

Smart Energy Code

Additional Certified Products List Guidance – Certificate Content Alignment or Supplementary Supporting Evidence

Version Number: 2.1

Date Published: February 2018

Relevant Parties

This guidance was drafted for:

- SEC Parties
- SEC Panel
- Manufacturers and any other interested parties

Purpose

This note is intended to provide additional clarity in relation to Certified Products List (CPL) submission requirements. The content will soon be added to an updated version of the CPL Submission Guidance available on the Certified Products List page on the SEC Website.

1. 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 Certified Product List (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 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 five 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 requires 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 2017, 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

This document is classified as
White in accordance with the
Panel Information Policy

Administered by



Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

certificates. The Panel agreed that the SEC requirements must be met, but recognised that SEC 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, SEC Parties and manufacturers who provide CPL information will need to ensure they provide the relevant information to the ZigBee Test Houses in hexadecimal format.

2. CPL Submission Requirements

The table 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).

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

3. Zigbee Certificate

The table 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 '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).
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 underscore. 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 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_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		

As noted above, from the 1st December 2017 SECAS will be rejecting submissions that do not meet the requirement relating to the ZigBee certificate, unless supplementary evidence is provided clearly setting out how the certificates map to the CPL submission (see section 5 below for further details). To meet the SEC requirement without providing additional mapping information, 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.

4. Single CPL Submission with matching ZigBee Certificate

It is possible to combine the version data for CPL submissions with an alphanumeric description when submitting the Device for ZigBee approval. The resulting alphanumeric string listed on the ZigBee certificate must allow the mapping to data used in the OTA Header fields when carrying out the CPL submission.

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

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

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

A similar approach is possible for the other OTA Header fields: `manufacturer_identifier`, `model_identifier` and `hardware_version`. The identification of a Device and the mapping to the associated ZigBee certificate is maintained.

5. Multiple CPL Submission without matching ZigBee Certificate

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 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.

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

6. Alignment with DLMS Certificate assurance

The Security Sub Committee Chair has formerly raised a question to the Device Language Message Specification (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.

7. Alignment with CPA Certificate assurance

In a similar manner, SECAS are working with the Department of Business, Environment and Industrial Strategy (BEIS) and the National Cyber Security Centre (NCSC) on whether the “version” field 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.*'.

Further information on CPL submissions

More CPL information can be found in [SEC Section F2 \(Certified Products List\)](#) and [SEC Appendix Z \(CPL Requirements Document\)](#).

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.