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

Certified Products List

Submission Guidance

Version 1.4 Status: Final

Date: 28 February 2019

Administered by

Gemserv

Change History

Version Number	Status	Date of Issue	Reason for Change
0.1	For Review	27/04/2016	Initial draft for SECAS internal review
0.2	For Review	09/05/2016	Updated following initial feedback.
1.0	Final	12/05/2016	Version for Publication
1.1	Final	09/10/2017	• General updates following internal review; and • Additional section added on CPL submission forms and alignment with Assurance Certificates added for clarity.
1.2	Final	12/12/2017	Updated CPL submission forms and alignment with Assurance Certificates section to include additional mapping evidence.
1.3	Final	20/03/2018	Added section on mapping the ZigBee manufacturer codes with the plain English device names to the relevant areas from the CPL.
1.4	Final	28/02/2019	Added section on Firmware Information Repository (FIR)

Contents

1. Purpose of the Certified Products List (CPL)

The Technical Specifications[1] set out which Physical Device Types are required to obtain which Assurance Certificates from one or more Assurance Certification Bodies. These Assurance Certificates are intended to prove a device meets a minimum standard in relation to its security and use of communication protocols such that the DCC is permitted to communicate with it. SEC Section F2.1 requires that the SEC Panel establish and maintain a listing of all Device Models which have received their required Assurance Certificates.

The CPL performs two main functions:

- acting as a listing for SEC Parties to identify which Device Models have received their required Assurance Certificates; and
- being used by the DCC to manage the Smart Metering Inventory[2].

2. Structure of this document

This guidance is intended for any party who would be adding information to the CPL and is seeking to understand the CPL submission process. It details:

- how to submit a product for inclusion on the CPL, and what information and documentation is required to support a new submission:
    - Section 3 describes the process for adding a product without a Manufacturer Image Hash; and
    - Section 4 describes the process for adding a Manufacturer Image Hash;
- the validation SECAS will perform upon receipt of a new submission – this is described in Section 4;
- information on what is a hash and why it is needed – Section 6 provides the detail;
- information on how to obtain and apply a digital signature to your submission – see Section 8; and
- how devices are suspended from the CPL – see Section 9.

Appendix A provides the necessary definitions and information on the required assurance processes. The relationship between the CPL and Smart Metering Inventory is also described there.

This guidance is based upon the latest version of the SEC and the SEC Subsidiary Document, Appendix Z - CPL Requirements Document.

[1] Communications Hubs Technical Specification and Smart Metering Equipment Technical Specification

[2] Please see Section 3 of Appendix A for more information on the SMI

3. Submission Procedure for Products Without a Manufacturer Image Hash

The submission procedure varies slightly, dependent on whether a Manufacturer Image Hash is included as part of submission. This section describes the process for submitting products without a Manufacturer Image Hash. Please see Section 4 of this guidance for information on how to add a product including a Manufacturer Image Hash and on adding a Manufacturer Image Hash to an existing CPL listing.

Submission Procedure

1) Download the latest CPL workbook from the SEC Website.

   The CPL page can be found here.

   The latest version of the CPL will be available for download under the Documents section of the page.

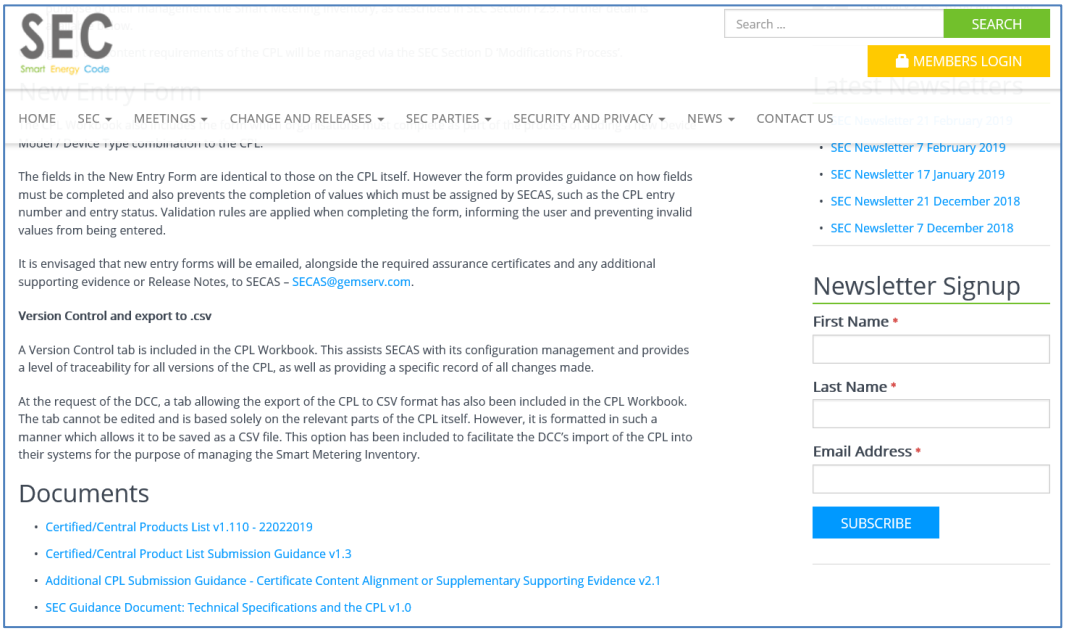


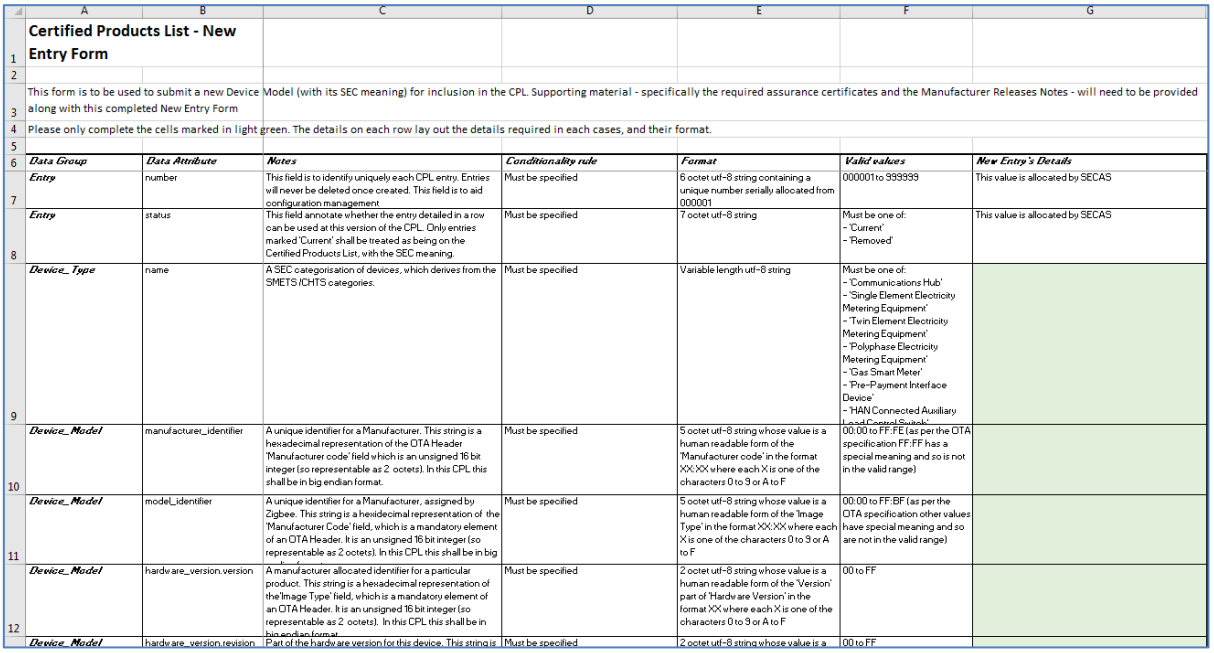
Figure 1: CPL Download Location

   Click on the link and the workbook will download.

2) Open the workbook and navigate to the CPL – New Entry tab.

Figure 2: New Entry Tab Location

3) Complete all fields highlighted in light green within the CPL – New Entry Tab.



	A	B	C	D	E	F	G
1	**Certified Products List - New Entry Form**						
2							
3	This form is to be used to submit a new Device Model (with its SEC meaning) for inclusion in the CPL. Supporting material - specifically the required assurance certificates and the Manufacturer Releases Notes - will need to be provided along with this completed New Entry Form						
4	Please only complete the cells marked in light green. 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 annotate 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.	Must be specified	Variable length 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' - 'Pre-Payment Interface Device' - 'HAN Connected Auxiliary	
10	***Device_Model***	manufacturer_identifier	A unique identifier for a Manufacturer. This string is a hexadecimal representation of the OTA Header 'Manufacturer code' field which is an unsigned 16 bit integer (so representable as 2 octets). In this CPL this shall be in big endian format.	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 characters 0 to 9 or A to F	00:00 to FF:FE (as per the OTA specification FF:FF has a special meaning and so is not in the valid range)	
11	***Device_Model***	model_identifier	A unique identifier for a Manufacturer, assigned by Zigbee. This string is a hexidecimal representation of the 'Manufacturer Code' field, which is a mandatory element of an OTA Header. It is an unsigned 16 bit integer (so representable as 2 octets). In this CPL this shall be in big	Must be specified	5 octet utf-8 string whose value is a human readable form of the 'Image Type' in the format XX:XX where each X is one of the characters 0 to 9 or A to F	00:00 to FF:BF (as per the OTA specification other values have special meaning and so are not in the valid range)	
12	***Device_Model***	hardware_version.version	A manufacturer allocated identifier for a particular product. This string is a hexadecimal representation of the'Image Type' field, which is a mandatory element of an OTA Header. It is an unsigned 16 bit integer (so representable as 2 octets). In this CPL this shall be in big endian format.	Must be specified	2 octet utf-8 string whose value is a human readable form of the 'Version' part of 'Hardware Version' in the format XX where each X is one of the characters 0 to 9 or A to F	00 to FF	
	Device_Model	hardware_version.revision	Part of the hardware version for this device. This string is	Must be specified	2 octet utf-8 string whose value is a	00 to FF	

Figure 3: New Entry – Required Fields

This tab is locked for editing aside from those fields which are required to be completed. Fields which must be completed are highlighted within the workbook in light green. The workbook itself provides guidance as to the correct completion of the form and also provides a reference source for all information.

4) Save the CPL – New Entry Tab as a new workbook.

Right click on the CPL – New Entry Tab and select 'Move or Copy…'

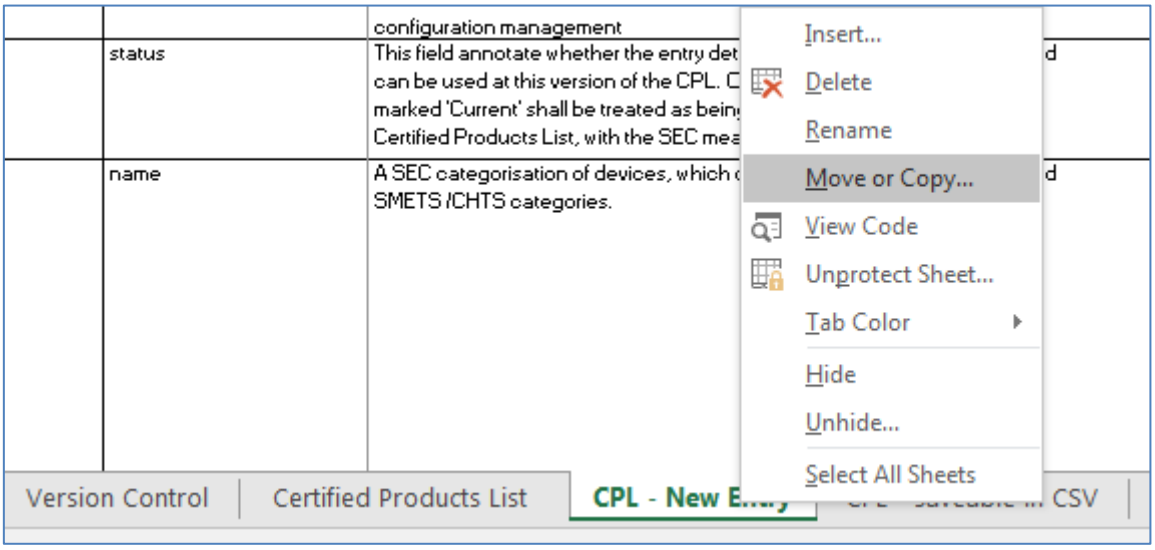


Figure 4: Saving the New Entry Form

The window below will open. Select 'To book: (new book)' and tick the 'Create a copy' checkbox.

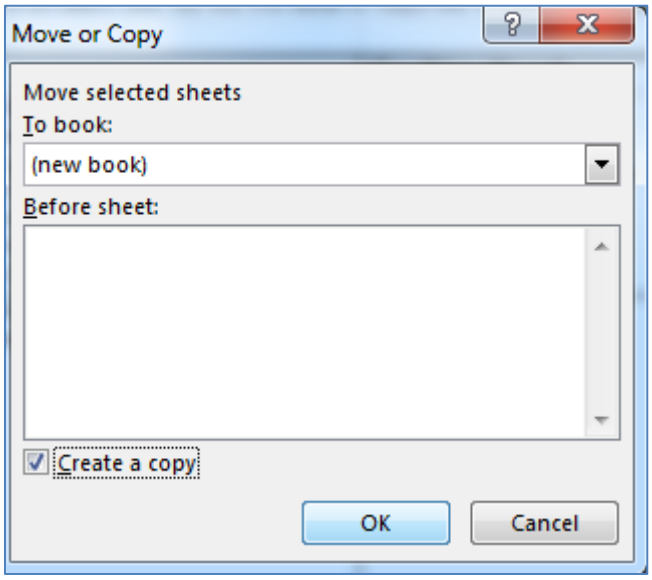


Figure 5: Saving the New Entry Tab

A new instance of Excel will open containing only the New Entry Tab. Give the workbook a descriptive filename and save it as normal.

5) Several device details contained in the Certified Products List are in hexadecimal format mandated by the SEC for the administration of the Smart Metering Inventory to enable communications with and the upgrade of firmware on Devices. For details, see Section 2.7 CPL Submission.

   The Version Control Tab of the CPL shows the change history of the CPL. Devices and Manufacturers are names are used in alphanumeric text format ("plain English"); these alphanumeric text formats are not mandated by the SEC but are added for the ease of readability.

It is recommended to combine the SEC mandated formats with the alphanumeric text description of the Device Manufacturer and the Device Model in the ZigBee certificate. Details are listed in Section 0 Table 2: CPL Submission Format Requirements

   ZigBee Certificate.

6) Email this new workbook alongside any required Assurance Certificates to SECAS@gemserv.com. Please ensure your email subject field identifies the email clearly as a submission to the Certified Products List.

   A member of the SECAS team will confirm receipt of your submission within one working day.

4. Submission Procedure for Products With a Manufacturer Image Hash

If you would like to include a Manufacturer Image Hash in your submission, this section describes the process for both adding a product with a Manufacturer Image Hash and adding a Manufacturer Image Hash to an existing product.

Where a Device Model is listed on the CPL but there is no hash associated, a new entry form can be submitted to associate a Hash with an entry. Simply complete the form using all of the same details used during the initial submission, however this time ensure the fields highlighted in yellow are completed. Indication should be provided in the submission email that the submission is for the purpose of updating a current entry. Submission of a Manufacturer Image Hash in this fashion also requires the associated Excel workbook to be digitally signed. Please see Section 8 of this guidance for application of Digital Signatures.

4.1 Submission Process

1) Complete steps 1) to 3) described in Section 3.

2) To include a Manufacturer Image Hash as part of the submission, the three fields highlighted in yellow must also be completed.

Data Group	*Data Attribute*	*Notes*	*Conditionality rule*	*Format*	*Valid values*	*New Entry's Details*
ZSE_Certificate	ZSE_version	Details the version ZSE that this Certificate was issued against. The format is not specified in SEC and is not required for automated matching.	Completion of field depends on SMETS/CHTS version. At current SMETS/CHTS, must be populated and valid for all Device Types.	Up to 40 octet utf-8 string	Must be populated. Must currently be one of: - 'ZigBee Smart Energy Standard 1.2a' - 'ZigBee Smart Energy Standard 1.2b'	
Manufacturer_Image	creator	To identifier the creator of the Manufacturer Image. The format is not specified in SEC but may be required for automated processing.	Fields in Manufacturer_Image must all be empty or all validly populated. It is a decision for manufacturers as to whether providing a Manufacturer Image is required for a particular CPL entry.	Up to 100 octet utf-8 string	Any utf-8 string of length up to 100 octets in length.	
Manufacturer_Image	hash	In line with SEC, a SHA256 hash calculated over the Manufacturer Image.	As for Manufacturer_Image.creator	95 octet utf-8 string whose value is a human readable form of the hash in the format XX:XX:...:XX where each X is one of the characters 0 to 9 or A to F	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 to FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF:FF	
Manufacturer_Image	descriptor	To describe whether this is an image in its entirety or a fragment of a larger image. The field is optional and for the manufacturer to chose how and whether they populate. For example "Fragment 1 of 2 of FW Version XX:XX:XX:XX"	Optional but should only be populated if Manufacturer_Image.hash is populated	Up to 45 octet utf-8 string	Any utf-8 string of length up to 45 octets in length.	
Contact	contact name	If there are any queries with this application, the person who SECAS should contact. NOTE this information will NOT be included in the CPL entry.				

Figure 6: Hash Submission

Note that the format of the Manufacturer Image – creator is not specified and so can be chosen by the submitting organisation. Typically, the submitting organisation that created the image is used to populate this field.

3) Apply your Digital Signature to the workbook.

For guidance on Digital Signature and their application please see Section 8 of this guidance.

4) Complete step 4) described in Section 3.

5. SECAS Validation of New Submissions

This section describes the checks that SECAS will perform on new submissions.

1) Upon a receipt on a new submission, SECAS will validate both the submission and the Assurance Certificates to confirm SEC compliance. SECAS will contact you if there is an issue with your submission.

a. The CPL – New Entry workbook contains validation rules which are applied when completing the form and prevent entry of invalid values. When invalid values are attempted to be entered, the workbook provides feedback to the user. SECAS will check that all the fields have valid entries.

b. In addition to this, SECAS will perform the following validation:

   i. Check the New Entry Form has been completed correctly. The validation rules within the workbook itself should ensure correct completion.

   ii. Validate digital signatures if a Manufacturer Image Hash is provided.

   iii. Check each Assurance Certificate against criteria agreed with the Device Language Message Specification User Association (DLMS UA), ZigBee Alliance (ZA), National Cyber Security Centre (NCSC). For more information on Assurance Certificates requirements, please see Section 2 of Appendix A.

2) SECAS will perform these additional checks before the New Entry Form is added to the CPL. The CPL will only be updated once it has been fully validated and the supporting documentation has been checked by SECAS.

3) SECAS will then issue the CPL in Comma Separated Values (CSV) file format to the DCC.

4) SECAS will publish a new version of the CPL on the SEC Website, updated to include your submission. A notification will be issued in the form of an email to all SEC Parties, informing them that a new version of the CPL has been published. If the DCC has loaded the submission into the DCC Systems, prior to the notification being issued, this will be indicated in the notification to SEC Parties.

6. Manufacturer Images and Hashes

In accordance with Section 4.1 of the CPL Requirements Document, if a Supplier Party or the DCC wish the Panel to associate the Hash of a Manufacturer Image with a Device Model on the CPL, the submitting Party must provide the Hash and the identity of person who created the Manufacturer Image in a digitally signed communication to the SEC Panel.

6.1 What is a Manufacturer Image?

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

6.2 What is a Hash?

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

This means that a Manufacturer Image will have a function applied and produce a string of letters and numbers of a fixed length. As the function applied is repeatable, the resultant string should always be the same, providing that the Manufacturer Image has not changed. If the Manufacturer Image has changed, then the string of letters and numbers the Hash function outputs will be different.

Devices are able to apply the specific Hash function themselves. Upon receipt of a Manufacturer Image the Device is able to calculate 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 that which the Supplier intended and therefore it will reject any installation commands.

6.3 Why include a Hash?

Firmware Hashes form part of the suite of cryptographic controls used within Smart Metering to achieve heightened security. If a Manufacturer Image Hash is not listed on the CPL for a specific Device Model, upgrading to the associated Firmware version will not be possible.

7. Firmware Information Repository

The Firmware Information Repository (FIR) has been introduced to the SEC via the SEC Modification Proposal 0009.

7.1 What is the need for the Firmware Information Repository?

Smart Meters for gas and electricity 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 Supplier Licence Conditions.

In 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 in order 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 Firmware Information Repository (FIR) provides this information and enables the Supplier to enquire with the Device manufacturer about firmware upgrade packages and further information.

7.2 What is the legal background?

The SEC specifies in Sections F2.14- F2.17 the obligations with regards to the FIR, these are in summary:

- The Panel has to establish and maintain a list of firmware releases named “Firmware Information Repository”.
- The FIR contains the following mandatory fields:
  - Unique identifier of a CPL record;
  - Manufacturer contact details including email address, telephone number and business address;
  - Release Notes where the content is at the discretion of the Manufacturer.
- The FIR will be updated alongside the Central Products List.
- The Party or any other person submitting Device details for addition to the CPL shall also supply the FIR details.

7.3 How does the FIR look, where is it stored and who has access?

The FIR is an Excel spreadsheet and is hosted on the SEC Website. The FIR is only available to SEC Parties which means access is only granted with a valid login to the SEC Website.

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

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

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 folllwing 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 Meter Ltd	123 Example Street Example City, AB12 CD3 United Kingdom 01234 567 8910 www.example.company.co.uk info@example.company.co.uk	General Release for use with SMETS2 VX.Y www.example.company.co.uk/sampleproduct/publicinformation

Figure 7: FIR Example

7.4 What data is required for the FIR and how is the data submitted?

The FIR details are only required for Metering Devices and must be included as part of the CPL Submission for the following Devices:

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

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 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 information about the firmware release and/or an URL. The URL must be functional.

As part of the CPL submission process 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 on the SEC Website (login required, see also Section 7.3).

7.5 FIR Release Notes and confidentiality

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 in order to access such information.

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

In case there is a concern with the FIR Release Notes in terms of commercial or confidential information, a SECAS Security Expert will vet the FIR Release Notes entry prior to releasing a new version of the FIR.

Possible example content for the FIR Release Notes could be:

- General Release
- General Release for use with SMETS2 VX.Y
- Commercial Release with bespoke functionality

It is also possible to include a URL pointing to the manufacturers 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.

8. Digital signatures

Section 4.1 of the CPL Requirements Document states that:

Where the DCC or a Supplier Party wishes the Panel to associate the Hash of a Manufacturer Image with a Device Model on the CPL, that Party shall provide the Hash and the identity of the person who created the Manufacturer Image in a communication to the Panel which has been Digitally Signed by the person who created the Manufacturer Image in a manner that reasonably enables the Panel to check that the communication originates from the person who created the Manufacturer Image.

8.1 What is a Digital Signature?

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 the SEC Panel to verify the identity of the sender and the integrity of the message sent.

8.2 Acquiring a Digital Signature

The signing of Excel spreadsheets, and options for associated publicly available Public Key Infrastructure (PKIs), are explained on Microsoft's website.

Note that the format of the 'identity of the organisation that created the image' is not specified and so can be chosen by the submitting organisation. However, whatever is chosen should be identical to that used when the submitter gets a digital certificate from their chosen public PKI provider. This is so that the Panel can discharge their responsibility to check this on receipt of a signed Excel file.

On receipt of a file notifying a request that a new Product related to a Manufacturer Image is to be added to the CPL, the Panel has to verify the digital signature as an additional check before updating the CPL.

8.3 Applying your Digital Signature

If submitting a Hash alongside your CPL entry, the CPL – New Entry tab of the Excel workbook is required to be digitally signed. Microsoft Excel has the functionality to apply Digital Signatures. Other non-proprietary pieces of software, such as Open Office, also has built in functionality for the application of Digital Signatures.

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

9. Removal of an entry from the CPL

Entries on the CPL will have one of two statuses:

- Current
- Removed

All entries will initially have a status of Current.

An entry will be altered to Removed if SECAS receive notification that one or more of the relevant Device Model's Assurance Certificates have been revoked. An entry will also be listed as Removed if the relevant Device Model's CPA certificates expire[3].

SECAS are required to issue notification that CPA Certificates are due to expire twelve and six months in advance of their expiry date, using the contact details provided in the initial submission form.

[3] DLMS/Companion Specification for Energy Metering (COSEM) and ZigBee Smart Energy Certificates do not expire.

Appendix A: Supporting Information

1. What needs to be on the CPL?

As per SEC Section F2.1, the SEC Panel is required to maintain a list of all Device Models for which the Panel has received all the Assurance Certificates required for the Device Type.

1.1 What is a Device Model?

The SEC definition is below:

Device Model *means, in respect of a Communications Hub or a Device (other than a Communications Hub Function or a Gas Proxy Function), the Manufacturer, the model, the hardware version and the firmware version of the Communications Hub or Device.*

The CPL is a listing of all Device Models. If a new version of firmware is released for a type of meter a new Device Model is formed. As the CPL is a listing of Device Models, a new submission would be required, including the relevant Assurance Certificates, for the new Device Model in this example.

1.2 What is Physical Device Type?

The SEC definition is below:

Physical Device Type *means, in respect of a device, its type which may be only one of: a Communications Hub; a Single Element Electricity Metering Equipment (as defined in SMETS); a Twin Element Electricity Metering Equipment (as defined in SMETS); a Polyphase Electricity Metering Equipment (as defined in SMETS), a Gas Smart Meter; a Pre-Payment Meter Interface Device; a HAN Connected Auxiliary Load Control Switch; an IHD; or a Type 2 Device (Other).*

1.3 What Device Types must be on the CPL?

Device Models of the following Physical Device Types must be listed on the CPL:[4]

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

[4] As per SEC Section H5.3(b), Type 2 Devices are not required to be included on the CPL.

2. Assurance Requirements

2.1 Assurance Requirements

Table 1 below shows what Assurance Certification is required by Physical Device Type for it to be listed on the CPL, as stated in the latest version of the SEC and the SEC Subsidiary Document, Schedule 9 - Smart Metering Equipment Technical Specifications Version 2 and Schedule 10 - Communications Hub Technical Specifications.

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

Table 1: Assurance Requirements

2.2 Commercial Product Assurance (CPA)

The CPA scheme is administered by a UK Government's national technical authority for information assurance, 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.

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. A list of approved CPA test labs can be found here.

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.

More information on NCSC's CPA scheme can be found here.

2.3 Alignment with CPA Certificate Assurance

SECAS are working with the Department of Business, Environment and Industrial Strategy (BEIS) and the NCSC on whether the "version" field of the certificate could reflect a concatenated "Device_Model" field. SEC Section F states that, *'An Assurance Certificate will not be valid unless it expressly identifies the Device Model(s) and the relevant Physical Device Type to which it applies.*'.

2.4 Adding Device Models to CPA Certificates

As per section 5 of SEC Appendix Z – CPL Requirements Document:

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

(a) the DCC for Communications Hubs; or

(b) a Supplier Party for Device Models of all other Physical Device Types,

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

When adding a Device Model under an existing CPA Certificate, SECAS require confirmation directly from the Supplier Party for Device Models and from the DCC for Communications Hubs that they are meeting their SEC Requirements, provided that it was originally issued only by virtue of having different versions of hardware and/or firmware that do not significantly impact on the security functions of the Device Model (as set out in the CPA Assurance Maintenance Plan).

2.5 ZigBee Certification

The ZigBee Certified Product program tests a device against a ZigBee Alliance 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 ZigBee Alliance. Further information on joining can be found here.

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

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

The ZigBee Alliance's guide on ZigBee Certification is available for download here.

2.6 Alignment with ZigBee Certificate Assurance

SEC Section F2.5 states that 'An Assurance Certificate will not be valid unless it expressly identifies the Device Model(s) and the relevant Physical Device Type to which it applies.' In addition, the CPL requires the supporting assurance certificate evidence to reflect what is included within the CPL submissions.

The requirement for CPL submissions and the supporting evidence has been present since the CPL went live; however, SECAS, on behalf of the Panel, has recently received Certified Product List (CPL) submissions with discrepancies between the content of the submissions and the content of associated assurance certificates.

The discrepancies are mainly due to the formatting of the 5 CPL Device_Model data fields:

- Device_Model - manufacturer_identifier
- Device_Model - model_identifier
- Device_Model - hardware_version.version
- Device_Model - hardware_version.revision

- Device_Model - firmware_version

In these CPL submissions, the Device Model was in the relevant utf-8 string format (e.g. 01:02:05:06 or 00:00:10:00) but the device model specified in the Zigbee assurance certificate was in a plain english format (e.g. Version 1.2.5.6 or v1.0). SECAS have noted discrepancies in all 5 fields of "Device_Model", However these inconsistencies related mostly to Device_Model - firmware_version.

To enable Suppliers to meet their SEC obligations on ensuring the compliance of Devices with SMETS and GBCS, the CPL needs to identify the exact make, model and version number of Devices and firmware. To be able to record this and to use it in the Inventory and Over The Air (OTA) firmware upgrades, the DCC needs to have the information in hexadecimal machine code format. The Devices themselves already have the information encoded in hexadecimal machine code so that they can respond to and interpret commands.

On the 15th September, the SEC Panel considered the requirement regarding CPL submissions and the types of discrepancies that were being received between the CPL submission and support assurance certificates.

The Panel agreed that the SEC requirements must be met, but recognised that Parties and manufacturers may be part way through assurance activities. With that in mind the Panel agreed that from the 1st December 2017 onwards, the relevant fields within the accompanying ZigBee Assurance certificates will need to be in the same hexadecimal format and match what is included in the CPL submissions. Following the 1st December 2017, SECAS will not accept new CPL submissions where there is a discrepancy.

Therefore, manufacturers and SEC Parties who provide CPL information will need to ensure they provide the relevant information to the ZigBee Test Houses in hexadecimal format.

2.7 CPL Submission

Table 2 below reiterates the requirements for CPL Submissions.

Data Group	Data Attribute	Format	Valid values
Device_Model	manufacturer_identifier	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 characters 0 to 9 or A to F	00:00 to FF:FE (as per the OTA specification FF:FF has a special meaning and so is not in the valid range)
Device_Model	model_identifier	5 octet utf-8 string whose value is a human readable form of the 'Image Type' in the format XX:XX where each X is one of the characters 0 to 9 or A to F	00:00 to FF:BF (as per the OTA specification other values have special meaning and so are not in the valid range)
Device_Model	hardware_version.version	2 octet utf-8 string whose value is a human readable form of the 'Version' part of 'Hardware Version' in the format XX where each X is one of the characters 0 to 9 or A to F	00 to FF
Device_Model	hardware_version.revision	2 octet utf-8 string whose value is a human readable form of the 'Revision' part of 'Hardware Version' in the format XX where each X is one of the characters 0 to 9 or A to F	00 to FF
Device_Model	firmware_version	11 octet utf-8 string whose value is a human readable form of the File Version in the format XX:XX:XX:XX where each X is one of the characters 0 to 9 or A to F	00:00:00:00 to FF:FF:FF:FF (note that the use of the octets as (octet 1) Application Release, (octet 2) Application Build, (octet 3) Stack Release and (octet 4) Stack Build is recommended in OTA but not mandated and so is not mandated in the CPL)

Table 2: CPL Submission Format Requirements

2.8 ZigBee Certificate

Table 3 below states the requirements for ZigBee assurance certificate fields:

Data Fields	Corresponding CPL field	Format	Valid values
Type of Device	Requirements unchanged		
Manufacturer	manufacturer_identifier	5 octet utf-8 string whose value is a human readable form of the 'Image Type' in the format XX:XX where each X is one of the characters 0 to 9 or A to F	00:00 to FF:FE (as per the OTA specification FF:FF has a special meaning and so is not in the valid range)
Model Identification	model_identifier	5 octet utf-8 string whose value is a human readable form of the 'Image Type' in the format XX:XX where each X is one of the characters 0 to 9 or A to F	00:00 to FF:BF (as per the OTA specification other values have special meaning and so are not in the valid range)
Hardware Version	Concatenation of 2 CPL items: • hardware_version.version; and • hardware_version.revision.	Concatenations of 4 CPL fields separated by and underscore. 5 octet utf-8 string whose value is a human readable form of the 'Image Type' in the format XX:XX where each X is one of the characters 0 to 9 or A to F	00_00 to FF_FF. (Should match the formatting of the hardware_version.version; and hardware_version.revision fields in the new CPL submission, separated by an underscore).
Firmware Version	firmware_version	11 octet utf-8 string whose value is a human readable form of the File Version in the format XX:XX:XX:XX where each X is one of the characters 0 to 9 or A to F	00:00:00:00 to FF:FF:FF:FF (note that the use of the octets as (octet 1) Application Release, (octet 2) Application Build, (octet 3) Stack Release and (octet 4) Stack Build is recommended in OTA but not mandated and so is not mandated in the CPL)
Certification Date	Requirements unchanged		
Certification ID Number	Requirements unchanged		

Table 3: ZigBee Assurance Certificate

It is recommended that the Manufacturer, Model Identification and Hardware 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. The submitter is responsible for the correct hexadecimal data and the alphanumeric text description when applying for ZigBee certification and subsequent CPL submissions.

A list of Manufacturer names and industry recognised ESME and GSME Meter Device names in alphanumeric text format is available on the CPL page on the SEC Website here:

https://smartenergycodecompany.co.uk/certified-products-list/.

As noted above, from the 1st December 2017 SECAS will be rejecting submissions that do not meet the requirement relating to the ZigBee certificate. This will require the ZigBee certificates to display the hexadecimal reference and ensures that SECAS (on behalf of the SEC Panel) can carry out their SEC obligation to check the accuracy of the information provided before passing the new CPL

submissions to the DCC. For instances where it is not possible for the information to match directly, see the subsequent sections below.

2.9 Single CPL Submission with matching ZigBee Certificate

This case describes the unique mapping between one ZigBee certificate and one Device.

The combination of hexadecimal data and alphanumeric descriptions shown on the ZigBee certificate must allow the mapping to the data used in the OTA Header fields when carrying out the CPL submission.

This is particularly important for the File Version/Firmware Version field. Table 4 below lists some examples:

CPL Item	CPL OTA Header Field Content	ZigBee Certificate Firmware Version	Comment
firmware_version	12:03:12:34	12.3 (Stack 1.2.3.4)	BCD coding
firmware_version	0C:03:0C:22	12.3 (Stack 12.34)	Hex coding
firmware_version	0D:07:00:00	Some String (14.7)	Hex coding; text omitted in CPL
firmware_version	00:00:07:8D	7.8D Other String	Hex coding; text omitted in CPL

Table 4: Version Mapping ZigBee Certificate – OTA Header

A similar approach must be followed for the other OTA Header fields: manufacturer_identifier, model_identifier and hardware_version. It is suggested to follow the recommendations in Section 0 Table 2: CPL Submission Format Requirements

ZigBee Certificate.

The identification of a Device and the mapping to the associated ZigBee certificate is maintained.

2.10 Multiple CPL Submission without matching ZigBee Certificate

This section describes the case of mapping one ZigBee certificate to multiple firmware versions of a single Device or multiple Devices.

Device manufacturers may use a modular approach when designing the firmware and create separate software packages for ZigBee functionality and other parts of the firmware. This modular approach allows manufacturers to either combine all software packages into a single firmware update image or to create partial images to upgrade only certain functions of the Device.

The modular approach may result in updates to Device firmware, which do not affect the ZigBee certification. Subject to the manufacturer undertaken appropriate checks 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 with the OTA Header details of the CPL submission. To ensure that a CPL submission is valid in this situation additional information is required from the manufacturer, which allows clear identification of the mapping between the Device details in the CPL submission form and the ZigBee certificate.

The manufacturer shall provide supporting evidence, which could take the form of the full or an extract from the related release notes of the Device and/or the affected firmware version. The supporting evidence shall clearly identify the ZigBee firmware module used; the identified ZigBee module must

uniquely relate to a ZigBee certificate. If the content of the supporting evidence is unclear in relation to how the certificate maps to the CPL submission SECAS will seek clarifications. In addition, a clear statement and/or supporting assertion in writing that no changes have occurred that would require updates to certificates is encouraged.

The release notes or equivalent supporting evidence shall be stored by SECAS as evidence in support of the related CPL submission. The release notes or equivalent evidence will not be made available publicly and will be retained for auditing purposes only.

2.11 Existing ZigBee Certificates

Where manufacturers are already in possession of a ZigBee Certificate, that will not match the content of your CPL submission from 1st December 2017, manufacturers may be able to request that the ZigBee Alliance re-issue a certificate, with the relevant fields updated or amended. However, this is entirely at their discretion and retesting may be required.

2.12 Device Language Message Specification Companion Specification for Energy Metering (DLMS/COSEM) Certification

DLMS COSEM is a communication standard used by certain Devices. It sets out the rules for data exchange with energy meters.

The DLMS User Association is formed of various stakeholders from within industry, such as manufacturers, utility providers, etc. They are responsible for development and maintenance of the standard, as well as developing the conformance test and its associated tools.

The DLMS User Association provide 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.

Further information on the DLMS certification process can be found here.

2.13 Alignment with DLMS Certificate Assurance

The Security Sub Committee Chair has formerly raised a question to the DLMS Chair to enquire whether the “Type” field can hold enough characters to match a concatenation of the 5 “Device_Model” fields from the CPL Submission. If so, SECAS will issue guidance on this requirement at a later date, on whether this information should be included.

2.14 Expiry of Certificates

As per SEC Section F2.6, Import Suppliers are required to ensure a replacement CPA Certificate (DLMS and ZigBee certification does not expire) is issued for all Device Types (other than Communications Hubs, which are the responsibility of the DCC to assure).

SEC Section F2.7 requires the SEC Panel to notify those mentioned above twelve and six months in advance of CPA Certificate expiry dates. When submitting a product for inclusion on the CPL, a contact email address is required as part of the submission form. Notification of CPA certificate expiry will be issued by SECAS twelve and six months in advance of expiration to these nominated points of contact.

3. What is the Smart Metering Inventory?

The Smart Metering Inventory (SMI) is established and maintained by the DCC in accordance with SEC Section H5. It is an electronic database of Devices which records information such as Device Type and MPAN/MPRN for all installed Smart Meters. Included within the SMI is a field called SMI Status which indicates the current state of the Device, such as ‘commissioned’ or ‘withdrawn.’ It is the

SMI and the associated SMI Status for a Device which dictates whether or not the Device can be communicated to and from via the DCC.

In order for a Device to be listed on the SMI it must first be fully assured and listed on the CPL.

The CPL is also used to manage the SMI Status of Devices already included in the SMI. If a Device Model is no longer fully assured, it's status shall be adjusted in the CPL to indicate this. The DCC will then use this to adjust the SMI Status for all applicable Device Models listed on the SMI.

Please see SEC Sections H5[5], H6[6] and SEC Subsidiary Document, Appendix AC – Inventory, Enrolment and Withdrawal Procedures for further information on the SMI and its relationship with the CPL.

4. How SEC Parties and the DCC are informed of changes to the CPL

As per SEC Section F2.8, the Panel is required to provide an updated version of the CPL to the DCC, publish an updated CPL on the SEC Website and notify all SEC Parties that an update has occurred. All of this must occur within one Working Day after being required to add or remove Device Models to or from the CPL.

4.1 Provision to the DCC

The CPL workbook includes a tab which has been tailored for the DCC. As per section 7.1 of the CPL Requirements Document, the Panel is required to provide a Digitally Signed copy of the CPL when providing it to the DCC. This digital signature shall be applied using the DCC's Infrastructure Key Infrastructure (IKI) tokens.

At the request of the DCC, a tab allowing the export of the CPL to CSV file format has also been included in the CPL Workbook. The tab cannot be edited and is based solely on the relevant parts of the CPL itself, however it is formatted in such a manner which allows it to be saved as a workable CSV file format. This option has been included to facilitate the DCC's import of the CPL into their systems for the purpose of managing the SMI. The DCC shall 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 published CPL and it being uploaded by the DCC into its Data Service Provider (DSP).

4.2 The SEC Website

The Certified Product List workbook will be uploaded to the SEC Website and will replace previous versions hosted. Full change control is included in the first tab of the workbook, so Parties are able to identify what the key changes are.

4.3 Directly Notifying SEC Parties

Once a copy has been uploaded to the SEC Website, a notification will be issued to all SEC Parties informing them that this has occurred. If the DCC process the submission, prior to notifications being issued to SEC Parties, SECAS will indicate whether it has successfully loaded. Where it is not loaded prior to the notification being issued by SECAS, this will be indicated in the email.

The SEC Panel is required to provide updated versions of the CPL to the DCC within one Working Day following a new submission.

[5] Smart Metering Inventory and Enrolment Services
[6] Decommissioning, Withdrawal and Suspension of Devices