MP231

‘Firmware upgrade pathways’

Modification Report

Version 1.0

20 December 2023

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

This document also has two annexes:

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

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 SSC has noted a concern raised by the Technical Architecture and Business Architecture Sub-Committee (TABASC) and reflected in reports from the Data Communications Company (DCC) that certain Device models need to have a firmware upgrade applied in a specific order. Failure to follow the specific order can result in unintended consequences. Investigation of the issue indicates that it is not an uncommon requirement for firmware updates to be implemented in a specific order.

The Firmware Information Repository (FIR) is available for manufacturers to update and contains some information relating to upgrades for Electricity Smart Metering Equipment (ESMEs) and Gas Smart Metering Equipment (GSMEs). Suppliers can access this FIR. However, the information required to ensure each Device has its firmware upgrade applied in the correct order is not currently included, nor is there a requirement in the SEC for that information to be provided.

The Proposed Solution is to include a requirement in the SEC to include the Central Products List (CPL) Entry Identifier (ID) of the base firmware version within a new field on every CPL submission. This would then be transferred into a new field within the FIR which Suppliers can access through the SEC website. The base CPL Entry ID for existing Devices on the CPL will be requested on a best endeavours basis.

The costs for this modification are limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort to update the CPL Tool to accommodate the new fields, as well as the FIR and supporting documentation.

This modification will target an Ad-Hoc SEC Release, two months after decision, and will be progressed under Self-Governance.

2. Issue

What are the current arrangements?

What is required in a Device upgrade?

The requirements relating to Device upgrades are included in the Great Britain Companion Specification (GBCS), specifically Section 11, which contains information relating to downloading firmware images to Devices. Section 11.1 states:

"…the contents of Manufacturer Images sent to Devices are manufacturer defined. Thus, a particular Manufacturer Image may consist of whatever the manufacturer requires to achieve the necessary update which could be a full image or just a patch to application code or any other manufacturer specified content.

Therefore, the steps taken by a Device when it activates the contents of a particular Manufacturer Image are manufacturer specific and specified in the release note for that Manufacturer Image."

This means a Device Manufacturer can specify any special requirements to be applied to a firmware upgrade on their Device, and what controls or dependencies are included. Some Devices may require a sequence of firmware versions to be applied in a particular order, whereas other Devices may be able to move from an earlier firmware version to any later firmware version.

Who upgrades Devices?

Suppliers are responsible for the distribution and activation of firmware on Devices and as such should understand the implications of carrying out the upgrade. However, there are several reasons why an upgrade process may not be successful. For instance, the technical dependencies of the upgrade may not be understood by those initiating the upgrade due to not having in-depth technical understanding. A technical dependency might be that a particular image needs to be installed and operating prior to the upgrade of a subsequent image.

Where is information relating to firmware upgrades held?

There is currently no location where this information relating to certain dependencies for each Device is publicised as a reliable source. The information may be able to be found within the Release Notes for that particular Device and firmware version. However, that information may either not be available to a Supplier as they could contain commercially sensitive information, or they could be difficult to interpret as Release Notes can be very complex or the Supplier may have inherited the Device as the consumer changed Supplier.

The Release Notes by themselves without specialist Device Manufacturer or engineer knowledge may not provide the clarity required to inform a Supplier.

What is the issue?

The SSC has highlighted that Devices could have a firmware upgrade applied that causes unintended consequences. Deeper investigation found that it is not uncommon for firmware updates to be required to be implemented in a specific order. Furthermore, there are examples where this required sequence of updates was not able to be verified during the update process. Whilst the Release Notes for one of the Devices specified a specific upgrade sequence, others did not.

When a firmware image is created by a Device Manufacturer, the Manufacturer will understand many of the variables required for the successful activation of that image on one of their Devices. Whilst the Device Manufacturer may have the capability and expertise to understand how the firmware image may need to be successfully activated, the same cannot always be said of those who need to apply the image.

A previous modification, SECMP0009 ‘Centralised Firmware Library’, delivered the Firmware Information Repository (FIR) which can be accessed only by SEC Parties, via the SEC website. This contains additional information for ESMEs and GSMEs, including contact details for the Manufacturer and Release information. However, that information is provided voluntarily at the discretion of the party making the CPL submission and does not necessarily specify an upgrade path.

What is the scope of the modification?

Whilst other issues, such as interoperability of Devices, can also cause Devices to have unintended consequences, the scope of this modification does not include providing information on the interoperability of Devices.

What is the impact this is having?

As certain Devices require their firmware to be upgraded in a specific order, failing to do this can result in a Device having unintended consequences, including losing functionality. In these instances, a Supplier would then be required to carry out a site visit to exchange the Device. This is an

unnecessary cost on the Supplier and an inconvenience for the consumer. Device Manufacturers could also have their reputation negatively impacted if their Devices suffer from this situation.

There are financial and environmental costs from scrapping Devices that otherwise would work had a firmware upgrade been applied correctly.

Impact on consumers

If a Device loses functionality, then the consumer is impacted by the period without a fully working Device, and the inconvenience of having to facilitate an engineer site visit. The added costs could also be fed back to all consumers through Supplier charges.

3. Solution

The solution will place an obligation on Device Manufacturers to provide additional information with their CPL submissions.

The additional information will be:

1. CPL Entry ID(s) of the previous firmware version that can be upgraded to the new version on their CPL submission. This could be one or many versions depending on their firmware. If there is no previous version, then 'N/A' should be used to populate the field.
2. ZigBee chipset vendor of the chipset that is included on that version of the Device Model
3. ZigBee stack version that is included on that version of the Device Model
4. ZigBee band information with regards Device behaviour when joining the Home Area Network (HAN). This will be a drop-down field within the CPL submission. The table below shows these options.

Joining options for ZigBee band	
Join Option	**Description**
2.4 GHz Only	Capable of operating on 2.4 GHz band only
Sub-GHz Only	Capable of operating on Sub-GHz band only
Multi MAC Selection – Auto	Capable of operating on either band & Device selects the band automatically during join
Multi MAC Selection – Manual	Capable of operating on either band & Device allows manual selection of band to join
Multi MAC Selection – Either	Capable of operating on either band & Device allows either automatic or manual join
Dual Band	Capable of operating on both bands simultaneously. Only Communications Hubs can perform this in SMETS2

The information related to firmware upgrade pathway will then be included in the FIR so that it is accessible for Suppliers, through the SEC website. The ZigBee information will be included in a database for the SSC only.

This information will be requested on a best endeavours basis for existing entries on the CPL. If it is not possible to source the information for some Device Models then these fields will be left empty.

The redlined changes to deliver the Proposed Solution can be found in Annex A.

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
✓	Meter Asset Providers		

Suppliers will be positively impacted by being able to simply access the firmware upgrade paths for any Device on the CPL. They will also be impacted if they are the Party authorising a CPL submission with this information.

Device Manufacturers, including Smart Metering Equipment Technical Specification (SMETS)1 Communications Hubs Manufacturers will be impacted by having to provide this extra information for upgrade pathways within their CPL submissions. SECAS will also request them to provide this information for existing CPL entries. As the DCC only endorses the CPL submissions from Communications Hub Device Manufacturers, and does not put this information together themselves, they are not impacted by this change.

Meter Asset Providers (MAPs) will be impacted in a positive way as it should mean that the Devices they own have a reduced risk of unintended consequences by applying firmware upgrades.

DCC System

There will be no impacts on DCC Systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section F ‘Smart Metering System Requirements’

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

Technical specification versions

This modification does not impact the Technical Specifications.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
✓	Communications Hubs		Gas Proxy Functions
	In-Home Displays	✓	Prepayment Meter Interface Devices
✓	Standalone Auxiliary Proportional Controllers	✓	Home Area Network Connected Auxiliary Load Control Switches
	Consumer Access Devices		Alternative Home Area Network Devices

This modification will not impact the behaviour of any Devices. However, the requirement to provide the information relating to upgrade path within the CPL submission will be mandated for these Devices.

During the Working Group, the consensus was that only SMETS1 Communications Hubs should be included within the scope of this modification as Suppliers are responsible for the upgrade to these, but not to SMETS2 Communications Hubs. However, the SSC believes that all Communications Hubs should be within the scope as the additional information would be used to assess the impact of any security defects found within the ZigBee stack on a Device.

Consumers

Consumers will be indirectly positively impacted by the change as it should reduce the risk of a consumer being left with a Device that is not working as intended.

Other industry Codes

There will be no impact on other industry Codes from this modification.

Greenhouse gas emissions

There will be no direct impact on greenhouse gas emissions from this modification. However, this could lead to a reduction in Devices needing to be exchanged and being scrapped so therefore a positive impact.

5. Costs

DCC costs

There are not expected to be any costs to the DCC to implement this modification:

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is 17 days of effort, amounting to approximately £20,696. 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.
- Updating the CPL Tool.

- Updating the FIR with new fields and entries for Device types not currently included.
- Updating the CPL Guidance Notes.
- Obtaining and populating pathway information for existing Device submissions on a best endeavours basis.

SEC Party costs

Discussion in the Working Group indicated there could be additional resource or process changes required for some Device Manufacturers to provide the extra data within the CPL submission.

Reducing the number of instances where a firmware upgrade is applied incorrectly would reduce Supplier costs from having to resolve any issue that arose from the error.

Further views and detail will be sought via the Refinement Consultation.

6. Implementation approach

Agreed implementation approach

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

- **Two months after decision** (Ad hoc SEC Release) if a decision to approve is received.

The changes needed to implement this modification are limited to SECAS time and effort. This is a non DCC System impacting change and should only include relatively minor process changes for SEC Parties. It is noted there are impacts to Device Manufacturers to supply this information, but SECAS does not believe this is a material change.

The CPL Tool changes will require approximately two months to develop, test and implement. However, due to the urgency suggested in the SSC Commercial Product Assurance Issue Resolution Subgroup (SCIRS), SECAS has agreed to commence work in advance of the decision if it is apparent from the Refinement Consultation, Working Group and TABASC engagement that the solution is very clear. It is not possible to target the June SEC Release, therefore an ad-hoc SEC Release will be targeted.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the 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 provide the following input to this modification:

Sub-Committee input	
Sub-Committee	**Input sought**
OPSG	Confirm issue and solution is appropriate for Suppliers
SMKI PMA	No input required
SSC	As Proposer seek input and feedback throughout
TABASC	Seek input on viable solution options

Observations on the issue

At the Change Sub-Committee (CSC) a member noted that under the discussion at TABASC, a Guidance Note had been produced to also help Parties immediately. SECAS noted that this had been produced and would be shared with SEC Parties once it had been approved. The Guidance Notes are currently in development pending feedback from the Technical Specification Issue Resolution Sub-group (TSIRS). SECAS highlighted this modification does not prevent human errors from occurring however it is likely to help reduce these errors. It was noted the cost of this modification is primarily down to SECAS administrative cost for building the required tool to help support the data which will be implemented in an ad-hoc standalone release. The CSC agreed the modification should be progressed to the Report Phase.

This issue was discussed at the SCIRS. Members noted that this was an urgent issue to be addressed. They questioned whether an interim solution could be delivered in the meantime. SECAS has confirmed that there is a free text field within the CPL submission that could be used now and would notify Parties of how this could be completed for this purpose. This action is currently outstanding.

The TABASC members supported making the information regarding supported firmware paths more accessible. They recognised that certain Users, such a Small Suppliers, while resourced appropriately for their size, may not have the resource or specialist knowledge to understand Release Notes and engage with Manufacturers.

Release Notes

A Working Group member, who was a Device manufacturer, stated that they had never encountered this issue and treat their Release Notes as the source of truth. They were not happy with having to duplicate this information and noted the queries they had previously received from Suppliers would all have been resolved by reading the Release Notes.

They also believed that Parties performing an Over-the-air (OTA) upgrade without reviewing the Release Notes were not taking a necessary procedural step as there may be other information that they need to be aware of, such as known defects.

Another Working Group member noted that Manufacturers had differing levels of complexity for upgrade paths. They advised that they receive contact from their customers around these pathways, particularly when Devices had churned. This view was supported by other Working Group members.

Solution development

Firmware version or CPL Entry ID as reference

SECAS suggested that a new column could be introduced to the FIR which would contain the previous CPL entry ID for the supported firmware upgrade. TABASC members stressed that they were more comfortable using the firmware version itself to denote the upgrade path as opposed to a

CPL row reference as it was thought this would introduce unnecessary complexity. The benefit of using a firmware version name relates to user experience as that is the terminology they are already familiar with.

Device Manufacturers advised they are opposed to using the CPL Entry ID to provide the reference for the firmware. They noted that they, and their customers, use the firmware version name far more commonly which would make a solution more easily usable.

TABASC members agreed that the commonly known name for firmware versions should be included in the FIR entries.

SECAS highlighted with TABASC members, as well as with the Working Group that there are instances on the CPL where there is the same firmware version but different Manufacturer Hashes are provided for different entries. Using the CPL Entry ID provides a one-to-one relationship and therefore removes any ambiguity for the User. This therefore mitigates further against incorrect firmware upgrades being applied. They also noted that this is how the FIR is currently structured, which allows this solution to remain relatively simple. The TABASC expressed surprise that this would be an issue and believed it would be an extremely rare occurrence. SECAS has since identified that this is the case currently for multiple firmware versions on the CPL.

Working Group members were happy to use the CPL Entry ID as the reference point.

ZigBee information

Following the initial Working Group, the SSC has requested additional information to be included in this modification scope. It is proposed that these would be additional fields within the CPL submission. Following feedback from Device Manufacturers and discussion at the Working Group, the Proposed Solution will contain these fields, but they will only be made available to the SSC in a separate database. They will not be made available to SEC Parties.

ZigBee band

The CPL currently contains a field that can be used to populate the ZigBee band information. This is currently an optional field and as a result is not being widely populated. This allows the options of Single Band (2.4GHz), Single Band (Sub-GHz) or Dual Band. The proposal aims to extend the information by breaking down the ‘Dual Band’ Devices to include how the Device acts upon joining the HAN, either automatic selection, manual or can be either. See section 3 for further detail.

This information will become more important with the development of Devices such as Electric Vehicle (EV) Chargers or Heat Pumps that would require load control and be situated further away from the Communications Hub.

ZigBee chipset vendor and stack certificate

The SSC has stated that the provision of these two data items would assist them in understanding the extent of a risk when security vulnerabilities are notified to them, as well assisting with risk assessment for deploying firmware fixes.

SECAS notes that the provision of this data would be additional work for Device Manufacturers. There is also concern that the availability of the information could be a commercial risk.

New submissions or retrospective?

The Working Group questioned whether the intention was to update the FIR for existing entries, or whether this solution is just for new CPL submissions. SECAS noted that a new requirement would only be forward facing but would like to populate existing entries on a best endeavours basis by reaching out to Device Manufacturers on a voluntary basis. This would be via informal information exchange via email with all the necessary information to update the FIR from an authorised source. A MAP noted they would happily help with data population where they could but didn't think this should be too onerous for manufacturers.

It is worth noting in the exceptional circumstances where Manufacturers would like to send through correction entries for the FIR Upgrade Path, they will be able to do so by sending through their request in the form of email. The correction request will then be reviewed and actioned accordingly.

Who would be responsible for the information?

A Working Group member queried who would be responsible for any errors within the submission, or if a more optimal path becomes available later, would that be possible to update. SECAS confirmed that the data must be editable by SECAS for this reason and acknowledged that the manufacturer is best placed to provide the information but confirmed that the Supplier is currently responsible for the CPL submissions. A Working Group member was uncomfortable with Suppliers being responsible. They questioned whether implementation of MP222 'CPL submission efficiency improvements' would remove their responsibility as Device Manufacturers would be able to provide their own submissions. SECAS confirmed that the responsible Party will be whoever submitted the information.

Does this solution fix the root cause?

Some Working Group members identified that this solution will not resolve the root cause of the issue. They noted that some manufacturers are exploring putting additional controls within their firmware that would prevent an incorrect version being applied. SECAS agreed that this solution would not fix the root cause but highlighted that any change to mandate Device Manufacturers how to develop their firmware would either sit outside the SEC or be a change to the GBCS concepts and would be very lengthy, complex and expensive to deliver.

What Devices are included in the scope?

The Working Group agreed that ESMEs, GSMEs, HAN Connected Auxiliary Load Control Switches (HCALCS), Standalone Auxiliary Proportional Controllers (SAPCs) and Prepayment Meter Interface Devices (PPMIDs) should all be considered within any solution.

The Working Group also requested that's SMETS1 Communications Hubs be included as Suppliers are responsible for upgrading the firmware to those. However, as SMETS2 Communications Hubs are the responsibility of the DCC to upgrade then these will not be included. One Party questioned whether this would need to be included for the new 4G Communications Hubs. The DCC confirmed that all new 4G Communications Hubs would be SMETS2 and therefore firmware deployment will be managed by the DCC.

Following the Working Group, the SSC stated that all Communications Hubs should be within the scope as the additional information would be used to assess the impact of any security defects found within the ZigBee stack on a Device.

The Working Group agreed that this modification should only target Device upgrades and not include the interoperability of Devices, noting that is a far wider and more complex issue.

8. Case for change

Business case

The TABASC, SSC and Working Group all agreed that this is an issue that needs resolving. Suppliers, and subsequently consumers, will be positively impacted by the modification as it mitigates the risk of an incorrect upgrade path being followed that affects a Device. The costs incurred by Parties to amend processes to support the modification should be minimal and there are no DCC costs associated with the modification.

The Working Group supported moving ahead with this Proposed Solution.

Views against the General SEC Objectives

Proposer's views

The Proposer believes this better facilitates SEC Objective (a)[1] by ensuring that Devices work as intended.

Industry views

The Working Group and respondents to the Refinement Consultation agreed with the Proposer's view. One respondent to the Refinement Consultation also thought that it would better facilitate SEC Objective (c)[2].

Views against the consumer areas

Improved safety and reliability

This change will have a positive impact in this area by reducing the risk of Devices having unintended issues from an out of sequence firmware upgrade.

Lower bills than would otherwise be the case

This change is neutral in this area.

Reduced environmental damage

Indirectly this change would provide a benefit in this area as SEC Parties would have more confidence in designing processes and functionality that would result in Devices being reused and not scrapped.

Improved quality of service

This change will have a positive impact in this area by ensuring Suppliers can easily access data that gives them the correct upgrade pathways to prevent unintended issues arising.

[1] facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain

[2] the third General SEC Objective is to facilitate Energy Consumers' management of their use of electricity and gas through the provision to them of appropriate information by means of Smart Metering Systems;

Benefits for society as a whole

This change is neutral in this area.

Final conclusions

The Working Group noted that although some larger organisations may not individually utilise the Proposed Solution, it would deliver a benefit to industry and should help to address issues of incorrect firmware upgrade paths being used by Parties with less resource and knowledge.

The SSC was supportive of the implementation of the modification.

The TABASC is supportive of the modification, although has previously noted a preference for using the Firmware Version as the identifier. The Working Group did not support this view on the basis that the evidence from SECAS showed it does not provide a one-to-one relationship in the same way the CPL Entry ID would.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	13 Feb 2023
Presented to CSC for comment and conversion to Modification Proposal	21 Feb 2023
Modification discussed with Working Group	1 Mar 2023
Modification discussed with SSC	12 Apr 2023
Refinement Consultation	19 Apr – 12 May 2023
Modification discussed with SSC	24 May 2023
Modification discussed with TABASC	1 Jun 2023
Modification discussed with Working Group	7 Jun 2023
Modification Report approved by CSC	19 Dec 2023
Modification Report Consultation	20 Dec – 15 Jan 2024
Change Board Vote	24 Jan 24

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**
CPL	Central Products List
CSC	Change Sub-Committee

Glossary	
Acronym	**Full term**
DCC	Data Communications Company
ESME	Electricity Smart Metering Equipment
EV	Electric Vehicle
FIR	Firmware Information Repository
GBCS	Great Britain Technical Specification
GHz	Gigahertz
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switches
ID	Identifier
MAC	Medium Access Control
MAP	Meter Asset Provider
OPSG	Operations Group
OTA	Over-the-air
PPMID	Prepayment Meter Interface Devices
SAPC	Standalone Auxiliary Proportional Controllers
SCIRS	SSC Commercial Product Assurance Issue Resolution Subgroup
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specification
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TSIRS	Technical Specification Issue Resolution Sub-group

MP231 'Firmware upgrade pathways'

Annex A

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.

Section F 'Smart Metering System Requirements'

These changes have been redlined against Section F version 16.0.

Amend Section F2 as follows:

Firmware Information Repository

F2.14 The Panel shall establish and maintain a list of firmware releases, updates, and corresponding Manufacturer contact details (the **"Firmware Information Repository"**)~~.~~, for the following Devices:

(A) ESME

(B) GSME

(C) PPMID

(D) HCALCS

(E) SAPC

(F) SMETS1 CH or SMETS2+ Communications Hub

F2.15 The Panel shall ensure that the Firmware Information Repository contains a minimum of four ~~three~~ fields:

(a) A number which uniquely identifies a record on the Central Products List, which is a mandatory field;

(b) Manufacturer contact details, which is a mandatory field, to include email address, telephone number and business address; ~~and~~

(c) A free text field for release notes that Manufacturers can record against, which ~~i~~s a mandatory field for completion but the content is at the discretion of the Manufacturer~~s~~;

~~(c)~~(d) Where a firmware upgrade to the Device Model identified by (a) is possible, the number(s) of the record(s) on the Central Products List which identify the suitable baseline Device Model(s), which is a mandatory field;

F2.16 The Firmware Information Repository will be updated alongside the Central Products List, with the number which uniquely identifies a record on the Central Products List providing a cross reference.

F2.17 The Party or any other person submitting Device details for addition to the Central Products List shall also supply the details listed in F2.15 for the same Device.

F2.17B The information contained within the Firmware Information Repository shall be available to SEC Parties only and must not be shared.

Add to Section F2 as follows:

Device Zigbee Information Repository

F2.33 The Panel shall establish and maintain a list of Device Zigbee releases, updates and corresponding Manufacturer contact details (the "**Device Zigbee Information Repository"**).

F2.34 The Panel shall ensure that the Device Zigbee Information Repository contains a minimum of four fields:

(a) ZigBee chipset vendor, which is a mandatory field;

(b) ZigBee stack version, which is a mandatory field;

(c) ZigBee band, which is a mandatory field; and

(d) Central Product List entry ID.

F2.35 The Device Zigbee Information Repository will be updated alongside the Firmware Information Repository and the Central Products List, with the number which uniquely identifies a record on the Firmware Information Repository and the Central Products List providing a cross reference.

F2.36 The Device Zigbee Information Repository will include the Central Products List entry ID to allow the Data in the Device Zigbee Information Repository to be mapped to the Device on the Central Product List.

F2.37 The Party or any other person submitting Device details for addition to the Central Products List shall also supply the details listed in F2.15 for the same Device.

F2.38 The Security Sub Committee shall manage the access to the Device Zigbee Information Repository.

Section A ‘Definition and Interpretation’

These changes have been redlined against Section A version 34.0.

Add into A1 after Device Type as follows:

Device Zigbee Information Repository	means a table established and maintained by the Panel that details Device Zigbee details and Device Zigbee information.

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.

MP231 'Firmware upgrade pathways'

Annex B

Refinement Consultation responses

About this document

This document contains the full collated responses received to the MP231 Refinement Consultation.

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

Question 1				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
EON UK	Large Supplier	Yes but with reservations / health warning.	While the modification has significant merit, the missing part is the ability to access the manufacturer's latest release notes. These release notes give both the optimal firmware upgrade paths which are updated on every release. This can be in a schematic format which is much easier to understand than the proposed solution. The release notes can also contain guidance, known issues and other useful information e.g. whether the firmware supports block tariffs or not. MP231 would show that you "can" upgrade to a certain version, but the release notes would indicate whether you "should" upgrade to that version i.e. is it beneficial to perform that upgrade based on scenarios and circumstances. A Supplier could perform an authorised "upgrade", without realising the deleterious consequences of that "upgrade".	SECAS agrees that full access to Release Notes would be helpful. However, the SEC does not mandate the information that should be included and therefore varying depths of information can be included. In addition, Device Manufacturers have previously indicated that these are commercial documents and therefore their availability should be at the discretion of the Manufacturer.
OVO Energy	Large Supplier	Yes	We don't experience any issues with the manufacturers we work with, but we believe that it would be useful for the ones that we don't have a contract with.	-

Question 1				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
Calvin Asset Management Limited	Other SEC Party	Yes	As a Meter Asset Provider we are keen for suppliers to upgrade and maintain the meters on the most recent firmware and we are supportive of measures to help this process. Providing parties with the necessary information to improve the efficiency and reduce errors in the upgrade process for devices should benefit all parties.	-
Northern Powergrid Metering Limited	Other SEC Party	Yes	Northern Powergrid Metering Limited (NPML) are supportive of this solution and believe that whilst this does not fix the root cause of the issue (suppliers not being diligent in their upgrade process) it provides a single, central source for all meter firmware versions. We also believe this solution supports the "all reasonable endeavours" licence condition to ensure that meters are maintained in an operational state and are not removed prematurely. Preventing unnecessary removals ultimately reduces costs and inconvenience for customers.	-
British Gas	Large Supplier	Yes	In principle, this is a really good idea. We would prefer it to also include a retrospective update, that matched what realistically might still be on customer's walls or in the warehouse … ie including N-2 or N-3 retrospectively if possible.	SECAS will endeavour to collect the information on retrospective Devices. However, the legal obligations in the SEC should be forward facing.

Question 1				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
			However, it is still worth doing, even if the data isn't 100% complete retrospectively. Ownership of the firmware upgrade pathway (and responsibility to update it in the FIR) needs to sit with the manufacturers. This is outside the scope of this mod, but included in MP222 (which is out for Report consultation at the same time as this Refinement Consultation).	MP222 'CPL submission efficiency improvements' is due for vote at Change Board on 24 May 2023. If the modification is not approved then this point can be discussed with the Working Group to agree a way forward.

Question 2: Which identifier should be used as a reference to denote previous firmware versions required for the upgrade pathway?

Question 2				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
EON UK	Large Supplier	CPL Entry ID	Using the CPL Entry ID cannot be misinterpreted	-
OVO Energy	Large Supplier	-	We don't feel that this will impact us and therefore have no preference.	-
Calvin Asset Management Limited	Other SEC Party	Firmware version	We suggest firmware version as the most suitable identifier – as stated this is the terminology used in practice. Using the CPL entry ID would likely introduce further look-ups / cross checks into the process which could reduce the intended improvement in accuracy and efficiency. Whichever option is taken forward, should not be overly complex and needs to be consistently applied.	-
Northern Powergrid Metering Limited	Other SEC Party	CPL Entry ID	As multiple entries share the same firmware version name, and this can be across manufacturer in some cases, **it is critical that any ambiguity is removed.**	-
British Gas	Large Supplier	-	For IHDs that could be SMETS1 or SMETS2 – they would need to be separate line items (but same firmware version). We don't mind CPL Entry ID,	SECAS believes this answer is in relation to PPMIDs rather than IHDs.

Question 2				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
			but can they clearly show Hex for easy reference (or Firmware version) – that is what we are used to seeing from release notes, and it would be simplest if we can keep looking for the same reference.	Those PPMIDs that work in either SMETS1 or SMETS2 currently have two entries on the CPL where the firmware version differs between SMETS1 and SMETS2 Device Models. MP202 'Enduring Solution for SMETS1 and SMETS2+ PPMIDs' will allow for the same firmware version to be used for SMETS1 and SMETS2 PPMID Device Models. Firmware upgrades to PPMID SMETS2 Device Models based on GBCS version 4.1 or higher are possible whereas it is not possible to carry out firmware upgrades of SMETS1 PPMID Device Models using the same firmware version as the corresponding SMETS2 PPMID Device Models. Using the firmware version as the look-up criteria would incorrectly suggest that firmware updates to SMETS1 PPMID Device Models are possible; therefore using the CPL Entry ID as the reference would provide a unique reference avoiding any ambiguity. Since the consultation was issued, SECAS has reviewed the current CPL entries more fully and noted that the same firmware versions are used by multiple manufacturers for Device Models. Therefore, to remove ambiguity the manufacturer code would also be needed as a minimum along

Question 2				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
				with the firmware version to become part of the Firmware Upgrade Path. It might also be required to add the device model identifier, and possibly the device hardware version and revision, to ensure uniqueness. Note that this will not be sufficient to differentiate between SMETS1 and SMETS2 PPMID Device models using the same firmware version (as explained above). The Firmware Upgrade Path is deemed to be only available to SEC Parties, this is why it is added to the FIR instead of the CPL. For ease of use the FIR and CPL can be combined by means of a standard Excel Xlookup using the CPL Entry Number as a key. This allows the creation of a single list which can be filtered.

Question 3: Do you agree that the provision of ZigBee stack version and ZigBee chipset vendor should be included?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	Yes	This is useful information if a known issue is related to the ZigBee stack version and ZigBee chipset vendor
OVO Energy	Large Supplier	-	We don't use this in Live, so believe it is more of a security point
Calvin Asset Management Limited	Other SEC Party	-	We do not have a view on this but would reiterate the need to keep the information as simple as possible.
Northern Powergrid Metering Limited	Other SEC Party	Yes	This being present in the repository will allow suppliers to better identify issues present in specific stack versions and may allow for better management of issues across manufacturers.
British Gas	Large Supplier	Yes	Yes, we would support this being included. It would be useful to know if there was a stack specific issue.

Question 4: Do you agree that information on a Device's ZigBee banding and how it is used to join the HAN, should be included within this modification?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	Yes	Useful for diagnostics and support
OVO Energy	Large Supplier	Yes	Although we don't use this, it may be of value for devices that don't upgrade to understand why
Calvin Asset Management Limited	Other SEC Party	-	We do not have a view on this but would reiterate the need to keep the information as simple as possible.
Northern Powergrid Metering Limited	Other SEC Party	Yes	The overall aim of this modification is to ensure that meters on the wall remain on the wall, and any information that will aid in joining the HAN should be included if there is an opportunity to provide this without incurring additional costs to industry
British Gas	Large Supplier	Yes	Yes, we would support this being included.

Question 5: Do you agree that both SMETS1 and SMETS2 Communications Hubs should be included within the scope of this modification?

Question 5				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
EON UK	Large Supplier	Yes	SMETS1 Communication Hubs should definitely be included as they are upgraded by Suppliers. SMETS2 Communication Hubs are optional as DCC upgrades them.	-
OVO Energy	Large Supplier	Yes	Yes, because it would be useful to know how many different FW upgrades would be required to get up to the current one.	-
Calvin Asset Management Limited	Other SEC Party	No	We are unclear why comms hubs are being considered as part of this as we understood this change only relates to meters, not comms hubs. Adding references to comms hubs may confuse entries further.	Working Group noted that Suppliers are responsible for SMETS1 Communications Hub firmware update and therefore suggested inclusion. The SSC has also asked that SMETS2 Communications Hubs be included as this information is deemed useful from a risk assessment perspective.
Northern Powergrid Metering Limited	Other SEC Party	Yes	Taking a consistent approach to populating this list makes sense, exclusion of comms hubs may cause confusion where a supplier is responsible for updating SMETS1 hubs.	-

Question 5				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
British Gas	Large Supplier	Yes	As a Supplier, we definitely want SMETS1 Comms Hubs included, as we are responsible for upgrades. As a Supplier, we are not particularly interested in SMETS2 Comms Hubs, as we don't upgrade them (the CSP does instead). However, if this database information is going to be used by more than just Suppliers, it seems sensible for SMETS2 Comms Hubs to be included.	-

Question 6: Do you agree that the legal text will deliver MP231?

Question 6				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
EON UK	Large Supplier	Yes	Although without release note access, I would not rely exclusively on the information contained in the Firmware Information Repository	-
OVO Energy	Large Supplier	Yes	-	-
Calvin Asset Management Limited	Other SEC Party	Yes	-	-
Northern Powergrid Metering Limited	Other SEC Party	Yes	The changes proposed are mandatory, and specific enough to ensure that the information provided will be usable by all SEC parties interested in the CPL.	-
British Gas	Large Supplier	Yes	Text seems correct, except for: F2.14 use of 'CH' abbreviation in (F). This looks like a typo. Nothing in the legal text supports the "Best Endeavours" point at the bottom of page 5 of the MP231 draft Modification Report. The legal text reads as though it is mandatory for all devices on the FIR (new ones going forwards, and old ones).	This definition for a SMETS1 Communications Hub is found in the SEC Definitions as "means a physical device comprising a SMETS1 CHF and a SMETS1 GPF. The best endeavours approach to retrospective population is not seen as a legal obligation. This would be an effort from SECAS to better facilitate the introduction of the process. This

Question 6				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
				discussion point can be covered off in the Working Group to determine other viewpoints.

Question 7: Do you agree with the proposed implementation approach?

Question 7				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
EON UK	Large Supplier	Yes	N/A	-
OVO Energy	Large Supplier	Yes	-	-
Calvin Asset Management Limited	Other SEC Party	Yes	-	-
Northern Powergrid Metering Limited	Other SEC Party	Yes	This change does not impact additional documentation outside of the CPL and FIR. As the implementation approach is aiming to make new entries mandatory, additional delays only create more blank entries on releases that occur between modification approval and implementation.	-
British Gas	Large Supplier	Yes	We would prefer the implementation to be retrospective as well (ie for older devices).	See response to Q6.

Question 8: Will there be any impact on your organisation to implement MP231?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	No	This assumes MP222 is completed. Otherwise, the Supplier would need to obtain the information for the submission process.
OVO Energy	Large Supplier	No	No, as upgrade paths already exist in Manufacturers Release Notes and we have access to the CPL
Calvin Asset Management Limited	Other SEC Party	Yes	We provide a firmware repository for our customers and this information will be useful for us to provide to our customers to give them the accurate upgrade path for firmware.
Northern Powergrid Metering Limited	Other SEC Party	No	-
British Gas	Large Supplier	No	Useful thing to have. No mandatory change for us.

Question 9: Will your organisation incur any costs in implementing MP231?

Question 9			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	No costs	N/A
OVO Energy	Large Supplier	Less than £100k	Modification costs
Calvin Asset Management Limited	Other SEC Party	No costs	-
Northern Powergrid Metering Limited	Other SEC Party	No costs	-
British Gas	Large Supplier	No costs	-

Question 10: How long from the point of approval would your organisation need to implement MP231?

Question 10			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	N/A	There would only be impact as and when a new CPL entry was being submitted.
OVO Energy	Large Supplier	Immediately	-
Calvin Asset Management Limited	Other SEC Party	N/A	-
Northern Powergrid Metering Limited	Other SEC Party	N/A	-
British Gas	Large Supplier	-	No implementation time required, as there is not mandatory change for us. However, it will be a useful resource to have access to as soon as it is available.

Question 11: Do you believe that MP231 would better facilitate the General SEC Objectives?

Question 11			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	Yes	Potentially, it may provide a more robust customer experience
OVO Energy	Large Supplier	Yes	-
Calvin Asset Management Limited	Other SEC Party	Yes	We consider this supports the facilitation of SEC Objectives A and C
Northern Powergrid Metering Limited	Other SEC Party	Yes	Firmware upgrades ensure that devices continue to work as intended and this modification will better facilitate SEC objective (a).
British Gas	Large Supplier	Yes	Agree that it would better facilitate General SEC Objective A.

Question 12: Do you believe there will be any impacts on or benefits to consumers if MP231 is implemented?

Question 12			
Respondent	**Category**	**Response**	**Rationale**
EON UK	Large Supplier	Yes	Potentially, it may provide a more robust customer experience
OVO Energy	Large Supplier	Yes	One benefit will be having extra information on the upgrade paths to help make things even clearer
Calvin Asset Management Limited	Other SEC Party	Yes	Positive benefit as this will help suppliers ensure they are taking the appropriate action to maintain installed meters with appropriate firmware which helps to maximise security of the meter and ensure it functions effectively.
Northern Powergrid Metering Limited	Other SEC Party	Yes	This will see fewer meters being damaged by incorrectly applied firmware. Depending on the issues resolved on the specific firmware versions, this will lead to mitigating any unintended consequences of not applying firmware correctly.
British Gas	Large Supplier	Yes	Helps ensure more devices are working.

Question 13: Noting the costs and benefits of this modification, do you believe MP231 should be approved?

Question 13				
Respondent	**Category**	**Response**	**Rationale**	**SECAS Response**
EON UK	Large Supplier	Yes	Noting that this does not solve the core issue of easy access to Manufacturer Release Notes (and firmware images)	See response to Q1.
OVO Energy	Large Supplier	Yes	As this is a relatively low cost when spread across all Suppliers, we don't have an issue with this being approved, as it's more of a nice to have.	-
Calvin Asset Management Limited	Other SEC Party	Yes	As per responses to questions 1 and 2	-
Northern Powergrid Metering Limited	Other SEC Party	Yes	The cost to implement this modification will likely be recovered via prevention of meter removal caused by incorrectly applying firmware upgrades.	-
British Gas	Large Supplier	Yes	Seems sensible, and cost is reasonable.	-

Question 14: Please provide any further comments you may have.

Question 14			
Respondent	**Category**	**Comments**	**SECAS Response**
EON UK	Large Supplier	N/A	-
OVO Energy	Large Supplier	-	-
Calvin Asset Management Limited	Other SEC Party	-	-
Northern Powergrid Metering Limited	Other SEC Party	Clarity should be added to the ability to modify the previous entries where a more efficient path becomes available to also include the ability to remove paths that have had issues identified.	SECAS will be able to update the FIR retrospectively. This is not called out in legal text but will form part of the solution and is covered in the Modification Report.
British Gas	Large Supplier	Particularly useful for meters we won't have installed ourselves.	-