PSA Certified™ Level 1 Step-by-step guide

Document number:	JSADEN005	Version:	1.4
Date of Issue:	15/02/2019		
Author:	Arm		

PSA Certified step by step guide – Level 1

Getting your product PSA Certified

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.

The following is provided as guidance for developers wanting to showcase their PSA Certified Level 1 solutions on the psacertified.org website. In Q2'19 we plan to have an independent PSA Certified scheme manager to run the process and manage interactions with the test labs. Until an independent scheme manager is in place Arm will act as caretaker for this role. If you have any questions, please email psacertified@arm.com or ask your chosen test lab.

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 TF-M to your chip or developing your own trusted firmware and adopting the PSA Developer APIs. Before applying for PSA Certified Level 1 please run and pass 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

Developers should download the latest version of the PSA Certified Level 1 questionnaire from www.psacertified.org

Obtain an agreement with your chosen lab to review your products Level 1 questionnaire and for them to hold your data confidentially.
Send an e-mail to your test lab allowing them to share the questionnaire with scheme moderators (see below). When filling in the questionnaire it is suggested that an unsigned draft application is first sent to the test lab for clarifications as a Word document. When the answers have been reviewed and agreed, then sign the questionnaire as the formal application.

When the test lab has reviewed the questionnaire and it has been assessed as passing the minimum threshold, they will add a globally unique 18 digit number (EAN-13 +5) to the questionnaire form as a reference. For more detail on using the EAN-13 +5 number please see the next section on "PSA Certified & Digital Certificate Numbers". The test lab will return the updated questionnaire to the developer and store a copy for a period of 5 years.

It is up to the developer if they wish to make their PSA Certified questionnaire public. Arm will publish the TF-M and Musca questionnaire as an example on psacertified.org

The Test Lab will email psacertified@arm.com with the draft digital certificate entry as an Excel spreadsheet. If the Developer has requested no publicity (for example a non-released product) a reduced information (redacted) draft digital certificate may also be sent for use on the web site.

If the developer has been told by the test lab that the product has passed and wants to showcase the products on psacertified.org they should send the following to psacertified@arm.com :

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

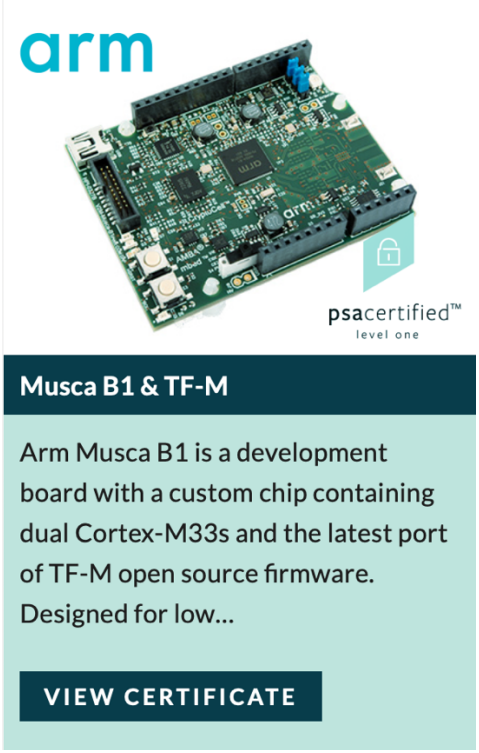

Fig 1. Certified products are showcased on www.psacertified.org

If the Developer wishes to use the PSA Certified logos and trademarks a trademark agreement will be sent by return email.

The PSA Certified scheme uses independent technical experts to additionally review the Level 1 questionnaires. The moderators will seek to harmonize the reviews and assess how the threshold is applied across labs. If the developer needs the moderator review under NDA then please let the reviewers know so that one can be put in place. The test lab will use PGP and email to send the completed questionnaire to the selected moderators and discuss the review focusing on the "N/A" and "Partial" answers. This moderator process will

be “behind the scenes” from the developer’s point of view. Moderators will not keep long term copies of the questionnaire (test labs will do that)

The scheme manager will check that the moderator's reviews have completed satisfactorily and then inform the psacertified.org web designers to add the developer’s showcase information and the digital certificate.

Digital Certificate Numbers and EAN-13 +5

The EAN-13 +5 is entered on the questionnaire by the test lab when they have reviewed the questionnaire and satisfied it meets the minimum Level1 threshold. The test lab will also use the EAN13 +5 on the draft digital certificate they send to psacertified@arm.com for use on the psacertified.org website.

The + 5 digits enables encoding of Trusted Firmware revisions and new certification attempts. Together the EAN-13 and the +5 describe the PSA-RoT i.e. chip-type and Trusted Firmware version.
The first digit 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 TF-M v1.0 this should be encoded as 0010.

As a (chip developer) example:
Chip initial attestation token = 6405123456789
Software is TF-M tag build v1.0
Digital Certificate Number entered on questionnaire /forms (case of first certification attempt and using TF-M v1.0)
6405123456789-10010

For RTOS vendors and OEMs
The chosen test lab will supply the EAN-13 number and update the questionnaire if it is assessed as passing the minimum threshold.
The + 5 digits enables 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.

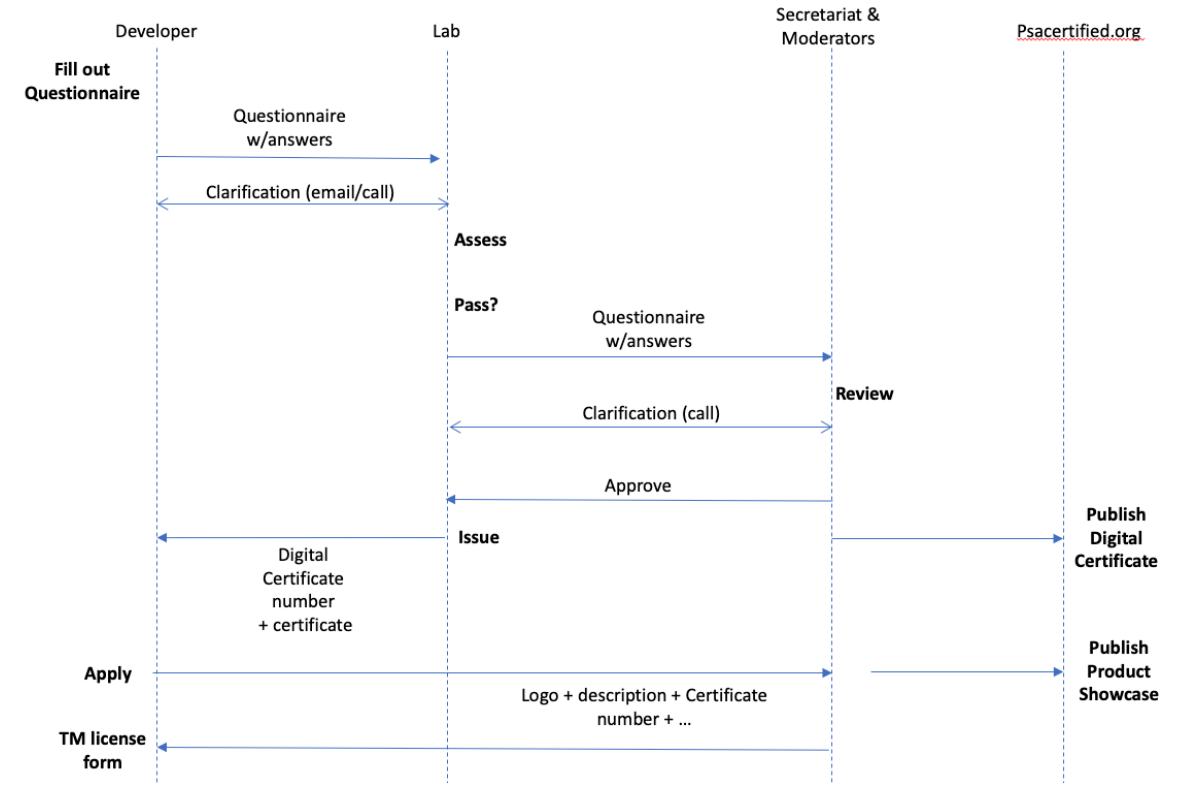

Fig 2. Process flow for PSA Certified