model differs from the Device Model for which the CPA Certificate was originally issued only by virtue of having different versions of hardware and/or firmware that do not have a significant impact on the security functions of the Device Model (as set out in the CPA Assurance Maintenance Plan). Where this is the case, the following persons may notify the Panel of one or more additional Device Models to be added to the CPA Certificate:

- (a) the DCC for Communications Hubs; or
- (b) a Supplier Party or a Manufacturer which is a Party for Device Models of all other Physical Device Types.

~~may notify the Panel of one or more additional Device Models to be added to the CPA Certificate.~~

- 5.2 Where the DCC ~~or~~, a Supplier Party or a Manufacturer which is a Party notifies the Panel of an additional Device Model pursuant to Clause 5.1, the DCC ~~or the~~, Supplier Party or Manufacturer shall:
- (a) only do so in accordance with the terms of the relevant CPA Assurance Maintenance Plan; and
  - (b) retain evidence that it has acted in accordance with the terms of the relevant CPA Assurance Maintenance Plan, such evidence to be provided to the Panel or the Authority on request.
- 5.3 The Panel shall not be required to check whether the DCC ~~or a~~, Supplier Party or Manufacturer (as applicable) is entitled to add a Device Model under the terms of the CPA Certificate and the CPA Assurance Maintenance Plan (as described in Clause 5.1).
- 5.4 [NOT IN USE]

## 6. Removal of Device Models from the List

- 6.1 Where an Assurance Certificate for a Device Model which was issued by the ZigBee Alliance or the DLMS User Association is withdrawn or cancelled by the ZigBee Alliance or the DLMS User Association (as applicable), then the Panel shall remove that Device Model from the Central Products List.
- 6.2 Where a CPA Certificate for a Device Model expires or is not renewed or is withdrawn or cancelled by NCSC, then the Security Sub-Committee shall determine whether the Device Model is to be removed from the Central Products List, and the Panel shall remove the Device Model (or not) as determined by the Security Sub-Committee. In reaching such a determination, the Security Sub-Committee:
- (a) shall consider the security implications of such circumstances, and weigh them against the consequences for Energy Consumers of Devices of the relevant Device Model being Suspended as a result of removing the Device Model from the Central Products List;
  - (b) shall take into account any relevant information provided to it by NCSC concerning the risks associated with the cancellation, withdrawal or expiry without renewal of the CPA Certificate;
  - (c) may determine, whether or not the Device Model is to be removed from the Central Product List, that a CPA Certificate Remedial Plan is to be imposed (for SMETS2+ Communications Hubs) on the DCC or (for all other Device Models) on the Import Suppliers (for Devices of that Device Model forming part of a Smart Metering System for which they are the Import Supplier) and/or the Gas Suppliers (for Devices of that Device Model forming part of a Smart Metering System for which they are the Gas Supplier); and
  - (d) shall reach a determination as soon as reasonably practicable taking into account the seriousness of the potential security consequences.
- 6.3 Where the Security Sub-Committee determines under Clause 6.2 that a CPA Certificate Remedial Plan is to be imposed on one or more Parties, then the Security Sub-Committee shall notify those Parties and each of those Parties shall:
- (a) (within such period as the Security Sub-Committee may require) propose a plan to the Security Sub-Committee setting out how the Party intends to remedy the security issue or issues that have resulted in or arise from the cancellation, withdrawal or expiry without renewal of the CPA Certificate, and within what time period;
  - (b) (within such period as the Security Sub-Committee may require) take into account any and all comments on the proposed plan raised by the Security Sub-Committee, and obtain the Security Sub-Committee's approval of the plan (the approved plan for each such Party, as modified from time to time with the approval of the Security Sub-Committee, being that Party's "**CPA Certificate Remedial Plan**");
  - (c) comply in all material respects with the CPA Certificate Remedial Plan; and
  - (d) (where requested by the Security Sub-Committee) report to the Security Sub-Committee on progress in respect of the CPA Certificate Remedial Plan.
- 6.4 Where the Security Sub-Committee initially determines under Clause 6.2 that a CPA Certificate Remedial Plan is to be imposed as an alternative to removing a Device Model from the Central Products List, then the Security Sub-Committee may at any time determine that the Device Model in question is to be removed from the Central Products List, in which case the Panel shall remove the Device Model from the Central Products List.
- 6.5 For the purposes of Section M8.1(g) (Events of Default), the obligations of a Party under Clause 6.3 are material obligations. Accordingly, failure by a Party to gain approval for, or failure by a Party to comply in all material respects with, a CPA Certificate Remedial Plan shall be an Event of Default if not remedied within 20 Working Days after notice from the Security Sub-Committee requiring remedy.

- 6.6 The DCC, ~~and~~ each Supplier Party and each Manufacturer which is a Party shall provide such relevant information as the Security Sub-Committee may reasonably request to assist it in reaching a determination under Clause 6.2 or 6.4.
- 6.7 The DCC, ~~and~~ each Supplier Party and each Manufacturer which is a Party shall notify the Panel of any withdrawal, expiry or cancellation of an Assurance Certificate of which the DCC ~~or~~, Supplier Party or Manufacturer becomes aware. Where removal occurs as a result of the withdrawal, expiry or cancellation of an Assurance Certificate, the Panel shall only remove a Device Model from the Central Products List after the Panel has confirmed with the relevant Assurance Certification Body that the Assurance Certificate for that Device Model has expired or has been withdrawn or cancelled (and no new Assurance Certificate has been provided to the Panel under Clause 3).
- 6.8 The Panel may also remove a SMETS1 Device Model from the Central Products List where either:
- (a) the Security Sub Committee advises that the Device Model should be removed from the Central Products List; or
  - (b) it is determined by the Authority or by the Panel under Section F3 (Panel Dispute Resolution Role) that Devices of the relevant Device Model are not compliant with SMETS1 (either on their own or in combination with Devices of other Device Models listed on the Central Products List).
- 6.9 The Panel may reinstate to the Central Products List a SMETS1 Device Model that it has removed pursuant to Clause 6.8; provided that the Panel may only reinstate a Device Model that has been removed pursuant to Clause 6.2A(b) where it determines that the issue that gave rise to the removal of the Device Model has been rectified.
- 6.10 For the purposes of this Code, a Communications Hub Function or a Gas Proxy Function shall be considered to be on (or not on) the Central Products List if the Communications Hub of which it forms part is on (or not on) the Central Products List.
- 6.11 The Panel may provide for the removal of a Device Model from the Central Products List by marking that Device Model as 'removed'. All references in this Code to the removal of a Device Model from the Central Products List (and similar expressions) shall be interpreted accordingly.

## **7. Digital Signatures on CPL**

- 7.1 When providing an updated Central Products List (or extract of it) to the DCC, the Panel shall provide a copy of the Central Products List (or of that extract) that is Digitally Signed so as to reasonably enable the DCC to check that the updates to the Central Product List originate from the Panel.
- 7.2 The DCC shall, before using and relying upon the Central Products List received by the DCC from the Panel, first confirm that the Digital Signature referred to in Clause 7.1 is that of the Panel (validated as necessary by reference to a trusted party).
- 7.3 Following receipt by the DCC of an updated Central Products List from the Panel, the DCC shall take all reasonable steps to establish whether the update included the removal of one or more Device Models from the Central Products List. Where the DCC establishes that an update did include the removal of one or more Device Models from the Central Products List, then:
- (a) the DCC shall take all reasonable steps to confirm that it was the intention of the Panel to remove such Device Models from the Central Products List; and
  - (b) where the DCC reasonably believes that it was not the intention of the Panel to remove such Device Models from the Central Products List, the DCC shall notify the Panel that this is the case and (notwithstanding Section F2.9) shall ignore the updated Central Products List.

## Section F ‘Smart Metering System Requirements’

---

These changes have been redlined against Section F version 15.0.

### Amend Section F as follows:

#### Communications with Communications Hubs by DCC over the SM WAN

- F4.8 Except where expressly permitted or obliged by this Code, the DCC shall ensure that the only Devices with which it communicates over the SM WAN are those listed in the Smart Metering Inventory. Where a Communications Hub Function or Gas Proxy Function has an SMI Status of ‘suspended’, the DCC shall only initiate a communication with that Device (where it is the target device) if following the successful execution of such communication the DCC can reasonably expect that the associated Communication Hub’s Device Model will become one that is listed on the Central Product List.
- F4.9 Except in the circumstances described in Section F4.9B, where the DCC receives a Power Outage Event (AD1) Alert from a Communications Hub Function indicating that no power supply has been available to that Communications Hub Function for a period of at least three minutes, the DCC shall send a copy of the Alert to the Import Supplier (if any) and Electricity Distributor (if any) for that Communications Hub Function.
- F4.9A The DCC shall maintain a list of Devices which are known to cause a Communications Hub Function to send a Power Outage Event (AD1) Alert for a short period (of greater than three minutes) following commencement of a firmware update.
- F4.9B In relation to Devices on such list, in the case of a ~~no~~ Power Outage Event (AD1) Alert being received by the DCC within the period of 30 minutes following commencement of a firmware update, the DCC shall not send a copy of the Alert to the Import Supplier or the Electricity Distributor (but the DCC shall record and store details of the Alert, including its suppression in accordance with this Section F4.9B).

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.

# MP222 ‘CPL submission efficiency improvements’

## Annex C

## Refinement Consultation responses

### About this document

---

This document contains the full collated responses received to the MP222 Refinement Consultation.

## Question 1: Do you agree that the solution put forward will effectively resolve the identified issue?

Question 1			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	Yes	No comment.
EDF Energy	Large Supplier	Yes	We agree that the solution put forward will speed up addition of new firmware and hardware changes to the CPL.



## Question 2: Do you agree that the legal text will deliver MP222?

Question 2			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	Yes	No comment.
EDF Energy	Large Supplier	Yes	The legal text is in line with the proposal. It adds the Manufacturer as a party capable of partaking in the process without removing the option for the Supplier to do so. However, it also removes the need for a Manufacturer to obtain the support of a Supplier to do so.

### Question 3: Do you agree with the proposed implementation approach?

Question 3			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	Yes	No comment.
EDF Energy	Large Supplier	Yes	The proposed implementation approach is only a minor procedural change, so very little impact to us overall.

## Question 4: Will there be any impact on your organisation to implement MP222?

Question 4			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	No	As a DNO we believe this modification will not directly impact us.
EDF Energy	Large Supplier	Yes	It will marginally reduce effort by not requiring a letter of endorsement to be sent for the updates by EDF.

## Question 5: Will your organisation incur any costs in implementing MP222?

Question 5			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	No costs	As a DNO we believe we will not incur any direct costs following this modification.
EDF Energy	Large Supplier	No costs	No significant cost will be incurred or saved by EDF due to the change as our overall testing process for new firmware will not be heavily impacted. The main impact we see this having is that the manufacturer will not have to wait for us to complete our own internal testing before being able to list the new firmware on the CPL.

## Question 6: How long from the point of approval would your organisation need to implement MP222?

Question 6			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	N/A	No comment.
EDF Energy	Large Supplier	None	Due to there being only a small impact to our process, we do not require any time period to implement this change.

## Question 7: Do you believe that MP222 would better facilitate the General SEC Objectives?

Question 7			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	Yes	We believe this Modification will better facilitate General SEC Objectives (a), (c) and (d).
EDF Energy	Large Supplier	Yes	We agree that this change will better facilitate SEC Objectives (a), (c) and (d).

## Question 8: Do you believe there will be any impacts on or benefits to consumers if MP222 is implemented?

Question 8			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	Yes	We believe consumers will be impacted by this modification for the reasons stated in the modification report.
EDF Energy	Large Supplier	Yes	It can speed up the time to fix operational issues seen on assets but adding a new firmware to the CPL does not automatically mean EDF deploys it to the meter estate. We do so after assessing the impacts of any changes, expected bug fixes and internal testing and field piloting, before mass deployment. The time to CPL is only one factor in the overall time to deploy a change.

## Question 9: Noting the costs and benefits of this modification, do you believe MP222 should be approved?

Question 9			
Respondent	Category	Response	Rationale
National Grid Electricity Distribution	Network Party	Yes	No comment.
EDF Energy	Large Supplier	Yes	The proposal is reasonable and offers a benefit of time to deployment at no significant cost to EDF.



## Question 10: Please provide any further comments you may have.

Question 10		
Respondent	Category	Comments
National Grid Electricity Distribution	Network Party	No further comments.
EDF Energy	Large Supplier	No further comments.