PSA Certified™ Level 2 Step by Step Guide Version 1.1

psacertified™

psacertified™
level two

Document number:	JSADEN011
Version:	1.1
Release Number:	01
Author	PSA JSA Members: Arm Limited Brightsight B.V. CAICT Prove & Run S.A.S. Riscure B.V. Trust CB B.V. UL TS B.V.
Authorized by:	PSA JSA Members
Date of Issue:	04/03/2020

Non-Confidential Proprietary Notice

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

Audience

Chip vendors

Background

PSA Certified is the independent security evaluation scheme for Platform Security Architecture-based IoT chips with a security component called a PSA Root of Trust (PSA-RoT) that provides trusted functionality to the platform.

This document provides guidance for developers wanting to showcase their PSA Certified Level 2 solutions on the www.psacertified.org website. TrustCB acts as the Certification Body for PSA Certified helping to run the process and manage interactions and ensure consistency across the test labs. If you have any questions, please email psacertified@trustcb.com or ask your chosen test lab.

Note for Chip Vendors

PSA Certified Level 2 requires a test lab evaluation of your PSA-RoT implementation. The PSA Certified Level 2 Protection Profile defines nine security functions that can be implemented by trusted firmware executing on your trusted hardware.
If Trusted Firmware-M is being used please use the latest version and read the release notes.

Note for PSA Certified Level 2 Ready Evaluations

PSA Certified Level 2 Ready is a pre-certification evaluation of a chip, FPGA or development based system that may not be able to meet all nine security functions of the PSA Certified Level 2 Protection Profile [PSA-PP]. In these cases, only the claimed security functions are tested by the Evaluation Laboratory who issues the Evaluation Technical Report (ETR). Only logical attacks are considered in a PSA Certified Level 2 Ready evaluation.

The developer proceeding to a PSA Certified Level 2 Ready evaluation should prepare a Security Target that clearly identifies which Security Functional Requirements (SFR) are being claimed. An example security target has been prepared for PSA Certified Level 2 Ready using Musca B development board and Trusted Firmware-M v1.0 that can be shared upon request.

When the ETR has been generated the developer can choose to have a "showcase" entry on www.psacertified.org that links to a summary of the SFR's evaluated as passing. There is no certificate generated for a PSA Certified Level 2 Ready evaluation, but the developer can obtain the rights to use a specific "PSA Certified Level 2 Ready" logo.

When the PSA Certified Level 2 Ready IP is implemented in a mass production chip, that product may proceed to a full PSA Certified Level 2 security assessment to receive a PSA Certified Level 2 certificate and logo.

Getting Your Product PSA Certified Level 2

1. Request PSA Certified Level 2 documentation from a PSA Certified test lab or PSA JSA member (Arm, Brightsight, CAICT, Riscure, TrustCB or UL):
   - PSA Certified Level 2 Protection Profile
   - Evaluation Methodology
   - Attack Methods
   - Example Security Target (ST) and supporting evidence documents

2. Obtain an agreement (e.g. agree fees) with your chosen PSA Certified lab to evaluate your chip at PSA Certified Level 2. Your chosen lab will make an application to the Certification Body, TrustCB, and if applicable will pay the €7,500 Certification Body costs.

3. Prepare a package of information for your evaluation "Security Target and Evidence". You may wish to use the Arm MuscaB1 and TF-M example ST Word document to help you (this can be provided by a PSA JSA member).

4. Provide a physical system (Target of Evaluation) to the test lab. We recommend providing a circuit board along with PSA Functional API test results (see "Functional API step by step guide" on psacertified.org) so that the test lab has a known starting point for evaluation. PSA Certified Level 2 security assessment will involve the test laboratory performing penetration testing. The primary threat is scalable remote software attacks. Check with your test laboratory if they need access to a network interface or other method of manipulating the PSA Functional APIs (or equivalent).

5. The test lab will perform the evaluation according to the Evaluation Methodology and Attack Methods documents. They will prepare an Evaluation Technical Report (ETR) which will be shared with you and the Certification Body. If the target is judged to have passed a certificate will be issued on the PSA Certified website. The certificate has a globally unique 18-digit number (EAN-13 +5) that acts as a searchable 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 ETR to the developer.

   The test lab will send the draft digital certificate entry to the Certification Body. 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 PSA Certified website.

   If the developer has been informed that the product has passed and wants to showcase the products on the PSA Certified website they should send the following to the test lab with psacertified@trustcb.com in copy:

   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. Software version

8. Hardware version

If the developer wishes to use the PSA Certified logos and trademarks, a trademark request should be submitted.

Digital Certificate Numbers and EAN-13+5

The EAN-13 +5 is entered in the ETR by the test lab once the security evaluation is completed, considered as approved and the results are validated by the Certification Body. The test lab will also use the EAN13 +5 on the draft digital certificate they send to TrustCB for use on the PSA Certified 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 successful certification attempts, or actual certifications on the same products, 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 v1.0 this should be encoded as 0010.

If you are using Trusted Firmware-M, it comes with a reference implementation of Entity Attestation Token (EAT). EAT enables a set of claims to be made that are cryptographically signed. It is recommended that the "HW version" claim is set to the EAN-13 number from the certificate to enable relying parties to understand the security certification of the chip.

As an example:

EAT HW version = certificate EAN-13 = 6405123456789

Software is Trusted Firmware-M tag build v1.0

Digital Certificate Number entered on questionnaire /forms (case of second certification attempt and using Trusted Firmware-M v1.0): 6405123456789-20010.

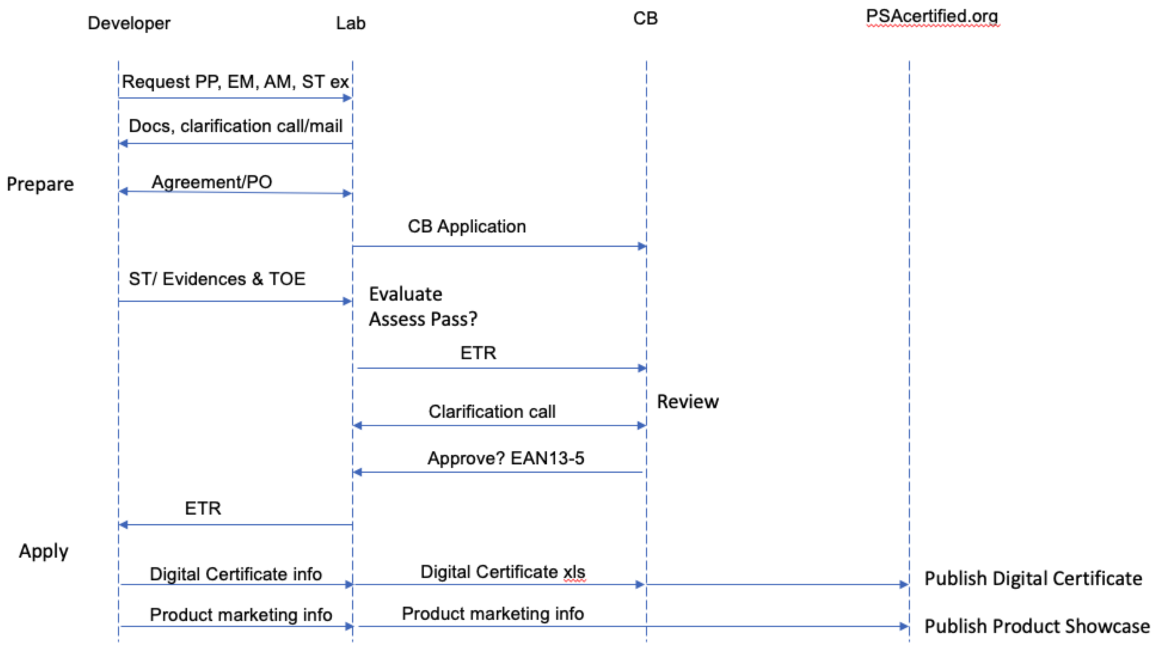

Figure 1. Process flow for PSA Certified Level 2