This document is classified as **CLEAR** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SECAS Guidance Document:
Central Products List (CPL) – Version 6.0

Contents

1 About this guidance document

This guidance document V6.0 applies to Central Products List (CPL) Version 3.000 or higher; it is aligned with the Smart Energy Code (SEC) v86.0. When necessary SECAS will replace this document with a new version.

With the changes introduced by the SEC v86.0, any CPL prior to Version 3.000 can no longer be used for CPL submissions.

Guidance Version	Change Summary
V6.0	Added Section 5.1 Details: 'Version Control' Tab
V6.0	Modified Section 7.2.4.3 Trial Device Certificate MP168: Security Characteristics must be set to 'Not Relevant' for Trial Device Certificates
V6.0	Modified Section 7.2.9 Data Group: 'Manufacturer Contact FIR' and 'FIR Release Notes' MP231: FIR information mandatory for all CPL submissions
V6.0	Added Section 7.2.10 Data Group: 'Firmware_Upgrade' MP231 – New Data Group
V6.0	Added Section 7.2.11 Data Group: 'ZigBee_Properties' MP231 – New Data Group
V6.0	Added Section 7.2.12 Data Group: 'Device_ZigBee_Information_Repository' MP231 – New Data Group
V6.0	Modified Appendix 6 Firmware Information Repository (FIR) MP231 – Addition of Firmware Upgrade Path
V6.0	Added Appendix 7 Device ZigBee Information Repository (DZIR) MP231 – New DZIR document

Table 1: Document changes

2 Who does this guidance apply to?

Any individual who needs to add information to the CPL should ensure they follow the guidance set out in this document.

The main section of this guidance covers:

- How to submit a product for inclusion on the CPL;
- What information and documentation is required to support a CPL submission;
- How SECAS validates and adds submissions; and
- How SECAS informs about changes to the CPL.

Additional information is contained in the appendices to further aid with understanding:

- What a Hash is and why it is needed;
- How to obtain and apply a digital signature to a submission if including a Hash;
- How Devices have their status set to 'Removed' on the CPL; and
- What the Firmware Information Repository (FIR) is and how to submit firmware information.

This guidance is based upon the latest version of the Smart Energy Code (SEC), namely SEC Section F2, and SEC Appendix Z - CPL Requirements Document.

3 What is the Central Products List?

The Panel (via SECAS) establishes and maintains the Central Products List (CPL) as per SEC Section F. Please view the latest version of the CPL here.

The CPL is made up of:

- **SMETS2+ Device Models** where all Assurance Certificates have been provided as required by the Technical Specifications; and
- **SMETS1 Device Models** where all information has been provided in accordance with the CPL Requirements Document.

4 Who uses the CPL?

The DCC uses the CPL to manage the Smart Metering Inventory (SMI). For a Device to be listed on the SMI, it must be listed on the CPL first.

The SMI is an electronic database that records whether a Device can communicate via the Data Communications Company (DCC).

SEC Parties also use the CPL to identify which Devices have received their required Assurance Certificates.

If you have any questions or would like further information, please contact us by emailing our SECAS Helpdesk or call 020 7090 7755.

5 The CPL format

The CPL is an Excel Macro-Enabled Workbook and it uses the file extension '.xlsm'.

The 'CPL – New Entry' tab is associated with an Excel macro which can be used to validate CPL submission details prior to the submission to SECAS. This Macro is only available when the CPL is saved as Excel Macro-Enabled Workbook (.xlsm).

There are four tabs on the CPL:

1. The **Version Control** tab shows a high-level change history of the CPL. Devices and Manufacturer names are listed in Plain English with a brief explanation of the change that is being made in each CPL version.
2. The **CPL - New Entry** tab is what you will need to complete to make a SMETS1 (for the DCC only) or SMETS2+ submission (for all Device Manufacturers) to SECAS.
3. The **Central Products List** tab lists the details of all current and removed SMETS1 and SMETS2+ Device Models.
4. The **CPL - Saveable in CSV** tab is issued by SECAS to the DCC in a *.csv formatted file to allow the DCC to successfully import the new version of the CPL into its systems.

Figure 1 below shows all CPL tabs with the 'CPL – New Entry' being highlighted:

Figure 1: CPL Tabs

All CPL tabs are protected to prevent inadvertent changes to the data; only the cells on the 'CPL – New Entry' tab where submission details are to be entered can be changed.

5.1 Details: 'Version Control' Tab

The 'Version Control' Tab contains the following information relating to the versioning of the CPL:

- Version Number
- Date Of Issue

- Changes incorporated

The Version Number uses the format X.YYY where the number before the decimal point identifies the principal version and the number after the decimal point identifies the sub-version.

The principal version is updated when the structure of the CPL changes, e.g. when adding a Data Group or a Data Attribute.

The sub-version is updated each time a new CPL is released; e.g. when new Device Models were added or after the selection options for an existing field had been changed.

Changes to the CPL are aligned with changes to the SEC, early visibility of upcoming changes is available as part of the SEC Modification process.

5.2 Details: 'CPL – New Entry' Tab

Any data item on the 'CPL – New Entry' tab is uniquely identified by the combination of the values contained in the

- **Data Group** fields in column A, and the
- **Data Attribute** fields in column B.

Additional columns on the 'CPL – New Entry' tab explain the data item further:

- **Notes**
  The 'Notes' field in column C contains explanations of the data item.
- **Conditionality Rule**
  The 'Conditionality Rule' field in column D specifies whether the data item must be populated for a given Device Model.
- **Format**
  The 'Format' field in column E shows the formatting that must be used for the data item.
- **Valid Values**
  The 'Valid Values' field in column F contains the permitted entry value(s) or entry ranges for the data item.

The actual CPL submission details must be entered by the submitter in the '**New Entry's Details**' fields in column G. When entering data items please ensure to:

- Follow the rules set out in the fields 'Conditionality Rule', 'Format' and 'Valid Values', and
- Use values from the pre-defined in-cell drop down selections where available.

All the above items may be subject to change when a new SEC is released, resulting e.g. in a new combination of Data Group and Data Attribute, or a change of entry values.

The Version Number and the Date Of Issue from the 'Version Control' tab are also repeated in cell 'A2' on the 'CPL – New Entry' tab. We recommend to always use the latest version of the CPL from the SECAS website when preparing a CPL submission.

5.3 Details: 'Central Products List' Tab

The tab 'Central Products List' contains all Device Models that have been added to the CPL.

The header lines of this tab mirror the corresponding fields from the columns in the 'CPL – New Entry' tab. The content in the fields 'Conditionality Rule', 'Format', and 'Valid Values' may change with a new SEC release, resulting in Device Models already present on the CPL to show different values. These values were valid at the time the Device Models had been added to the CPL.

The status of a Device Model is shown in the column identified by the 'Entry' Data Group and the 'status' Data Attribute. There are two possible settings:

- 'Current', meaning that the DCC can communicate with the Device Model, or
- 'Removed', meaning that only non-critical communication with the Device Model is possible.

6 SMETS1 CPL Submission Procedure

6.1 Standard SMETS1 CPL Submission Procedure (for the DCC only)

The DCC is responsible for submitting all SMETS1 CPL submissions. There are a number of governance steps SMETS1 submissions must pass through before they can be added to the CPL:

1. The SMETS1 Pending Products Combination List (PPCL) tracks SMETS1 Device Model Combinations (DMCs) whilst they are undergoing eligibility testing **pending** BEIS approval to be added to the Eligible Products Combination List (EPCL).
2. BEIS decides which DMCs are eligible for enrolment into the DCC and these are added to the SMETS1 Eligible Products Combination List. Only Device Models present on the EPCL can be added to the CPL.
3. Once SECAS has received all the required information as per SEC Appendix Z, SMETS1 CPL submissions can be added to the CPL.
4. Once a Device Model has been successfully deployed by a User and is enrolled in the DCC, it is listed on the Deployed Products List (DPL).

SMETS1 Device Models do not require any Assurance Certificates.

For the DCC to note: The submission form and process used is the same as for SMETS2+ Devices, as outlined below.

6.2 SMETS1 Supplier Party CPL Notification Procedures (for Suppliers only)

The SEC allows a Supplier Party to add a SMETS1 Device Model to the CPL; this is limited to cases where an urgent material security vulnerability needs resolving for a commissioned Device and where the Supplier is the Responsible Supplier. For all other cases, the DCC is responsible for submitting SMETS1 submissions as explained in Section 6.1.

Only Device Models that are not be present on the EPCL can be added by following the process below. The latest version of the EPCL is available for download here and, as an initial step, the Supplier must verify whether the Device Model is present on the EPCL. If the Device Model is not on the EPCL, the Supplier should email the SECAS Security Team at ssc@gemserv.com and the SECAS Helpdesk at secas@gemserv.com, providing the necessary reasons for the urgent material security vulnerability fixes required. The Security Team will then provide this to the Security Sub Committee (SSC). The SSC will then advise the Supplier on the material required to carry out the review.

The SSC will review whether an urgent material security vulnerability exists before the Device Model can be added to the CPL and communicate the result of this review to the Supplier and SECAS.

If the SSC confirms that there is a need for an urgent security vulnerability fix, the Supplier should email the SSC confirmation email and a new CPL submission form to the SECAS Helpdesk for processing within one working day.

Should the SSC come to the conclusion that there are no urgent material security vulnerabilities present, then the Supplier will be informed.

7 SMETS2+ CPL Submission Procedure

When adding a SMETS2+ Device to the CPL, please follow the steps below carefully. SECAS will check and validate your submission(s) upon receipt. However, it is important that you take care when following the process and ensure that you include and check all the required information & supporting documents.

7.1 Step One: Download the latest version of the CPL

Please view the latest version of the CPL here. Click on this link to download the CPL workbook.

The 'CPL - New Entry' worksheet of the CPL spreadsheet contains a **Validation Macro** which allows you to validate new Device Model entries. This tool is further explained Section 7.4 and Appendix 7.

Please note that for the macro to work you must save the CPL as a *.xlms (Excel Macro-enabled Workbook) file; and ensure that the '**CPL - New Entry**' worksheet is present and **has not been renamed**.

As a submitter, you may:

- Change the CPL file name (e.g. to reflect your submission);
- Remove the 'Version Control', 'Central Products List' and 'CPL - saveable in CSV' worksheets (but not the 'CPL - New Entry' worksheet); and
- Add further worksheets.

7.2 Step Two: Enter Device Model details

Open the workbook and navigate to the 'CPL - New Entry' worksheet.

You must **only** add details to the fields that you are required to complete within Column G 'New Entry's Details'. This depends on the type of Device being submitted and Table 2 below shows for each 'Data Group' in column A whether the fields need to be populated.

Data Group	Device Applicable
Entry	Assigned by SECAS after submission, all Devices
Device_Type	All Devices
Device_Model	All Devices
SMETS/CHTS Version	All Devices
GBCS Version	All Devices
CPA_Certificate	All SMETS2+ devices **except** Pre-Payment Interface Devices.
DLMS_Certificate	SMETS2+ Electricity Metering Equipment including the SAPC
ZSE_Certificate	All SMETS2+ devices
Manufacturer_Image	All Devices which include a Manufacturer Image Hash
Contact-CPA	All SMETS2+ Devices **except** Pre-Payment Interface Devices.
Manufacturer Contact FIR	All SMETS1 and SMETS2+ ESME and GSME Devices
FIR Release Notes	All SMETS1 and SMETS2+ ESME and GSME Devices

Table 2: Submission form field applicability

7.2.1 Data Group: 'Device_Type'

The following Device types must be present on the CPL and require CPL Submissions:

- Communications Hub
- Gas Smart Meter
- HAN Connected Auxiliary Load Control Switch
- Polyphase Electricity Metering Equipment
- Pre-Payment Interface Device
- Single Element Electricity Metering Equipment
- Twin Element Electricity Metering Equipment

Please note that the 'Standalone Auxiliary Proportional Controller' (SAPC) must be entered as Device type 'Single Element Electricity Metering Equipment'.

The Device types 'In Home Display' and the 'Consumer Access Device' are not listed on the CPL and don't require CPL submissions.

7.2.2 Data Group: 'Device_Model'

In the Data Group 'Device_Model' the 'CPL – New Entry' tab lists five Data Attributes:

- manufacturer_identifier
- model_identifier
- hardware_version.version
- hardware_version.revision
- firmware_version

These fields follow the notation of the ZigBee Over the Air (OTA) header information defined by the Connectivity Standards Alliance (CSA). In case a field contains several bytes, these must be separated by a colon ":".

Please note that it must be possible to uniquely identify a Device Model by the above Data Attributes on the Assurance Certificates (Commercial Product Assurance (CPA), Device Language Message Specification (DLMS), and ZigBee) which are part of the CPL submission. This also applies to letters from the National Cyber Security Centre (NCSC), the SSC, and Test Labs.

In case the unique identification is not possible, **additional information is required** to clearly identify the mapping between the Device details in the CPL Submission form and the Assurance Certificate(s). This may take the form of the full, or an extract from, the related **Release Notes** of the Device.

7.2.3 Data Group: 'SMETS/CHTS Version' and 'GBCS Version'

The September 2020 Release of the SEC introduced Device Level Versioning for SMETS2+ Devices. All SMETS2+ documents are referred to by their release date; the version numbering is applied to the Device specific sections of the SMETS (instead of the entire SMETS document).

For SMETS2+ Devices, the CPL continues to use the term "SMETS" followed by a version number which refers to the Device specific subsection of the SMETS.

The Communications Hub Technical Specifications (CHTS) versions selectable in the CPL refer to the entire CTHS documents as published on the SECAS website.

Device Level Versioning and valid SMETS/CHTS and GBCS version combinations for all devices can be found in SEC Schedule 11 - Technical Specification Applicability Tables (TSAT).

It is the responsibility of Device Manufacturers to check they have used the correct SMETS/CHTS and GBCS combinations when submitting new device models.

7.2.4 Data Group: 'CPA_Certificate'

There are three types of CPA certificates that can be used for CPL submissions:

- Lifetime CPA Certificate
- Expiring CPA Certificate
- Trial Device Certificate

The Data Group 'CPA_Certificate' is required for all SMETS2+ Devices with the exception of the PPMID. It contains three Data Attributes:

- identification_number
- security_characteristics_version
- expiry_date

All fields must be populated on the CPL Submission form, the values of the information that need entering depend on the CPA Certificate type; please see the subsections for each CPA Certificate below.

One or more Devices can be added to **an existing CPA Certificate** (Section 5 of SEC Appendix Z) as long as the changes to the new Device Model do not significantly impact the security functions (as set out in the CPA Assurance Maintenance Plan). In this case SECAS requires a confirmation letter from an authorised Test Lab (NCC Group or KPMG or CyTAL) to confirm that there are no security impacts.

Please note that it must be possible to match the Device details on the CPA Certificate with the Device Model details of the CPL submission; this also applies to letters from the NCSC, the SSC, and authorised Test Labs, where these form part of the CPL submission. See Section 7.2.2 and Appendix 4 for further information.

For Device Models already present on the CPL a new CPL submission is not needed where:

- a new CPA Certificate has been issued,
- the CPA expiry date has changed, or
- the CPA renewal date has changed.

Please send the necessary documentation (CPA Certificate etc) to SECAS@gemserv.com.

7.2.4.1 Lifetime CPA Certificate

For all new Devices the NCSC issues Lifetime CPA Certificates showing the CPA Certificate Number and date the Certificate has been awarded. The Lifetime CPA certificate doesn't show an expiry date. The NCSC also issues a separate letter stating the date of the next Risk Review, this date must be used for the 'expiry_date' attribute. You need to place the prefix '[R] ' in front of the Lifetime CPA Certificate Number when filling in the 'CPL – New Entry' form.

Data Attribute	Example	Data Source
identification_number	**[R]** ABC123456789	CPA Certificate
security_characteristics_version	Security Characteristics version 1.4	CPA Certificate
expiry_date	25/10/2026	NCSC Letter

Table 3: Lifetime CPA Certificate example

7.2.4.2 Expiring CPA Certificate

Some Devices may still use the Expiring CPA Certificate issued by the NCSC; these show the CPA Certificate Number, the date the Certificate has been awarded and the date when the Certificate expires. An extension of the expiry date is documented in a letter from the NCSC. You need to place the prefix '[E] ' in front of the Expiring CPA Certificate Number when filling in the 'CPL – New Entry' form.

Data Attribute	Example	Data Source
identification_number	**[E]** DEF123456789	CPA Certificate
security_characteristics_version	Security Characteristics version 1.4	CPA Certificate
expiry_date	25/10/2026	CPA Certificate or NCSC Letter

Table 4: Expiring CPA Certificate example

7.2.4.3 Trial Device Certificate

It is possible to add devices to the CPL using a Trial Device Certificate. These are issued by the SSC and show the Identifier code, the date the Trial Device Certificate has been awarded and the expiry date. The Trial Device Certificate isn't based on a particular version of the Security Characteristics and the data attribute 'security_characteristics_version' must be set to 'Not Relevant' when making a CPL submission. You need to place the prefix '[T] ' in front of the Identifier code from the Trial Device Certificate when filling in the 'CPL – New Entry' form.

Data Attribute	Example	Data Source
identification_number	**[T]** GKL123456789	Trial Device Certificate
security_characteristics_version	Not Relevant	Trial Device Certificate
expiry_date	25/10/2026	Trial Device Certificate

Table 5: Trial Device Certificate example

7.2.5 Data Group: 'DLMS_Certificate'

The Data Group 'DLMS_Certificate' is only required for SMETS2+ ESME Devices, it contains two Data Attributes:

- identification_number
- DLMS_version

The values present on the DLMS Certificate must be entered in the CPL Submission form.

Please note that it must be possible to match the Device details on the DLMS Certificate with the Device Model details of the CPL submission, see Section7.2.2 for further information.

7.2.6 Data Group: 'ZSE_Certificate'

The Data Group 'ZSE_Certificate' is required for all SMETS2+ Devices, it contains two Data Attributes:

- identification_number
- ZSE_version

The values present on the ZSE Certificate must be entered in the CPL Submission form.

Please note that it must be possible to match the Device details on the ZSE Certificate with the Device Model details of the CPL submission, see Section7.2.2 for further information.

7.2.7 Data Group: 'Manufacturer_Image'

The Data Group 'Manufacturer_Image' Attributes relates to the Hash of the Manufacturer Image and is required if the Device Model will be used for firmware upgrades of Devices. There are three Data Attributes and all fields must be populated:

- creator
- hash
- descriptor

For SECAS to associate a Hash with a Device Model you must provide the identity of the person who created the Manufacturer Image: Submitters must digitally sign each CPL submission that contains a Hash (See Section 7.5).

If you are unsure what a Manufacturer Image is, or why you may need to include a Hash, please go to Appendix 1 of this guide.

7.2.8 CPL submissionData Group: 'Contact-CPA'

The items in the Data Group 'Contact-CPA' must be provided for all SMETS2+ devices except the PPMID. There are three Data Attributes in this Data Group:

- Contact.contact name
- Contact.contact telephone
- Contact.contact email

All fields must be populated.

7.2.9 Data Group: 'Manufacturer Contact FIR' and 'FIR Release Notes'

The Firmware Information Repository (FIR) is an Excel spreadsheet available to SEC Parties with a valid SEC website login. SEC Parties can register for a SEC website account here.

The latest version of the FIR can be downloaded here.

You must provide FIR details for all Devices.

Release notes should only contain **public information**. All content is at the discretion of Device Manufacturer.

SECAS will extract this information from the 'CPL - New Entry' worksheet and add it to the FIR spreadsheet; these items will not be published on the CPL.

For more information about the FIR, please see Appendix 6 of this guide.

7.2.10 Data Group: 'Firmware_Upgrade'

The Data Group 'Firmware_Upgrade' contains a single Data Attribute named 'Path'; SECAS will extract the submission data and add this to the Firmware Information Repository.

This field is mandatory for all Devices and you must provide the details; it can hold up to 15 CPL Entry numbers of Device Models already present on the CPL in column B 'Entry.number'.

Any Device Model already present on the CPL, which can be upgraded **directly** (no interim step needed) to the Device Model in the new CPL submission, must be listed in the 'Path' field with its CPL Entry number. This serves as a quick guidance for Suppliers to ensure that firmware upgrades are carried out in the correct order.

Please set this field to 'NA' in case

- the CPL submission doesn't contain a Hash of the Manufacturer Image;
- the GBCS Version doesn't allow firmware upgrades; or
- there is no existing Device Model on the CPL which can be upgraded to the Device Model in the new CPL submission.

For more information about the FIR, please see Appendix 6 of this guide.

There is no requirement to add this information to Device Models which were already listed on the CPL prior to the release of SEC v86.0. If you wish to add this information to a historic Device Model please contact SECAS@gemserv.com.

7.2.11 Data Group: 'ZigBee_Properties'

The Data Group 'ZigBee_Properties' contains a single Data Attribute named 'Bands_Join'. This provides the information of the ZigBee radio frequency band(s) supported by the Device and how the selection of the radio frequency band is done.

You must provide the details as part of the CPL submission.

This information is published on the CPL in column V 'Zigbee_Properties.Bands_Join'.

There is no requirement to add this information to Device Models which were already listed on the CPL prior to the release of SEC v86.0. If you wish to add this information to a historic Device Model please contact SECAS@gemserv.com.

7.2.12 Data Group: 'Device_ZigBee_Information_Repository'

The items in the Data Group 'Device_ZigBee_Information_Repository' must be provided for all Devices. There are two Data Attributes in this Data Group:

- Stack_Vendor
- Stack_Version

All fields must be populated.

This information is listed in the Device Zigbee Information Repository (DZIR); this document is not publicly available and is controlled by the Security Sub Committee.

There is no requirement to add this information to Device Models which were already listed on the CPL prior to the release of SEC v86.0. If you wish to add this information to a historic Device Model please contact SECAS@gemserv.com.

7.3 Step Three: Saving the completed CPL - New Entry Tab

The populated CPL must be saved using the standard Excel methods by selecting "File" from the top menu followed by "Save as" and select an appropriate name for the Excel Workbook.

- You must ensure you save it as a ***.xlms (Excel Macro-enabled Workbook) file** in order for the 'Validate New Entry' macro to work.
- The name of the "CPL - New Entry" worksheet must not be changed.

Note that using the Excel method "Move or Copy" to save a copy of the 'CPL - New Entry' form in another Excel workbook may result in issues and must not be used.

7.4 Step Four: Validating your submission entries

The 'CPL - New Entry' worksheet contains a built-in macro which validates the entry details.

- For every field: The formatting of the data.
- For fields with a selection list: Whether the data matches a selection from the list.
- For linked fields: Whether the combination of entries is permitted, e.g. for Device Level Versioning.

Please ensure that there is only one instance of the 'CPL – New Entry' form open on your computer before executing the macro.

The '**Validate New Entry**' macro is executed by clicking the soft button as shown here:

Figure 2: Validation Macro Soft Button

Any error will be returned in a pop-up window summarising the errors received as well as in red text directly onto the worksheet in Column I. You must correct all errors before proceeding.

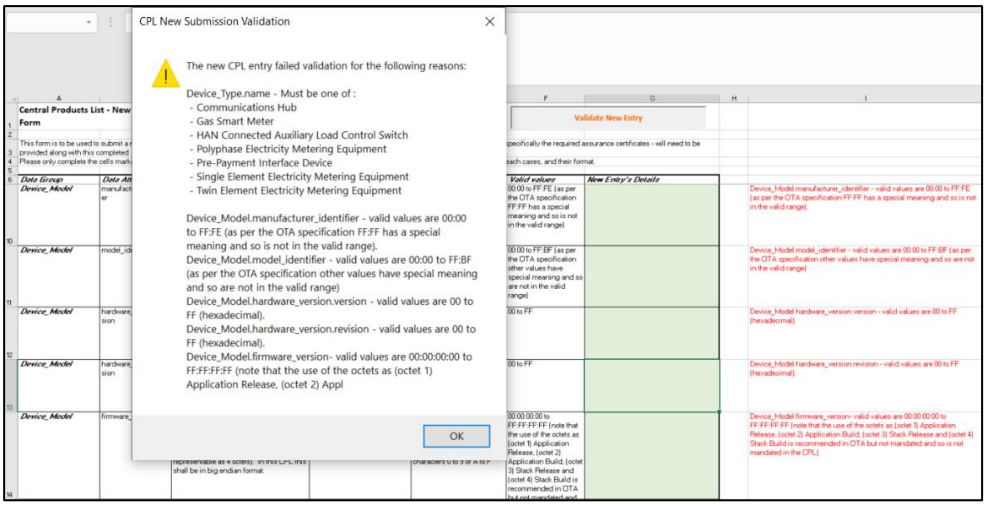

Figure 3: Validation Results

If the submission is valid, a **Success Message** will state 'The new CPL entry passed validation checks' and all items will be set to '**OK**' in black font in Column I.

You can run the '**Validate New Entry**' macro multiple times to address all issues prior to submission.

7.5 Step Five: Adding your Digital Signature (if including a Hash)

You must apply a digital signature to the 'CPL - New Entry' worksheet when making a submission that contains an associated Hash, see also Section 7.2.7. The submission must be digitally signed by the person who created the Manufacturer Image.

SECAS will continue to accept existing authorisations until MP168 is fully implemented and Manufacturers can obtain IKI Certificates.

The signing of Excel spreadsheets is explained on Microsoft's website. To read more about applying a digital signature, please see Appendix 2 of this guide.

7.6 Step Six: Attaching relevant Assurance Certificates to your submission email

A Smart Meter Assurance Certificate provides a guarantee that SMETS2+ Devices have been tested, are interoperable and secure.

Table 6: Assurance Requirements below shows the Assurance Certifications required by each SMETS2+ Device Type:

Device Type	ZigBee	CPA	DLMS
Pre-Payment Interface Device	✓		
Communications Hub	✓	✓	
Gas Smart Meter	✓	✓	
HAN Connected Auxiliary Load Control Switch	✓	✓	
Single Element Electricity Metering Equipment	✓	✓	✓
Twin Element Electricity Metering Equipment	✓	✓	✓
Polyphase Electricity Metering Equipment	✓	✓	✓

Table 6: Assurance Requirements

You must ensure all relevant certificates are attached before emailing your submission(s) to SECAS.

This is the case even if the certificate has been submitted as part of a previous submission. If the certificate is not included, it will not be possible for SECAS to process the submission.

More information on the three certificate types can be found below and in Appendix 3 of this guide.

7.7 Step Seven: Attaching relevant auxiliary documents to your submission email

A number of auxiliary documents may need to be added to your CPL submission email.

If the Device Model can't be identified on the Assurance Certificates by using the Device Model details, then an additional document must be included which allows a unique mapping. This could be done by including the device release notes or redacted release notes (see Section 7.2.2).

If a Device Model is added to an existing CPA Certificate, then SECAS requires a confirmation letter from an authorised Test Lab (NCC Group or KPMG or CyTAL) which must be included in the CPL submission (see Section 7.2.4). The Device Model of the CPL submission must be uniquely identified in the confirmation letter (see Section 7.2.2).

In certain cases the SSC may issue letters relating to CPA Certificates or Trial Device Certificates; these letters must be attached to the CPL submission. The Device Model of the CPL submission must be uniquely identified in the confirmation letter (see Section 7.2.2).

7.8 Step Eight: Sending your submission to SECAS

Before sending, please conduct the final checks below to ensure your submission is not rejected. Please check the following:

- Are all necessary Assurance Certificates attached to your submission email?
- Do all details from the Assurance Certificates match the submission(s)?
- Is ZigBee mapping required if details from the ZigBee Certificate(s) do not match the submission(s)?
- Is Test Lab confirmation provided in your submission email if providing a previously used CPA Certificate?
- Have you stated whether your CPA Certificate is set for either Expiry or Renewal, and included the expiry / renewal date set by the NCSC?

- Have you stated whether your Device Trial Certificate details are set and included the expiry date set by the SSC?
- For ESME devices, have you provided confirmation that the DLMS Certificate is for the newly submitted firmware?
- Has the submission been digitally signed with a valid signature if there is a Hash?
- Have you checked that the Hash number is correct?
- Have you checked that you have provided the correct SMETS/CHTS and GBCS combination?

Once you are satisfied that the form has been completed, please submit it along with all the necessary Assurance Certificates and supporting documents (i.e. Release Notes), to SECAS@gemserv.com.

Note that the SEC has changed and there is no longer a requirement for a Supplier or the DCC to endorse a CPL submission. This endorsement had been required if a CPL submission used a new CPA Certificate or added a Device Model to an existing CPA Certificate.

8 How SECAS Validates New Submissions

The CPL will only be updated once a submission has been fully validated and the supporting documentation has been checked by SECAS.

SECAS validates both the submission and the Assurance Certificates to confirm SEC compliance. SECAS will contact you if there are any issues with your submission.

SECAS performs the following steps to validate submissions:

1. Confirms the New Entry Form has been completed correctly and the tab has not been renamed. The validation rules within the workbook itself should ensure correct completion.
2. Validates the digital signature if a Manufacturer Image Hash has been provided. We will check that the digital signature has not expired, has been created by the person who created the image, and is from a trusted Certification Authority.
3. Check each Assurance Certificate against criteria agreed with the relevant Assurance Certification Body.
4. A duplicate check to confirm if the same Device Model already exists on the CPL. If providing multiple submissions, we will also check for duplicates between the submissions.

9 How SEC Parties & the DCC are informed of changes to the CPL

Within **one Working Day** of a valid submission being made to SECAS to add or remove Device Models, SECAS will provide an updated version of the CPL to the DCC (as per Section F2.8), publish the updated CPL version on the SEC website and notify all SEC Parties each time the CPL is updated. To be notified of any CPL changes, SEC Parties can use our online form to be added to our CPL mailing list. CPL submitters who aren't SEC Parties will be included in the notification email for their CPL submissions.

Using the 'CPL - Saveable in CSV' worksheet of the CPL, the DCC can make any modifications to the SMI up to 24 hours from receipt of the updated CPL. Please note, there may be a delay between the publication of the CPL and it being uploaded by the DCC into its Data Service Provider (DSP).

Appendix 1 Why include a Hash?

A Manufacturer Image is a firmware image that a Device can apply to upgrade its firmware, alongside any manufacturer specific data needed. A firmware image is the code which comprises a specific version of firmware.

A firmware Hash is the result of the application of a Hash function to the Manufacturer Image. A Hash function is a repeatable process to create a fixed size and condensed representation of a message using a specific algorithm.

This means that a Manufacturer Image, as defined in SEC Schedule 8: Great British Companion Specification (GBCS), will have a function applied to it and produce a string of letters (A to F) and numbers (0 to 9) of fixed length. A Hash is made up of 32 combinations separated by colons (example below taken from CPL Entry 000001):

13:7E:D5:BC:81:A2:1F:6D:21:87:BC:38:03:81:AE:A7:70:5B:F6:5D:3E:4D:AE:A2:8E:FD:44:11:30:79:D5:E9

It is the responsibility of the Device Manufacturer and the supporting Supplier / the DCC to check that the Hash number is correct before submitting to SECAS.

As the function applied is repeatable, the resultant string should always be the same, provided that the Manufacturer Image has not changed. If the Manufacturer Image has changed, the string of letters and numbers of the Hash will be different.

Devices can apply the specific Hash function themselves. The firmware can be distributed to Devices Over the Air (OTA) and upon receipt of a Manufacturer Image, the Device calculates the Hash. If the Hash it calculates differs from that which is listed on the CPL, it is an indication that the firmware provided to the Device is not what the Supplier intended. Therefore, it will reject any installation commands.

Appendix 2 What is a Digital Signature and how do you get one?

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message or digital document. Application of a digital signature is required to allow SECAS to verify the identity of the sender and the integrity of the message sent as required by SEC Appendix Z section 3. On receipt of a submission that includes a Hash value, SECAS will verify the digital signature as an additional check before updating the CPL.

Submitters must digitally sign each CPL submission that contains a Hash.

Microsoft Excel has the functionality to apply digital signatures. Once you have validated your submission, you will be able to add the digital signature to it using a Certificate from a recognised Certification Authority.

Microsoft's guidance on applying digital signatures to Excel workbooks can be found here.

The submitting organisation can choose the content of the Data Attribute Manufacturer_Image.creator. Typically, the submitting organisation that created the image is used to populate this field.

The Digital Signature must come from a recognised Certification Authority. You must not use a Digital Signature that's internal to your organisation.

The submitter must ensure that the format of the 'identity of the organisation that created the image' is **identical** to that provided when they obtained a digital certificate from their chosen Public Key Infrastructure (PKI) provider. This allows SECAS to verify the authenticity of the digital signature on receipt of a signed Excel file.

Appendix 3 Assurance Certificates Overview

Appendix 3.1 Commercial Product Assurance (CPA) Certificates

The CPA scheme is administered by the UK Government's national technical authority for information assurance, the National Cyber Security Centre (NCSC). The scheme evaluates commercial security, enforcing products and their manufacturers against security and development standards. CPA is open to suppliers of products within the UK, and assessment is carried out by independent approved CPA Test Labs (NCC Group, KPMG or CyTAL).

CPA certification is granted against a specific set of CPA Security Characteristics. These characteristics describe the properties which NCSC expect a good product to exhibit. Testing against these Security Characteristics must be performed at a NCSC approved CPA Test Lab.

Once a Test Lab has finished its analysis of a product, they will send their findings to NCSC who will review the assessment and, if successful, award a Foundation Grade Certificate. It is a copy of this certificate which must be provided alongside your submission form if applicable.

Appendix 3.2 Trial Device Certificate

SMETS2+ Device Models can be added to the CPL using a Trial Device Certificates instead of a CPA Certificate. Device trials have a limited time duration and the total number of Devices which can be used as part of the trial is also limited.

Trial Devices are connected to the live DCC systems and may therefore present some security risks that need to be assessed and mitigated. The SSC will grant a Trial Device Certificate on the condition that the necessary security principles have been applied to the Trial Devices.

At the end of the trial the Trial Device Certificate must be replaced by a CPA Certificate for the Device Model to remain on the CPL, otherwise the status of the Device Model will be set to removed.

The SSC Guidance section on the SECAS website hosts the 'SSC - SSC Guidance on applying for Approval of Trial Devices for Field Trials without CPA Certification v1.1' explaining the process for obtaining a Trial Device Certificate and the application form for a Trial Device Certificate.

For more information about the process for obtaining a Trial Device Certificate please contact SECAS via email at ssc@gemserv.com.

Appendix 3.3 ZigBee Certificates

The ZigBee Certified Product program tests a Device against a Connectivity Standards Alliance (CSA) developed standard. In order to achieve certification, the product must be able to execute all mandatory commands successfully.

Those wishing to achieve ZigBee certification must first become a member of the CSA. Further information on joining can be found here.

Once you have joined the CSA, you must select an Authorised Test Service Provider. These are authorised, independent test laboratories who have been qualified by the CSA as capable of testing ZigBee technology. A list of CSA authorised test service providers can be found here.

Once the test laboratory has completed their analysis, they will provide their findings to the CSA. Once the CSA verifies the findings of the test lab, they will issue a certificate against the Device Model.

Appendix 3.4 DLMS Certificates

Device Language Message Specification Companion Specification for Energy Metering (DLMS COSEM) is a communication standard used by certain Devices. It sets out the rules for data exchange with Electricity SMETS2+ meters. The DLMS User Association is formed of various stakeholders from the energy industry, such as manufacturers, utility providers, etc. They are responsible for the development and maintenance of the standard, as well as developing the conformance test and its associated tools.

The DLMS User Association provides a certification scheme. Testing can either be performed using the DLMS User Association provided Conformance Test Tool, or it can be performed by a third party.

If the firmware on the DLMS Certificate does not match the CPL submission, the Manufacturer must provide written confirmation to confirm that the DLMS Certificate is valid for the new submission.

Appendix 4 Aligning Assurance Certificates with Submission details

To be compliant, Assurance Certificates must identify the Device Model(s) and the relevant Physical Device Type. The CPL lists five Data Attribute fields in the Data Group ‘Device_Model’:

- manufacturer_identifier
- model_identifier
- hardware_version.version
- hardware_version.revision
- firmware_version

These fields follow the notation of the ZigBee Over the Air (OTA) header information defined by the Connectivity Standards Alliance (CSA and in GBCS. In case a field contains several bytes, these must be separated by a colon “:” in the ‘CPL – New Entry’ form.

It must be possible to map these CPL Device Model fields between the Assurance Certificate and the CPL submission.

If the Assurance Certificate uses the same format as written in the submission, the values will be identical. However, if the Device Model is listed on the Assurance Certificate in a Plain English format (e.g. Version 1.2.5.6 or v1.0), instead of the CPL format (e.g. 01:02:05:06 or 00:00:10:00), it cannot be established whether the certificate relates to the submission.

Appendix 4.1 Mapping Assurance Certificate using Release Notes

If the Device Model details on the Assurance Certificate are listed in a format different from the ZigBee OTA specification, you must clearly explain how the CPL submissions map onto the Assurance Certificate.

You are also encouraged to include a clear written statement confirming that no changes have occurred that would require updates to Assurance certificates.

The Release Notes or equivalent evidence will not be made publicly available and will be retained for auditing purposes only.

Appendix 4.2 ZigBee Assurance Certificate Alignment

You should ensure that the Manufacturer & Model Identification, Hardware Versions and Firmware Version fields of the ZigBee Certificate fields contain the format required for CPL submissions and descriptive alphanumeric text. The alphanumeric text should accurately reflect the Device details used in the market for product identification.

This combination of alphanumeric text and hexadecimal data allows the unique identification of the Device Model and the Manufacturer. You are responsible for the correct hexadecimal data and the alphanumeric text description when applying for ZigBee certification and subsequent CPL submissions.

If the relevant fields are not identical between the submission and Zigbee Certificate, we would require supporting evidence (either release notes or a confirmation email) to confirm that the certificate relates to the submission.

Appendix 4.3 Can I reuse a ZigBee Certificate?

Some updates to Device Firmware do not affect ZigBee certification. Subject to the manufacturer undertaking appropriate checks to confirm that re-testing is not required, along with supporting evidence to show that an existing ZigBee certificate is still valid, the same ZigBee Certificate can be used for multiple CPL entries.

When reusing the ZigBee Certificate, the Device related fields of the certificate no longer match the details of the CPL submission. To ensure that a CPL submission is valid, additional information is required from the manufacturer to clearly identify the mapping between the Device details in the CPL Submission form and the ZigBee certificate.

The manufacturer must provide supporting evidence, which may take the form of the full, or an extract from, the related Release Notes of the Device. The supporting evidence must clearly identify the ZigBee firmware module used.

Appendix 4.4 CPA Assurance Certificate Alignment

The CPA Certificate should contain the Manufacturer & Model Identification, Hardware Versions and Firmware Version fields in the format required for CPL submissions; it may contain descriptive alphanumeric text.

This combination of alphanumeric text and hexadecimal data allows the unique identification of the Device Model and the Manufacturer. You are responsible for the correct hexadecimal data and the alphanumeric text description when applying for CPA certification and subsequent CPL submissions.

If the relevant fields are not identical between the submission and the CPA Certificate, we would require supporting evidence (either release notes or a confirmation email) to confirm that the certificate relates to the submission.

Appendix 4.5 Can I reuse a CPA Certificate?

As long as the changes to the new Device Model do not significantly impact the security functions (as set out in the CPA Assurance Maintenance Plan) one or more Devices can be added to an existing CPA Certificate. The manufacturer must undertake appropriate checks to confirm that re-testing is not required, and SECAS requires a confirmation letter from an authorised Test Lab (NCC Group or KPMG or CyTAL) to confirm that there are no security impacts.

The confirmation letter of the authorised Test Lab must clearly identify the mapping between the Device details in the CPL Submission form, the original CPA certificate, and the confirmation letter itself.

Appendix 4.6 DLMS Assurance Certificate Alignment

The DLMS Certificate should contain the Manufacturer & Model Identification, Hardware Versions and Firmware Version fields in the format required for CPL submissions; it may contain descriptive alphanumeric text.

This combination of alphanumeric text and hexadecimal data allows the unique identification of the Device Model and the Manufacturer. You are responsible for the correct hexadecimal data and the alphanumeric text description when applying for DLMS certification and subsequent CPL submissions.

If the relevant fields are not identical between the submission and the DLMS Certificate, we would require supporting evidence (either release notes or a confirmation email) to confirm that the certificate relates to the submission.

Appendix 4.7 Can I reuse a DLMS Certificate?

Some updates to Device Firmware or hardware do not affect DLMS certification. Subject to the manufacturer undertaking appropriate checks to confirm that re-testing is not required, along with supporting evidence to show that an existing DLMS certificate is still valid, the same DLMS Certificate can be used for multiple CPL entries.

When reusing the DLMS Certificate, the Device related fields of the certificate no longer match the details of the CPL submission. To ensure that a CPL submission is valid, additional information is required from the manufacturer to clearly identify the mapping between the Device details in the CPL submission form and the DLMS Certificate.

The manufacturer must provide supporting evidence, which may take the form of the full, or an extract from, the related Release Notes of the Device.

Appendix 5 Expiry of CPA Certificates and the new Lifetime Certificate Risk Review Process

On 1 August 2022, MP209 ‘Lifetime CPA Certificates’ was implemented. This Modification was implemented to reflect the new CPA Lifetime Certificates and the CPA Certificate Risk Review process that applies to expiring CPA Certificates and those requiring periodic renewal.

The formal documentation for the enduring process is still being finalised. SECAS will update these Guidance Notes on an ad-hoc basis as the new process matures and becomes more familiar.

The NCSC provides guidance on CPA Certificates here.

Appendix 5.1 Pilot CPA Certificate Re-Certifications

These initial re-certifications will be treated as pilots for this new process and the arrangements will differ from the enduring process which is detailed below (subject to updates).

For pilot re-certifications, the below process will need to be followed:

1. Before the current CPA Certificate is due to expire, the NCSC will provide the Device Manufacturer and the SSC with a new CPA Certificate and an accompanying letter which will specify by which date the Risk Review must be completed.
2. Once these have been granted to the Device Manufacturer and the new Lifetime CPA Certificate number appears on the NCSC webpage, they should email the SECAS Helpdesk, attaching the new CPA Certificate and the accompanying letter from the NCSC, asking SECAS to update the relevant rows of the CPL that contained the expiring CPA Certificate.
3. SECAS will manually amend these rows; adding an [R] in front of the new certificate number and adding the new renewal date. SECAS will then release a new version of the CPL on the SEC website.

Before the deadline set out in the NCSC letter, the Device Manufacturer will be required to complete a Risk Review on the Devices with CPL entries linked to the CPA Certificate following the process set out in the NCSC Risk Review Process. If the NCSC considers that any security risks identified are within risk tolerance, the NCSC will then submit a new Lifetime CPA Certificate to the Manufacturer and the SSC. The SSC will then review the risk advice from the NCSC and confirm the renewal date.

Appendix 5.2 Enduring Lifetime CPA Certificate Process

If a completely new Device is submitted for CPA Certification and is successful, the NCSC will issue a Lifetime CPA Certificate which may be submitted to SECAS in line with the process set out below in the section ‘Process for CPL submissions with Lifetime CPA Certificates’.

In the case of a Device already on the CPL which is approaching expiry, once the Lifetime CPA Certificate Process has matured and becomes BAU (date to be confirmed), the below process will need to be completed:

1. No more than 12 months and no less than six months before the expiry date, the Manufacturer must initiate a Risk Review by having a Risk Review Questionnaire accepted by the NCSC.
2. The Risk Review has three possible outcomes:
   - **a)** The Device may be found to be fully compliant with the CPA Security Characteristics;
   - **b)** The Device may be found to be partially compliant with the CPA Security Characteristics but is considered to be within risk tolerance; or
   - **c)** The Device is found to be non-compliant with the CPA Security Characteristics.
3. For the scenario in 2(a) above, on completion of the Risk Review, the NCSC will provide the Lifetime CPA Certificate and an accompanying letter to the SSC and the Device Manufacturer requiring a further Risk Review in six years’ time. The Manufacturer should then email the SECAS Helpdesk, attaching the new CPA Certificate, asking SECAS to update the relevant rows of the CPL that contained the expiring CPA Certificate.

4. For the scenario in 2(b) above, the NCSC will provide a Lifetime CPA Certificate and an accompanying letter to the SSC and the Manufacturer on completion of the Risk Review. The SSC will consider the risk advice from the NCSC and any other relevant prevailing factors and will decide on a renewal date and will provide this in a letter to the Device Manufacturer and SECAS.

The Manufacturer should then email the SECAS Helpdesk, attaching the new CPA Certificate and the accompanying letter from the SSC, asking SECAS to update the relevant rows of the CPL that contained the expiring CPA Certificate.

For both 2(a) and 2(b), SECAS will manually amend the relevant rows; adding an [R] in front of the new certificate number and adding the new renewal date. SECAS will then release a new version of the CPL on the SEC website.

For the scenario in 2(c) above, the NCSC will provide a letter to the SSC and the Manufacturer to confirm that CPA Certification has been withdrawn. The SSC will then consider the risk advice from the NCSC and follow the process in SEC Appendix Z Section Six to determine whether the Device should remain on the CPL for a period.

Appendix 5.3 Process for CPL submissions with Expiring CPA Certificates

If the CPA Certificate associated with the new CPL submission contains an expiry date, Device Manufacturers should provide CPL submissions as normal to SECAS using the latest version of the CPL - New Entry form.

The only difference is that Device Manufacturers will need to add an [E] and a space in front of the CPA Certificate number to mark that the certificate will be expiring. An example of a valid submission can be found here: **[E] 1234567891-2345**. SECAS will then add the new submissions to the CPL and publish the new version.

Appendix 5.4 Process for CPL submissions with Lifetime CPA Certificates

If the Device Manufacturer wants to add new CPL submissions to granted Lifetime CPA Certificates, they should provide the new submissions to SECAS using the latest version of the CPL - New Entry form.

Device Manufacturers will need to add an [R] and a space in front of the CPA Certificate number to mark that the certificate will be up for renewal. An example of a valid submission can be found here: **[R] NCSC-1234567891-2345**.

Device Manufacturers will also need to provide the Lifetime CPA Certificate and the renewal date confirmation letter from the SSC.

SECAS will then add the new submissions to the CPL and publish the new version.

SECAS will notify the relevant submitting Manufactures and Suppliers / the DCC by email **12 months, six months** and **one month** in advance of the CPA Certificate renewal / expiry date.

If a CPL entry's CPA certificate expires or is withdrawn by the NCSC, then the SSC shall determine if the Device should be removed from the CPL. The SSC may determine that either a remedial plan is required, or immediate removal is necessary. If the SSC decides a remedial plan is sufficient, they have the power to overturn their decision and remove the entry at any time.

Appendix 6 Firmware Information Repository (FIR)

Appendix 6.1 What is the FIR and when is it required?

Smart Meters for gas and electricity (GSME and ESME) may require firmware upgrades. The Responsible Supplier has to carry out these firmware upgrades in accordance with the obligations set out in the SEC, and the Ofgem Standard Licence Conditions (SLCs).

In the case of a Change of Supplier (CoS) event, the Gaining Supplier may not have enough information about the gained Smart Meter to fulfil their regulatory obligations. The Supplier must obtain the firmware upgrade packages, and possibly additional technical information related to the device firmware, to carry out the firmware upgrade. These are typically only available from the Device Manufacturer.

The gaining Supplier may not have the contact details of the Device Manufacturer. The FIR (the latest version can be downloaded here) provides this information and enables the Supplier to enquire with the Device Manufacturer about firmware upgrade packages and request further information.

SEC Sections F2.14 - F2.17 specify the obligations with regards to the FIR. In summary, the FIR contains the following mandatory fields:

- Unique identifier of a CPL record;
- Manufacturer contact details; including an email address, telephone number and business address; and
- Release Notes where the content is at the discretion of the Manufacturer.

The FIR will be updated alongside the CPL when a new ESME / GSME firmware is submitted. The Device Manufacturer submitting ESME / GSME Device details to be added to the CPL needs to supply the FIR details.

Appendix 6.2 Who can access the FIR and where to find it?

Below is a sample view of the FIR with a single entry:The five fields on the FIR are populated by SECAS using data from the CPL Submission form:

This document is classified as **Green.** Information can be shared with other SEC Parties and SMIP stakeholders at large, but not published (including publication online).

The following table provides information to allow a gaining Supplier to easily identify which Manufacturer to contact, with regards to the latest firmware on a device following an update to the CPL. All entries to the Firmware Information Repository have been vetted by a SECAS security expert prior to publication.

Before carrying out any Device upgrades, the relevant Release Notes must be referred to. These are available from the Meter Asset Provider or Manufacturer as appropriate. Manufacturers and Suppliers will not be held responsible for any misuse or incorrect information contained within the Firmware Information Repository.

CPL Firmware Information Repository

CPL Reference	Manufacturer	Contact Details	Manufacturer Firmware Description / Information	Firmware Upgrade Path
000633	Example Name	36, Example Street Example City, 1234 ABC UK 0123456789	General release for SMETS2	000626; 000630

Figure 4: FIR Entry

- **CPL Reference** - Assigned by SECAS once a CPL submission has been accepted and added to the CPL;
- **Manufacturer** - This corresponds to a field in the CPL Submission form;

Figure 5: FIR Entry

- **Contact Details** - The CPL Submission form contains several items which all relate to the business address and additional contact information. These fields are part of the data group 'Manufacturer Contact FIR';
- **Manufacturer Firmware Description / Information** - The CPL Submission form contains a plain text field named FIR Release Notes where the Submitter enters **non-confidential** information about the firmware release and / or a URL. The URL must be functional; and
- **Firmware Upgrade Path** – The CPL Submission form contains a field which lists the Device Model Entry numbers already present on the CPL which can be upgraded directly (no interim step needed) to the Device Model in the new CPL submission.

SECAS will extract the data from the CPL Submission form and add it to the FIR. The new version of the FIR is then made available to all logged in SEC Parties on the SEC website here.

It is recognised that full release notes for firmware upgrades may contain commercial and confidential items which are not suitable for publication, even when a login is required to access it.

For this reason, the FIR Release Notes **must only contain public information**, not commercial or confidential information; the actual content is at the Device Manufacturers' discretion.

In case there are concerns with FIR Release Notes in terms of commercial or confidential information, a SECAS Security Expert will check them prior to releasing a new version of the FIR.

Possible content for the FIR Release Notes field could be:

- General Release;
- General Release for use with version [Technical Specification version number]; and
- Commercial Release with bespoke functionality.

It is also possible to include a URL pointing to the manufacturer's website with access to public release notes or allowing the user to register for access. As part of the submission process, SECAS verifies that the URL is working.

Appendix 7 Device ZigBee Information Repository (DZIR)

Appendix 7.1 What is the DZIR and when is it required?

Smart Metering Devices use ZigBee technology for communications in the Home Area Network (HAN), this requires dedicated hardware and firmware for the radio access and the handling of ZigBee messages between the Devices.

The ZigBee solution is offered by ZigBee vendors providing chipsets and specific firmware operating on these chipsets; the firmware is also known as the Zigbee stack. Device Manufacturers integrate the ZigBee solution – chipset and firmware – in their Device, e.g. an Electricity Meter, where the Device firmware interacts with the ZigBee stack.

The information about the ZigBee vendor and the ZigBee stack version used in the Device is collected as part of the CPL submission and then entered into the 'Device ZigBee Information Repository'. This allows a quick identification of impacted Devices in case of issues with a particular ZigBee solution.

SEC Sections F2.33 - F2.38 specify the obligations with regards to the DZIR. In summary, the DZIR contains the following mandatory fields:

- Unique identifier of a CPL record;
- ZigBee Vendor; and
- ZigBee Stack version.

The DZIR will be updated alongside the CPL when a new Device Model is submitted. The Device Manufacturer submitting the Device details to be added to the CPL needs to supply the DZIR details.

Appendix 7.2 Who can access the DZIR and where to find it?

Below is a sample view of the DZIR with three sample entries:

This document is classified as **RED**. It contains non-disclosable information and is restricted to the Security Sub-Committee members (including alternates). Participants must not disseminate the information outside of the governance group. **RED** information may only be discussed during a meeting where all participants present have signed a declaration form, stating their acceptance to abide by these terms. **RED** information should not be discussed with anyone who is not a member of the governance group.

The following table provides information about the ZigBee Stack Vendor and the ZigBee Stack Version used by the Device Model. Historic Device Models without this information are marked accordingly.

Device ZigBee Information Repository

CPL Reference	ZigBee Stack Vendor	ZigBee Stack Version
000635	Silicon Labs	1.2.A.B
000636	Silicon Labs	3.4.11.12
000637	NXP	R22

Figure 6: DZIR Entry

The three fields on the DZIR are populated by SECAS using data from the CPL Submission form:

- **CPL Reference** - Assigned by SECAS once a CPL submission has been accepted and added to the CPL;
- **ZigBee Stack Vendor** - This corresponds to a field in the CPL Submission form; and
- **ZigBee Stack Version** - This corresponds to a field in the CPL Submission form.

SECAS will extract the data from the CPL Submission form and add it to the DZIR. The new version of the DZIR is then made available exclusively to the SSC.

Appendix 8 Device Level Versioning

The September 2020 Release of the SEC introduced Device level versioning for SMETS2+ Devices. The SMETS documents are now referred to by their release date and the version numbering is applied to the Device specific sections of the SMETS instead of the entire document. This change has also been applied to earlier versions of SMETS.

For SMETS2+ Devices, the CPL continues to use the term “SMETS” followed by a version number. However, this version number now refers to the Device specific subsection of the SMETS.

Device Level Versioning and valid SMETS/CHTS and GBCS combinations for all devices can be found in SEC Schedule 11 - Technical Specification Applicability Tables (TSAT).

It is the responsibility of Device Manufacturers to check they have used the correct SMETS/CHTS and GBCS combinations when submitting new device models.

The combination of 'Device Type', 'SMETS/CHTS Version' and 'GBCS Version' is verified when executing the 'Validate New Entry' macro. A warning message is displayed if an invalid Device level version combination is detected.

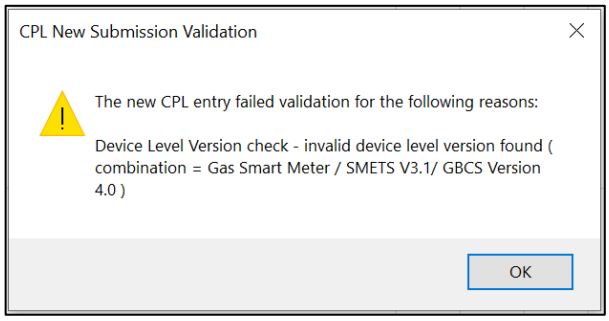

Figure 7: Error message – failed Device Level Version check

In this case, the selection must be changed to the permitted values. The 'Validate New Entry' macro should be executed again to verify that the Device level version combination is correct.

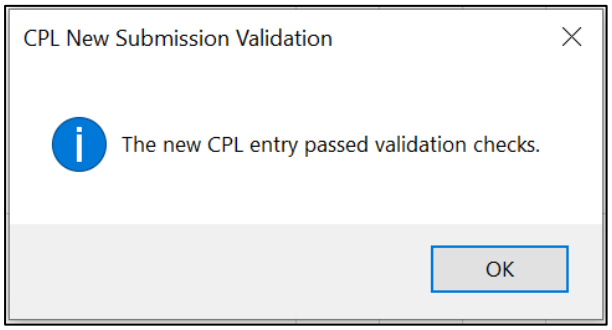

Figure 8: Successful CPL submission check

Appendix 9 Glossary

Acronym	Meaning
CHTS	Communications Hub Technical Specifications
CoS	Change of Supplier
CPA	Commercial Product Assurance
CPL	Central Products List
CSA	Connectivity Standards Alliance
CSV	Comma Separated Value
DCC	Data Communications Company
DMC	Device Model Combination
DLMS	Device Language Message Specification
DLMS/COSEM	Device Language Message Specification Companion Specification for Energy Metering
DPL	Deployed Products List
DSP	Data Service Provider
DZIR	Device Zigbee Information Repository
EPCL	Eligible Products Combination List
ESME	Electricity Smart Metering Equipment
FIR	Firmware Information Repository
GHz	Gigahertz
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
IKI	Infrastructure Key Infrastructure
MP	Modification Proposal
NCSC	National Cyber Security Centre
OTA	Over the Air
PKI	Public Key Infrastructure
PPCL	Pending Products Combination List
SAPC	Standalone Auxiliary Proportional Controller
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SLC	Standard Licence Condition
SMETS1	Smart Meter Equipment Technical Specification Version 1
SMETS2+	Smart Meter Equipment Technical Specification Version 2
SMI	Smart Metering Inventory
SSC	Security Sub Committee
TSAT	Technical Specification Applicability Tables
URL	Uniform Resource Locator
ZSE	ZigBee Smart Energy