PSA Certified™ Level 1 Step-by-Step Guide

psacertified™
level one

Document number: JSADEN005

Version: 2.1

Author	PSA Joint Stakeholder Agreement (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: 31/03/2021

PSA Certified Level 1 Step-by-Step Guide

Getting Your Product PSA Certified Level 1

Audience: Chip vendors, System Software suppliers & OEM developers

Background

PSA Certified is an independent security evaluation scheme for chips, system software 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 evaluation laboratory.

TrustCB provides a set of independent technical experts to review the evaluation laboratory's assessment of the PSA Certified Level 1 questionnaires. This allows for harmonization of assessments across labs. The Certification Body will check that the evaluation laboratory assessment has been completed satisfactorily and then forward the spreadsheet containing the digital certificate entry to the psacertified.org administrators.

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

Which section should I fill out?

The questionnaire has three main sections: chip assessment, system software assessment and device assessment. This layering or composition approach is designed to make security certification more efficient and also reduces the workload for device manufacturers if they are using pre-certified chips or system software. Please read the description of options for evaluation and layer composition carefully to determine which section(s) you should be completing.

Getting Your Product PSA Certified Level 1

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

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

Document Number: JSADEN005

Download and complete the latest version of the PSA Certified Level 1 questionnaire from the resources page of www.psacertified.org. It is your responsibility as developer (OEM, system software vendor or chip vendor) to complete the applicable part(s) of 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 evaluation laboratory for clarifications as a Word document. Your lab may request additional supporting documentation to support the responses provided in the questionnaire. When the answers have been reviewed and agreed, sign and create the final formal version of the questionnaire to be submitted to the Certification Body. Ask the evaluation lab to send you the Certification Body application form for you to sign as the developer.

When the evaluation laboratory has reviewed the questionnaire and it has been assessed as passing the minimum threshold, they will email the certification body using psacertified@trustcb.com, with subject line "New PSA Certified Application" and attach the following:

A. Completed application form
B. Passing questionnaire
C. Test lab evaluation report
D. Spreadsheet containing pre-filled information for the publication of the certificate
E. Any relevant, additional supporting documentation

For item D, the spreadsheet, the following information will be required:

1. The revision code (the +5 digits) to use in the 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 developer will need to provide and confirm this information. It is required for the application for certification.

Once the evaluation laboratory 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".

An example product showcase can be seen in Figure 1 below.

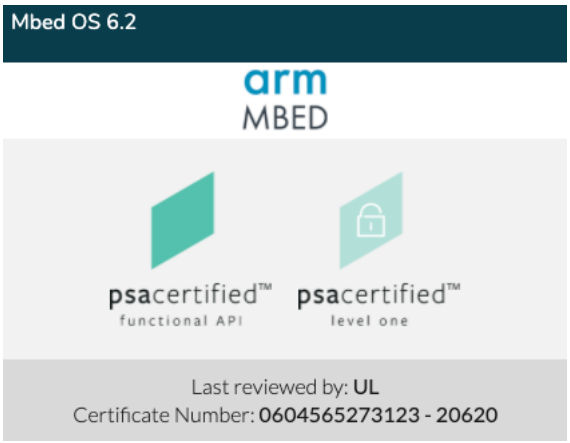

Fig.1 Certified products are showcased on the PSA Certified website

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

Note for Chip Vendors

PSA Certified Level 1 asks chip vendors questions on support of Crypto, Secure Storage and Secure Boot. This functionality is available by porting open source (e.g. Trusted Firmware-M or OP-TEE), commercial trusted firmware or your own firmware to your trusted hardware. Achieving PSA Functional API Certified by running the test suites is optional for security certification. When you have passed the PSA Certified Level 1 certification process you will 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 if you are supporting this functionality.

Digital Certificate Numbers and EAN-13+5

The globally unique 18-digit number (EAN-13+5) is provided by the Certification Body following a successful application.

The +5 digits enable encoding of firmware or software revisions and new certification attempts. The first digit of the +5 encodes the number of the certification attempts by the lab of the product, starting with '1'.

For example, if the product was evaluated as a delta certification then this leading digit of the +5 would be incremented. The following 4 digits encode the software version. As an example, if a chip developer uses Trusted Firmware-M version 2.0, this could be encoded as 0020.

As a (chip developer) example:

The PSA Certified Level 1 application is given an EAN-13 number by the Certification Body of: 6405123456789

Software is Trusted Firmware-M tag build v1.0 and it is a first certification of this product, so the +5 digits are -10010

The digital certificate number (EAN-13+5) is therefore: 6405123456789-10010

Typical Process Flow

Figure 2. shows a typical interaction between the developer and the evaluation laboratory. The lab will also liaise with the Certification Body who will make the final assessment if the product passes and issue the EAN13+5 number and digital certificate.
If the quality of responses from the developer is good there might be a couple of rounds of clarification /improvement cycles between the developer and evaluator. The whole process typically takes a few days' work spread out over a month.

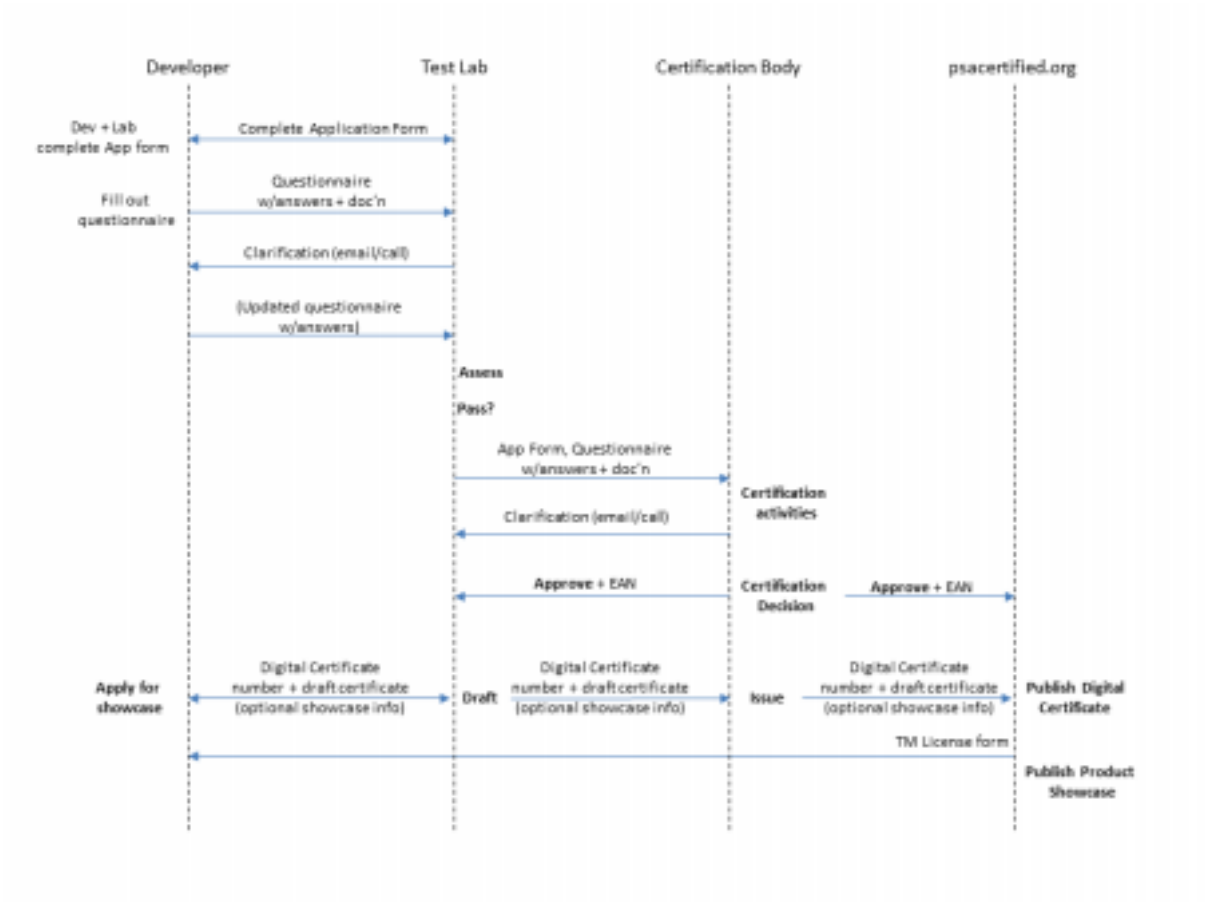

Fig.2 Process flow for PSA Certified Level 1

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third-party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at https://www.arm.com/company/policies/trademarks.

Arm Limited. Company 02557590 registered in England. 110 Fulbourn Road, Cambridge, England CB1 9NJ.