PSA Certified™ Level 1 Step-by-Step Guide
PSA Certified Level 1 Step-by-Step Guide

Getting Your Product PSA Certified Level 1

Audience: Chip vendors, OS suppliers & OEM developers

Background

PSA Certified is the independent security evaluation scheme for PSA based IoT chips, OS and devices. It aims to build trust for the IoT value chain using a progressive multi-level assurance program for developers using a security domain called a PSA Root of Trust (PSA-RoT) to provide trusted functionality to the platform.

TrustCB has been appointed as the Certification Body for PSA Certified. TrustCB was selected for its strong experience in operating high assurance certification schemes. Any questions relating to the PSA Certified scheme operation can be emailed to psacertified@trustcb.com, or can be discussed with your chosen test lab.

The following is provided as guidance for developers wanting to gain PSA Certified Level 1 for their solutions and optionally to showcase their PSA Certified Level 1 solutions on psacertified.org.

Note for Chip Vendors

PSA Certified Level 1 asks chip vendors questions on support of Crypto, Secure Storage and Entity Attestation Token. This functionality is available by porting Trusted Firmware-M to your chip or developing your own trusted firmware and adopting the PSA Functional APIs. Before applying for PSA Certified Level 1, chip vendors should run, and ensure their solutions passes, the PSA Functional API test suites. When you have passed and receive a digital certificate number (EAN-13+5 format) it is recommended that this is used as the “HW version” claim of the Entity Attestation Token.

Getting Your Product PSA Certified Level 1

You should choose a test lab and obtain an agreement with your chosen lab to review your products PSA Certified Level 1 questionnaire and for them to hold your data confidentially.

Work with your selected test lab to complete the PSA Certified Level 1 application form, which can be downloaded from trustcb.com/iot/psa-certified.

Download and complete the latest version of the PSA Certified Level 1 questionnaire from www.psacertified.org. It is your responsibility as developer (chip vendor, OS supplier or OEM developer) to complete the PSA Certified Level 1 questionnaire and submit it to your chosen lab. When filling in the questionnaire it is suggested that an unsigned version is first sent to the test lab for clarifications as a Word document. Your lab may request additional supporting documentation to support the responses provided in

---

1 This requirement has been waived by Arm until TechCon in October 2019
the questionnaire. When the answers have been reviewed and agreed, then sign and create a PDF file of the final, formal version of the questionnaire.

Send an email to your test lab allowing them to share the completed application, questionnaire and required supporting documentation with the certification body (see below).

When the test lab has reviewed the questionnaire and it has been assessed as passing the minimum threshold, they will email psacertified@trustcb.com, using “New PSA Certified Application” as a subject line and attaching the completed application form, passing questionnaire and required supporting documentation.

Once the test lab has received notification of approval from TrustCB and the EAN-13, the test lab will also return the passing questionnaire (with the 18 digit reference, EAN-13+5) to the developer and store a copy for a period of five years. For more detail on using the EAN-13+5 number please see the next section on “PSA Certified & Digital Certificate Numbers”.

Additionally, the lab will send to the certification body an Excel spreadsheet containing pre-filled information for the publication of the certification. There is an additional tab on the Excel spreadsheet to be completed if the developer wants to showcase the product on psacertified.org, in which case the following additional information should be provided:

1. Digital Certificate Number (EAN-13+5)
2. Company logo
3. Product name or product family name
4. Short description (25 words)
5. Image or graphic to represent the product
6. Link to the developer’s website for the product (if appropriate)
7. Whether the developer would like to use the PSA Certified logo and trademarks

The PSA Certified scheme uses TrustCB as a Certification Body to provide a set of independent technical experts to review the test lab’s assessment of the PSA Certified Level 1 questionnaires. This allows for harmonization of assessments across labs. The Certification Body will check that the test lab’s assessment has been completed satisfactorily and then forward the Excel spreadsheet containing the draft digital certificate entry (and details for showcasing if required) to inform the psacertified.org web designers to add the developer’s showcase information and the digital certificate.

It is up to the developer if they wish to make their PSA Certified questionnaire public. Arm has published the Trusted Firmware-M and Musca questionnaire as an example on psacertified.org. The corresponding product showcase can be seen in Figure 1 below.
If the developer wishes to use the PSA Certified logos and trademarks, a **trademark request should be made via the PSA Certified website.**

**Digital Certificate Numbers and EAN-13+5**

The globally unique 18-digit number (EAN-13+5) is entered on the questionnaire by the test lab when they have received details of the EAN 13 from TrustCB, along with approval of the PSA Certified Level 1 results. The test lab will also use the EAN-13+5 on the draft digital certification they send to TrustCB for use on the PSA Certified website.

**For Chip Vendors**

The +5 digits enable encoding of Trusted Firmware revisions and new certification attempts. Together the EAN-13 and the +5 describe the PSA-RoT i.e. the chip-type and Trusted Firmware version.

The first digital of the +5 encodes the number of the certification attempts by the lab of this chip type, starting with ‘1’. For example, if the product was evaluated as a delta certification or at a higher level then this leading digit of the +5 would be incremented. The following 4 digits encode the software version. For example, if a chip developer uses Trusted Firmware-M version 1.0, this should be encoded as 0010.

As a (chip developer) example:

Chip initial attestation token: 6405123456789

Software is Trusted Firmware-M tag build v1.0

Digital certificate number entered on questionnaire/forms (case of first certification attempt using Trusted Firmware-M v1.0): 6405123456789-10010
For RTOS Vendors and OEMs

The +5 digits enable encoding of new certification attempts and software version. As with silicon vendors, it is proposed that the first digit of the +5 encodes the number of the certification attempts by the lab, starting with ‘1’.

The developer should let the test lab know how it wishes to encode the last 4 digits to represent the software version.

![Fig.2 Process flow for PSA Certified Level 1](image-url)