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

psacertified™

psacertified™
level one

| | |
|---|---|
| Document number: | JSADEN005 |
| Version: | 1.4 |
| Author | Arm Limited |
| Authorized by: | PSA JSA Members |
| Date of Issue: | 15/02/2019 |

© Copyright Arm Limited 2017-2019. All rights reserved.


Copyright © 2017 – 2020 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 TM 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 http://www.arm.com/company/policies/trademarks.
Copyright © 2019 Arm Limited (or its affiliates). All rights reserved. Arm Limited. Company 02557590 registered in England.
110 Fulbourn Road, Cambridge, England CB1 9NJ.

# 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. 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)


Copyright © 2017 – 2020 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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

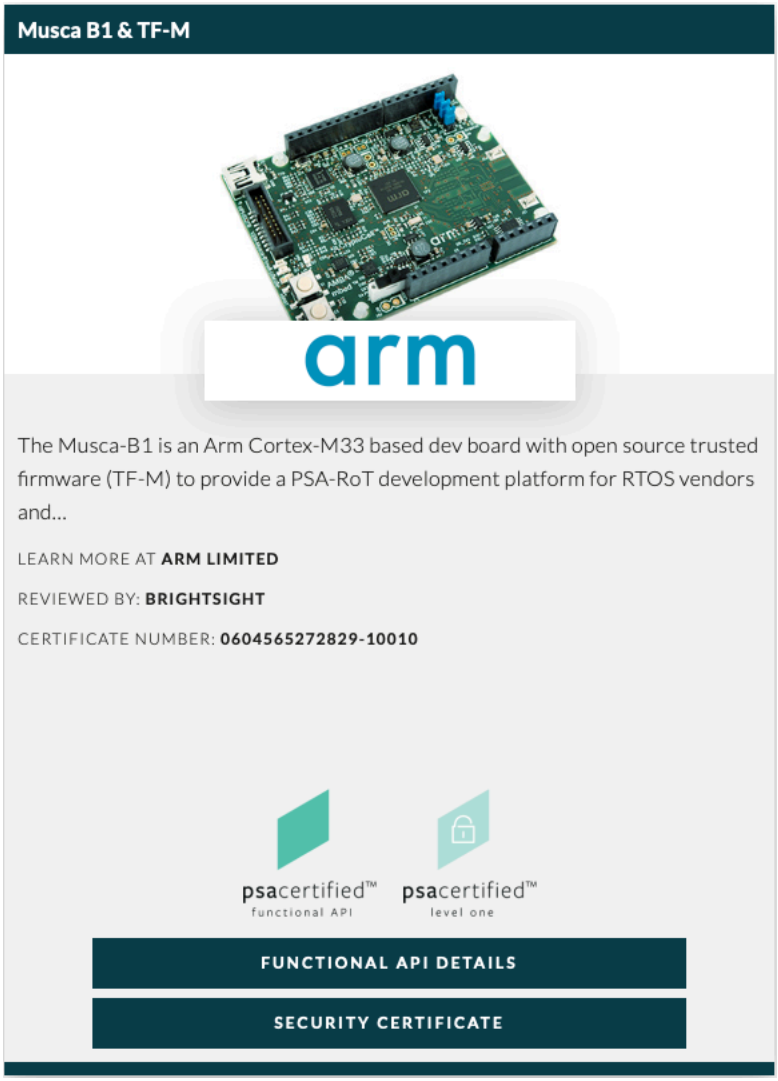


Fig 1. Certified products are showcased on www.psacertified.org

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


Copyright © 2017 – 2020 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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.


Copyright © 2017 – 2020 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

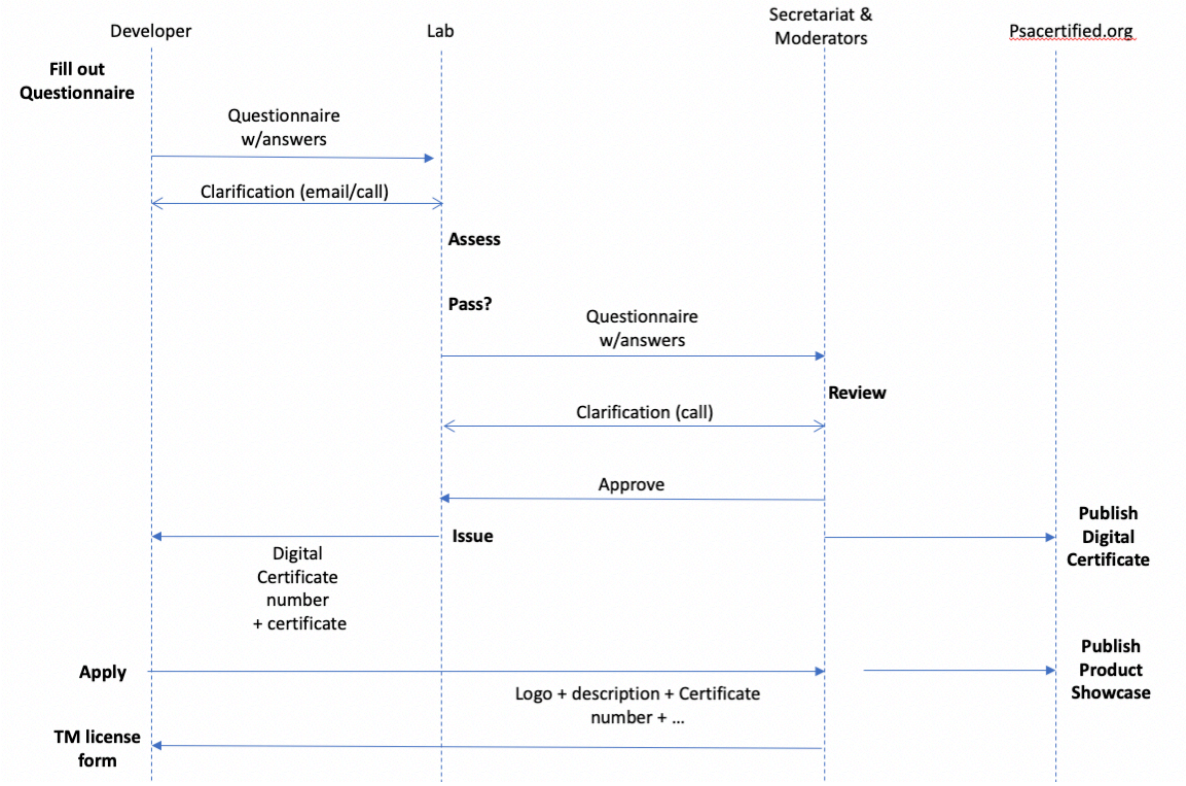


Fig 2. Process flow for PSA Certified


Copyright © 2017 – 2020 Arm Limited or its affiliates. All rights reserved.
Non-Confidential