SECAS Guidance Document: Central Products List (CPL)

Contents

1. 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 guidance covers:

- How to submit a product for inclusion on the CPL, and what information and documentation is required to support it;
- How SECAS validates and adds submissions;
- 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 SEC, namely SEC Section F2, and SEC Appendix Z - CPL Requirements Document.

2. 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.

3. 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 should be listed on the CPL first.

The SMI is an electronic database that records whether a Device can communicate via the DCC.

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

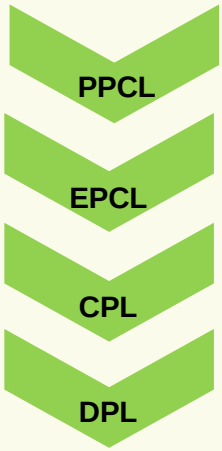
There are four tabs on the CPL:

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 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.

4. SMETS1 CPL Submission Procedure

4.1. Standard SMETS1 CPL Submission Procedure (for the DCC only)

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



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).

BEIS decides which DMCs are **eligible** for enrolment into the DCC and these are added to the SMETS1 Eligible Products Combination List.

Once SECAS has received all the required information as per SEC Appendix Z, SMETS1 submissions can be added to the Central Products List **(CPL)**.

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.

4.2. 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 4.1.

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 ECPL, 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.

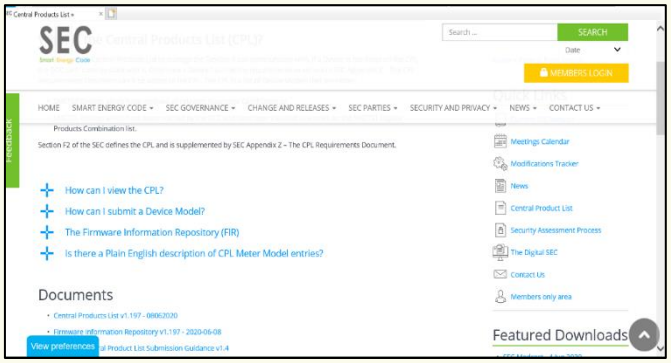
The SSC will review whether an urgent material security vulnerability exists before the Device Model can be added to the CPL and communicate the result of this review to the Supplier and SECAS.

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.

5. 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.



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 in Step 8: Validating your submission entries.

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:

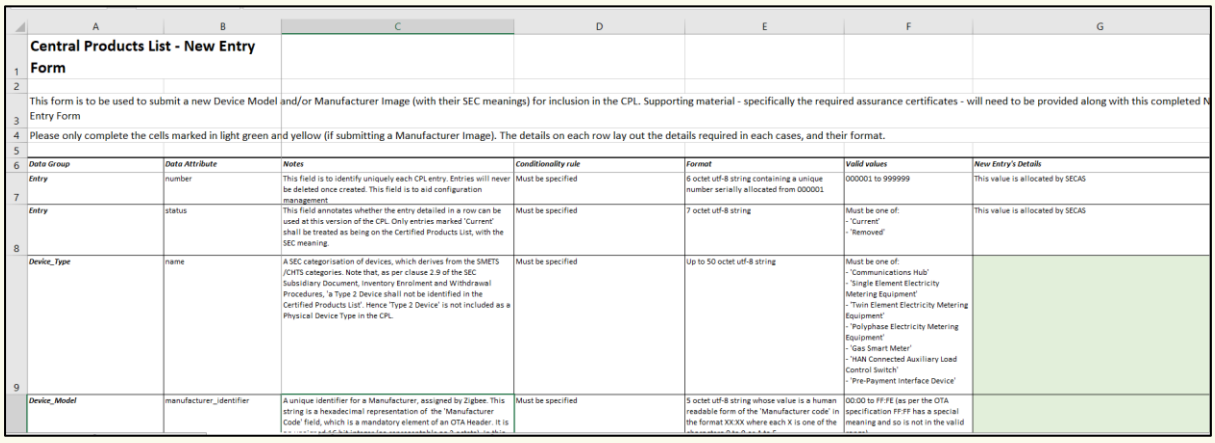
- Change the CPL file name (e.g. to reflect your submission);
- Remove the 'Version Control' and 'CPL - saveable in CSV' worksheets (but **not the 'CPL - New Entry' worksheet**); and
- Add further worksheets.

Step two: Enter Device Model details

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

Figure 2: New Entry Worksheet Location

2. Complete the relevant Device Model details in Column G. **Please note**, the yellow cells in rows 24 and 25) only need to be filled out for submissions which include a **Hash; please add ZigBee Band information in row 26.** The FIR information, rows 30 to 39, only need to be included for **ESME / GSME devices**.



	A	B	C	D	E	F	G
1	**Central Products List - New Entry Form**						
2							
3	This form is to be used to submit a new Device Model and/or Manufacturer Image (with their SEC meanings) for inclusion in the CPL. Supporting material - specifically the required assurance certificates - will need to be provided along with this completed N Entry Form						
4	Please only complete the cells marked in light green and yellow (if submitting a Manufacturer Image). The details on each row lay out the details required in each cases, and their format.						
5							
6	***Data Group***	***Data Attribute***	***Notes***	***Conditionality rule***	***Format***	***Valid values***	***New Entry's Details***
7	*Entry*	number	This field is to identify uniquely each CPL entry. Entries will never be deleted once created. This field is to aid configuration management	Must be specified	6 octet utf-8 string containing a unique number serially allocated from 000001	000001 to 999999	This value is allocated by SECAS
8	*Entry*	status	This field annotates whether the entry detailed in a row can be used at this version of the CPL. Only entries marked 'Current' shall be treated as being on the Certified Products List, with the SEC meaning.	Must be specified	7 octet utf-8 string	Must be one of: - 'Current' - 'Removed'	This value is allocated by SECAS
9	*Device_Type*	name	A SEC categorisation of devices, which derives from the SMETS /CHTS categories. Note that, as per clause 2.9 of the SEC Subsidiary Document, Inventory Enrolment and Withdrawal Procedures, 'a Type 2 Device shall not be identified in the Certified Products List'. Hence 'Type 2 Device' is not included as a Physical Device Type in the CPL.	Must be specified	Up to 50 octet utf-8 string	Must be one of: - 'Communications Hub' - 'Single Element Electricity Metering Equipment' - 'Twin Element Electricity Metering Equipment' - 'Polyphase Electricity Metering Equipment' - 'Gas Smart Meter' - 'HAN Connected Auxiliary Load Control Switch' - 'Pre-Payment Interface Device'	
	Device_Model	manufacturer_identifier	A unique identifier for a Manufacturer, assigned by Zigbee. This string is a hexadecimal representation of the 'Manufacturer Code' field, which is a mandatory element of an OTA Header. It is	Must be specified	5 octet utf-8 string whose value is a human readable form of the 'Manufacturer code' in the format XX:XX where each X is one of the	00:00 to FF:FE (as per the OTA specification FF:FF has a special meaning and so is not in the valid	

Figure 3: New Entry - Required Fields

You must **only** add details to the fields that you are required to complete within Column G in Figure 3 above. The fields that need completing are dependent on the type of Device being submitted. Table 1 below lists all fields, as specified in column A of the submission form 'Data Group', specifying which of these need to be filled depending on the Device type you are submitting.

Data Attribute	Devices Applicable
Device Type	All Devices: Communications Hubs, Single Element Electricity Metering Equipment, Twin Element Electricity Metering Equipment, Polyphase Electricity Metering Equipment, Gas Smart Meter, Pre-Payment Interface Device and HAN Connected Auxiliary Load Control Switch.
Device Model (Covers 5 consecutive fields)	All Devices.
SMETS/CHTS Version	All Devices. **SMETS1 Devices** must be SMETS V1.2. For **SMETS2+ Devices**, include the relevant version of SMETS or CHTS (see note on Device level versioning below this table).
GBCS Version	All Devices. **SMETS1 Devices** must be GBCS Version 0.0. For **SMETS2+ Device Models**, include the relevant version of GBCS.
CPA Certificate (Covers 3 consecutive fields)	All SMETS2+ devices **except** Pre-Payment Interface Devices.
DLMS Certificate (Covers 2 consecutive fields)	SMETS2+ Electricity Metering Equipment.
ZSE Certificate (Covers 2 consecutive fields)	All SMETS2+ Devices.
Manufacturer Image (Covers 3 consecutive fields)	Only if including a **Hash**. SMETS2+ device submitters are encouraged to provide their **Zigbee Band information**.
Contact CPA (Covers 3 consecutive fields)	All SMETS2+ Devices **except** Pre-Payment Interface Devices.
Manufacturer Contact FIR (Covers 9 consecutive fields)	All SMETS1 and SMETS2+ ESME and GSME Devices.
FIR Release Notes	All SMETS1 and SMETS2+ ESME and GSME Devices.

Table 1: Submission form field applicability

The workbook provides guidance on how to correctly complete the form and includes a reference source for all information.

The September 2020 SEC Release introduced Device level versioning 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. See 'Device Level Versioning' of this guide for further details.

Please note that the SMETS2 November 2020 Release introduced a new Device type: **Standalone Auxiliary Proportional Controller** (SAPC). Any CPL submission for a SAPC Device must select '**Single Element Electricity Metering Equipment**' in the Device Type row.

Step three: Add the Manufacturer Image Hash (if applicable) and ZigBee Bands

You will see three yellow highlighted fields in the submission form related to the Manufacturer Image Hash. If a SEC Party or the DCC wants SECAS to associate the Hash of a Manufacturer Image with a Device Model, you must provide the Hash and the identity of the person who created the Manufacturer Image.

Please note: Submitters must digitally sign each CPL submission that contains a Hash (Step four).

If you are unsure what a Manufacturer Image is, or why you may need to include a Hash, please go to Section 11: Why include a Hash? of this guide.

For all SMETS2+ submissions, you are encouraged to include the ZigBee band(s) supported by the Device in the **'Manufacturer_image descriptor' field** by entering one of the choices below:

- Single Band (2.4 GHz);
- Single Band (Sub-GHz); or
- Dual Band.

Step four: 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. The submission must be digitally signed by the person who created the Manufacturer Image.

The signing of Excel spreadsheets is explained on Microsoft's website. To read more about applying a digital signature, please see Section 12: 'What is a Digital Signature and how do you get one?' of this guide.

Step five: Add the FIR Details

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 the following SMETS1 and SMETS2+ Metering Devices:

- Single Element Electricity Metering Equipment
- Twin Element Electricity Metering Equipment
- Polyphase Electricity Metering Equipment
- Gas Smart Meter

The final 10 rows (rows 30 to 39) on the CPL - New Entry worksheet is where the FIR information must be provided. SECAS will then extract this information and add it to the FIR spreadsheet.

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

For more information about the FIR, please see Section 13: 'Firmware Information Repository' of this guide.

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 2 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 2: 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 Section 14: 'Assurance Certificates' of this guide.

6. Adding Device Models to CPA Certificates

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).

To comply with the SEC when submitting a Device using an existing CPA certificate, prior to acceptance, you must provide SECAS with a supporting confirmation email from:

a. The **DCC** for Communication Hubs; or
b. A **Supplier SEC Party** for all other Device Models (excluding PPMIDs). All Supplier SEC Parties can be found in the SEC Parties List.

Additionally, if adding a new Device to a previously used CPA Certificate, SECAS would require a confirmation letter from an authorised Test Lab (NCC Group or KPMG or CyTAL) to confirm that there are no security impacts.

7. Aligning ZigBee Certificates with Submission details

To be compliant, Zigbee Assurance Certificates must identify the Device Model(s) and the relevant Physical Device Type. The CPL lists five Device_Model data fields:

1. Device_Model – manufacturer identifier
2. Device_Model – model identifier
3. Device_Model – hardware version version
4. Device_Model – hardware version revision
5. Device_Model – 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 ":".

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

If the ZigBee Certificate uses the same format as written in the submission, the values will be identical. However, if the Device Model is listed on the ZigBee 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.

Therefore, 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 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.

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.

The Release Notes must clearly explain how the CPL submissions map onto the Zigbee Certificate.

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

The Release Notes or equivalent evidence will not be made publicly available and will be retained for auditing purposes only. More information on ZigBee mapping can be found here.

8. 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 National Cyber Security Centre (NCSC) provides guidance on CPA Certificates here.

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 Security Sub-Committee (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.

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 adding 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 rows; adding an **[R]** in front of the new CPA 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.

Process for adding 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.

Process for adding 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 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 supporting 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.

Step seven: 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.

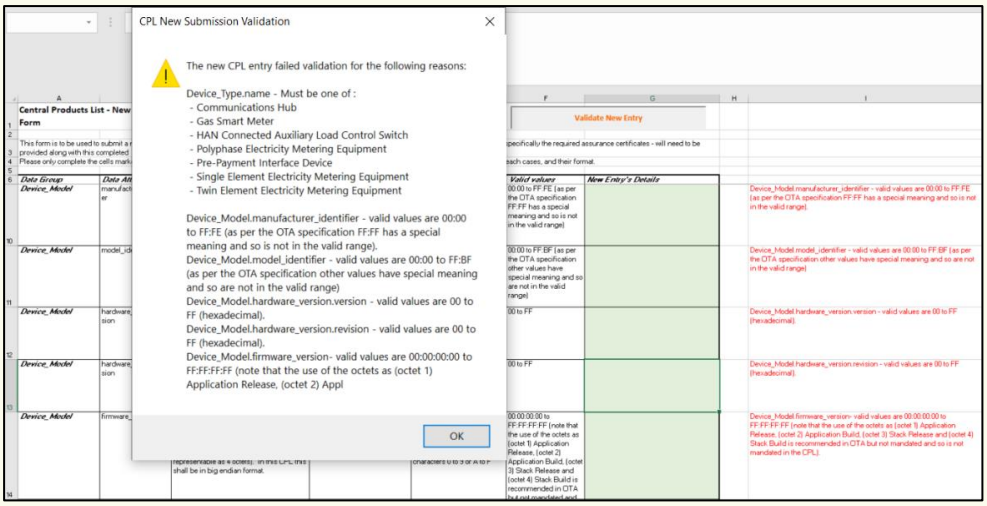
- You must ensure you save it as a ***.xlms (Excel Macro-enabled Workbook) file** in order for the ‘Validate New Entry’ macro to work.
- The name of the “CPL - New Entry” worksheet must not be changed.

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

Step eight: Validating your submission entries

The CPL - New Entry worksheet contains a built-in macro which validates the entry details. This ‘**Validate New Entry**’ macro is executed by clicking the soft button as shown here:

Any errors 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.



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.

Once validation has been successful, you will be able to digitally sign the spreadsheet if including a Hash.

Step nine: 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 Supplier / DCC and 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?
- 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?
- If using a new CPA Certificate and including a Hash, do you have a supporting email from a Supplier / the DCC?
- 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.

9. 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.

10. 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.

Using the CPL - Saveable in CSV worksheet of the CPL (explained on page 2 of this guide), the DCC can make any modifications to the Smart Metering Inventory (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).

Additional Information

This section supports the earlier sections in this guide to further aid your understanding.

Manufacturer Image: 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.

11. Why include a Hash?

A firmware Hash is the result of the application of a Hash function. 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. 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.

12. 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.

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

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.

On receipt of a submission that includes a Hash value, SECAS will verify the digital signature as an additional check before updating the CPL.

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

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.

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

The submitting organisation can choose the format of the **Manufacturer Image – creator**. Typically, the submitting organisation that created the image is used to populate this field.

13. Firmware Information Repository (FIR)

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.

Who can access the FIR and where to find it?

Below is a sample view of the FIR with a single-entry:

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.

CPL Firmware Information Repository

CPL Reference	Manufacturer	Contact Details	Manufacturer Firmware Description / Information
1234	Example Manufacturer	123 Example Street Example City 1234 ABC	General Release for use with SMETS2

Figure 4: FIR Entry

The four fields on the FIR 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;
- **Manufacturer** - This corresponds to a field in the CPL Submission form;

- **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'; and
- **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.

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 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.

Assurance Certificates

14. 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.

15. 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.

16. 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.

From 2 February 2022, the option to select Conformance Test Tool (CTT) 3.0 was removed from the CPL spreadsheet. The only possible options are now: CTT 3.1, CTT 4.0, CTT 4.1 or CTT 4.2.

17. Device Level Versioning

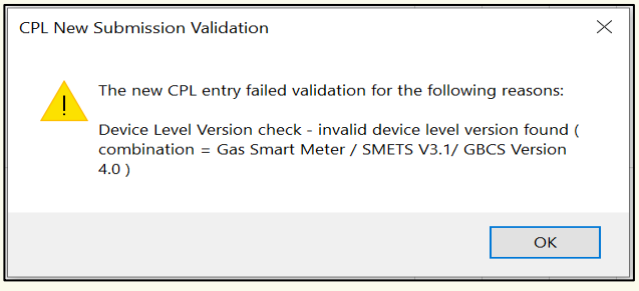
The September 2020 Release of the SEC introduced Device level versioning for SMETS2+ Devices. The SMETS documents are now referred to by their release date and the version numbering is applied to the Device specific sections of the SMETS instead of the entire document. This change has also been applied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

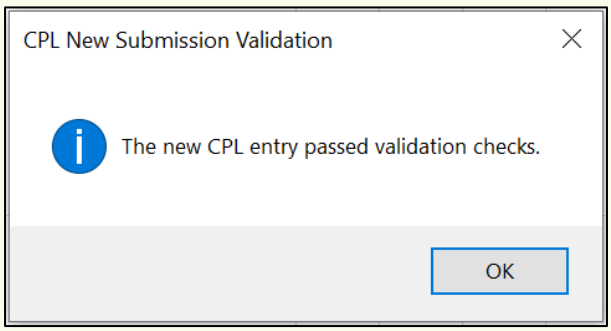
Device Level Versioning and valid SMETS/CHTS and GBCS combinations for all devices can be found in SEC Schedule 11 - Technical Specification Applicability Tables (TSAT).

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.



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.



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