|  |  |  |  |
| --- | --- | --- | --- |
|  | | PSA Certified™ Level 1 Evaluation Methodology Version 1.0 | |
| Document number: | JSADEN026 | |
| Version: | 1.0 | |
| Release Number: | Beta 01 | |
| Author | PSA JSA Members:  Applus+ Laboratories Arm Limited CAICT DEKRA Testing and Certification ECSEC Laboratory Inc Institute for Information Industry ProvenRun S.A.S. Riscure B.V. Serma Safety & Security S.A.S SGS Brightsight B.V. TrustCB B.V. UL TS B.V. | |
| Authorized by: | PA JSA Members | |
| Date of Issue: | 10/09/2024 | |

© Copyright Arm Limited 2017-2024. All rights reserved.

Abstract

PSA Certified is an independent security evaluation scheme for Platform Security Architecture (PSA) based chips, system software and for connected devices, including IoT, Edge devices, industrial and automotive applications. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust that provides trusted functionality to the platform. The multi-level scheme has been designed to help device makers and businesses get the level of security they need for their use case.

PSA Certified Level 1 is a test laboratory assessment of the developer’s responses to a set of security requirements that are aligned to the PSA Security Model, EN 303 645, NIST 8425 and cybersecurity regulation. **This document describes how test labs should complete their assessment of developer responses.**

Keywords

PSA Certified Level 1, Evaluation Methodology, certification, chip, connected device, internet, IoT, Platform Security Architecture, questionnaire, PSA, security, system software, device, Cyber Resiliency Act, Product Security and Telecommunications Infrastructure Act, Radio Equipment Directive, Cyber Trust Mark.

Copyright ©2017-2024 Arm Limited or its affiliates. All rights reserved. The copyright statement reflects the fact that some draft issues of this document have been released, to a limited circulation.

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 <http://www.arm.com/company/policies/trademarks>.

Copyright © 2024 Arm Limited (or its affiliates). All rights reserved.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

Contents

1 About this document 5

1.1 Current Status and Anticipated Changes 5

1.2 Release Information 5

1.3 References 6

1.4 Terms and Abbreviations 7

1.5 Feedback 9

2 Introduction & PSA Certified Overview 10

2.1 Introduction 10

2.1.1 PSA Certified Overview 10

2.1.2 PSA Certified API Certification 11

2.2 Scope for Security Evaluation 11

2.3 Roles for PSA Certified Level 1 12

2.4 Options for Evaluation and Layer Composition 12

2.4.1 Options for submission directly to the PSA Certification Body 13

2.4.2 Valid Alternative PSA Certified Chips 14

2.5 Process for PSA Certified Level 1 14

2.6 Operational Environment Assumptions 15

3 Content of Evaluation Technical Report (ETR) 16

3.1 The Evaluator shall provide content in the ETR for all the applicable parts of this section.Evaluation Identification 16

3.2 TOE Identification 16

3.3 Conformity Analysis 17

# About this document

## Current Status and Anticipated Changes

Current Status: v1.0 Beta 01

## Release Information

The change history table lists the changes that have been made to this document.

| Date | Version | Confidentiality | Change |
| --- | --- | --- | --- |
| 10/09/2024 | 0.3 Alpha 01 | Non-confidential | Cleaned up document and added JSADEN reference |
| 10/29/2024 | 1.0 Beta 01 | Non-confidential | Version 1.0 Beta released for use |
|  |  |  |  |
|  |  |  |  |

## References

This document refers to the following informative documents.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref | Doc No | Author(s) | Title | |
|  | JSADEN 0014 | Arm, PSA JSA | Platform Security Model |
|  | EN 303 645 | ETSI | Cyber Security for Consumer Internet of Things; V2.1.1 (2020-06) |
|  | NISTIR 8259A | NIST | IoT Device Cybersecurity Capability Core Baseline; May 2020 |
|  | JSADEN001 | Arm, PSA JSA | PSA Certified Level 1 v3.1 |

## Terms and Abbreviations

This document uses the following terms and abbreviations.

|  |  |
| --- | --- |
| Term | Meaning |
| Application Root of Trust Service(s) | Application specific security service(s) that are not defined by PSA. Such services execute in the Secure Processing Environment and are required to be in Secure Partitions. |
| Application Specific Software | Software that provides the functionality required of the specific device. This software runs in the Non-Secure Processing Environment, making use of the System Software, Application RoT Services and PSA-RoT Services. |
| Best Practice Cryptography | Use of cryptographic algorithms, modes and protocols, key generation and random number generation approved by a government or by an industry body in the intended deployment market(s). Use of cryptographic algorithms with a cryptographic strength suitable for the expected lifetime of the device should be used. Where possible, the ability to change the algorithms in use should be considered. |
| Critical Security Parameter | Secret information, with integrity and confidentiality requirements, that is used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc. Critical Security parameters are considered to be Sensitive Data. In some contexts, these data are classed as assets. |
| Evaluation Laboratory | Laboratory or facility that performs the technical review of questionnaires submitted for Level 1 PSA certification. The list of evaluation laboratories participating to PSA Certified can be found on [www.psacertified.org](http://www.psacertified.org) |
| Evaluation Technical Report (ETR) | A report that documents the overall verdict and its justification, produced by the evaluator and submitted to an evaluation authority |
| Factory Reset | Factory reset means reset to any state that might be as delivered from the manufacturer, for example, including any manufacturer provided updates after the initial delivery of the device. |
| Hardware Unique Key (HUK) | Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a critical security parameter. |
| Non-secure Processing Environment (NSPE) | The processing environment that executes the non-secure System Software and Application Specific Software. PSA requires the NSPE to be isolated from the SPE. Isolation between partitions within the NSPE is not required by PSA though is encouraged where supported. |
| Partition | The logical boundary of a software entity with intended interaction only via defined interfaces, but not necessarily isolated from software in other partitions. Note that both the NSPE and SPE may host partitions. |
| PSA | Platform Security Architecture |
| PSA Certification Body | The entity that receives applications for PSA security certification, issues certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories. |
| PSA Certified API | PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation. |
| PSA Certified API Certification | Functional certification confirms that the device implements the PSA Certified APIs correctly by passing the PSA Certified API Certification test suites. |
| PSA Root of Trust (PSA-RoT) | The PSA defined combination of the Immutable Platform Root of Trust and the Updateable Platform Root of Trust, and which is the most trusted security component on the device. See [1]. |
| Immutable Platform Root of Trust | The minimal set of hardware, firmware and data of the PSA-RoT, which is inherently trusted because it cannot be modified following manufacture. There is no software at a deeper level that can verify that it as authentic and unmodified. |
| Updateable Platform Root of Trust | The firmware, software and data of the PSA-RoT that can be securely updated following manufacture. |
| Personally Identifiable Data | Information that relates to an identified or identifiable individual. Such data is considered to be Sensitive Data if disclosure or modification causes harm to the identified individual. |
| Platform Root of Trust Service(s) | PSA defined security services for use by PSA-RoT, Application RoT Service(s) and by the NSPE. Executes in the Secure Processing Environment and may use Trusted Subsystems. This includes the services offered by the PSA Certified APIs. |
| Secure Partition | A Partition in the Secure Processing Environment. |
| Secure Processing Environment Partition Management | Management of the execution of software in Secure Partitions. Typical implementations will provide scheduling and inter-partition communication mechanisms. Implementations may also enforce isolation between the managed Secure Partitions. |
| Secure Processing Environment (SPE) | The processing environment that executes the PSA-RoT, the PSA-RoT Services, and any Application RoT Service(s). |
| Secure Boot | The process of verifying and validating the integrity and authenticity of updateable firmware and software components as a pre-requisite to their execution. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded, which may extend the NSPE secure boot chain further. |
| System Software | NSPE software that may comprise an operating system or some run-time executive, together with any middleware, standard stacks and libraries, chip specific device drivers, etc., but not the application specific software. |
| Sensitive Data | Any data that if, for example, is disclosed or modified, could result in a device vulnerability, jeopardize any service that relies on it, or cause harm to an identifiable individual. |
| Trusted subsystem | A security subsystem that the PSA-RoT relies on for protection of its critical security parameters, or that implements some of its services. |

## Feedback

The PSA JSA Members welcome feedback on its documentation.

If you have comments on the content of this documentation, send an e-mail to psacertified@arm.com. Give:

* The title (PSA Certified Level 1 Evaluation Methodology).
* The number (JSADEN-026) and version.
* The page numbers to which your comments apply.
* The rule identifiers to which your comments apply, if applicable.
* A concise explanation of your comments.

PSA JSA Members also welcome general suggestions for additions and improvements.

Note: PDFs are tested only in Adobe Acrobat and Acrobat Reader and cannot guarantee the appearance or behavior of any document when viewed with any other PDF reader.

# Introduction & PSA Certified Overview

## Introduction

This document is the result of the cooperation of PSA JSA group of companies, it provides guidance (in section 3) on how to proceed to the evaluation of a TOE according to Level 1 of PSA Certified scheme. This document describes the elements that the Evaluator shall include in its Evaluation Technical Report (ETR).

This document is directly aimed at Evaluation Laboratories, who perform PSA Certified Level 1 evaluations according to the security requirements of JSADEN001 [4].

This document describes the mandatory sections expected in the Evaluation Technical Report and the content the Evaluator is expected to provide for each of them.

### PSA Certified Overview

PSA defines a common hardware and software security platform, providing a generic security foundation allowing secure products and features to be deployed.

The PSA Certified scheme involves the mandatory evaluation against a set of security requirements by an Evaluation Laboratory. The evaluation laboratory examines security measures to ensure that the device, including its critical security parameters, is not vulnerable to identified threats.

The scheme recognizes that there will be different security requirements and different cost and security trade-offs for different applications and ecosystems. This is reflected in specifications by introducing a range of *assurance levels*.

PSA Certified Level 1 assurance, the target of this document, relies on questionnaires filled out by the Chip vendor, the System Software vendor or the Device OEM. The questionnaires defined in this document cover the baseline security requirements to mitigate common threats and security requirements for PSA based products. The Evaluation Laboratory relies on this questionnaire to examine the security measures.

Example answers for the questions can be found in the web-based version of this document, which can be found at [certify.psacertified.org](https://certify.psacertified.org/).

In the case of a successful evaluation a digital certificate is issued by the PSA Certification Body for that certification, which can optionally be published on [www.psacertified.org](http://www.psacertified.org). The certificate number is a globally unique EAN-13 number that can be supplied by the Evaluation Laboratory or by the company seeking certification. PSA devices that support, for example, an IETF Entity Attestation Token[[1]](#footnote-2) can include the EAN-13 to inform relying parties that the chip, system software or device has been evaluated and is PSA Certified.

### PSA Certified API Certification

PSA Certified APICertification, which is optional, means that a device has implemented the [PSA Certified API](https://pages.arm.com/psa-apis.html)[[2]](#footnote-3) and passed the PSA Certified APICertification test suites. The PSA Certified APIs cover three security functions: Attestation, Cryptography and Secure Storage. A step-by-step guide for getting a product PSA Certified APIcertified is available on [www.psacertified.org/resources](http://www.psacertified.org/resources).

## Scope for Security Evaluation

There are three evaluation scopes: the chip, the system software and the device. The security evaluation covers the combination of the hardware and software components. Figure 1 illustrates the typical components in the PSA architecture and the related evaluation scopes. This figure distinguishes a Non-secure Processing Environment (NSPE) and a Secure Processing Environment (SPE), for which the Chip level shall provide isolation[[3]](#footnote-4).



Figure 1: Logical Scope of Chip, System Software and Device Levels

The Chip security evaluation scope includes the following Secure Processing Environment PSA-RoT elements, see also [1]:

* Immutable Platform Root of Trust, for example, the Boot ROM, any root parameters, the NSPE/SPE isolation hardware, and any hardware-based security lifecycle management and enforcement.
* Updateable Platform Root of Trust, for example, a main bootloader, the code that implements the SPE Partition Management function, the code that implements the PSA defined services[[4]](#footnote-5) such as attestation, secure storage, and cryptography.
* Any Trusted subsystems that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

The Chip scope hardware may be a System-on-Chip or a System-in-Package, possibly supported by board level trusted subsystem components, for example, a Secure Element or Subscriber Identification Module.

The System Software in the scope of the security evaluation executes in the Non-secure Processing Environment. System Software evaluation dependencies on the Chip layer are detailed in section 2.4.

For the Device, the scope of the security evaluation includes the following software components:

* Applications and any other software developed by the OEM. These may execute in the Non-Secure Processing Environment or as Application Root of Trust Services in the Secure Processing Environment
* Configuration of the System Software for the device.

Device evaluation dependencies on the System Software and Chip layers are detailed in section 2.4.

## Roles for PSA Certified Level 1

PSA Certified Level 1 involves the following roles:

* Chip Vendor: Develops the chip, the immutable and updateable parts of the PSA-RoT (including any trusted subsystems).
* System Software Vendor: Develops the system software for the Non-secure Processing Environment.
* Device OEM: Conceives and develops a device based on the PSA specifications.
* Evaluation Laboratory: Performs the technical review of questionnaire(s) submitted for PSA Certified Level 1 and if successful provides a digital certificate reference number (EAN-13) for the applicable evaluation scope.
* Certification Body: The entity that receives applications for PSA certification, issues certificates, maintains the security certification scheme, and ensures consistency across the evaluation laboratories.

## Options for Evaluation and Layer Composition

The purpose of PSA Certified Level 1 is to assess the security foundation of a device. The certification scheme is organized in layers: device, on top of the system software, on top of the chip. The certificate for a given layer is only applicable if the lower layers have either been separately evaluated and hold a PSA L1 certificate or, if not, are covered in the evaluation that leads to the considered certificate. The evaluation options are as follows:

1. Chip evaluation can proceed independently of the other layers. Section 4 must be filled in.
2. System Software evaluation can proceed with one of the following:
   1. with a PSA Certified chip. Section 5 must be filled in and section 3.3 must give the chip EAN-13.
   2. with an uncertified chip the evaluation must also include the chip part. Sections 4 and 5 must be filled in. Note that an independent certificate for the chip will not be issued.
3. Device evaluation can proceed with one of the following:
   1. on PSA Certified system software with either:
      1. a valid PSA Certified chip other than that declared in the system software certificate; see section 2.4.2 on validity. Section 6 must be filled in and section 3.3 must give the system software EAN-13 and the PSA Certified chip EAN-13. Section 3.8 also must be filled in.
      2. the chip declared in the system software certificate. Section 6 must be filled in and section 3.3 must give the system software EAN-13, and the named chip. If the named chip is PSA Certified, section 3.3 must give the chip EAN-13.
   2. on uncertified system software with a PSA Certified chip. The evaluation must include the system software part. Sections 5 and 6 must be filled in and section 3.3 must give the EAN-13 of the PSA Certified chip. An independent certificate for the system software will not be issued.
   3. if the chip is neither a valid PSA Certified chip (it does not have its own certificate) nor the chip named in any certificate for the System Software[[5]](#footnote-6) then the evaluation must include both the system software and the chip parts. Sections 4, 5 and 6 must be filled in. Note that independent certificates for the system software and for the chip will not be issued.

Certification of a device requires the device vendor to confirm that the device and any device vendor configuration of the system software results in the correct use of the PSA-RoT. Confirmation is accessed via the device Developer responses in section 6. The optional PSA Certified APIcertification can help in this process. Device evaluation is performed with a specific system software and chip combination, and the resulting device certificate is valid for that combination only.

From version 3.0 of JSADEN001 [4], the vendor may choose to have their solution evaluated in the context of the regulations covered in section 7. In this case, the vendor must complete the required part or parts of section 7.

### Options for submission directly to the PSA Certification Body

Where a product is developed from one already PSA Certified and the exact same questionnaire answers and declarations are applicable, then section 3.7 can be completed instead of the sections stated above and submitted directly to the PSA Certification Body. Checking for acceptability with the PSA Certification Body or chosen Evaluation Laboratory is recommended. Section 3.7 can be used in the following situations:

* a new Chip uses the same certified PSA-RoT implementation,
* updated certified System Software on the same Chip declared in the referenced certification,
* a new device using the same System Software and Chip declared in the referenced certification.

### Valid Alternative PSA Certified Chips

Flexible composition via 3)a)i) above relies on the interchangeability of the chip level PSA-RoT. Typically, this means that the alternate PSA Certified chip must support at least the same PSA-RoT functionality as the chip named in the System Software certificate. In practice, this likely means that all the requirements in section 4 must be met. PSA Certified APICertification can be used as evidence of interchangeability.

If the PSA Certified System Software relies on chip-level security functionality in addition to that required for the PSA-RoT then the alternative chip must provide at least the same additional functionality. In practice, this is likely to mean that such compositions may be difficult and the alternative chip will need to be covered by its own certification.

The full rules on validity can be found at [www.psacertified.org/getting-certified/silicon-vendor/overview/level-1/questionnaire-composition](http://www.psacertified.org/getting-certified/silicon-vendor/overview/level-1/questionnaire-composition).

## Process for PSA Certified Level 1

The process for Level 1 certification is the following:

1. The Chip Vendor, the System Software Vendor or the Device OEM (all named Developer below) complete the relevant questionnaire provided in sections 4, 5, 6 or 7 as specified in section 2.4. It is recommended that the Developer also complete the assessable organizational best practices questions in Appendix A1.
2. For each requirement in the relevant section, a single box corresponding to the fulfilment of the requirement is ticked (or marked in an equivalent way) as follows, note that a gray box means that answer is not acceptable. All guidance given in italic should be deleted.
   * Yes: for full compliance with the requirement, the Developer describes how this requirement is met according to any guidance given *in italic*.
   * Partial: for partial compliance with the requirement, the Developer describes how the requirement is partially met according to any guidance given *in italic* and what impact that has on the security.
   * N/A: where the requirement is not applicable for one of the following reasons, the Developer must in all cases provide a rationale:

* the required feature is not supported (typically those requirements that start with “if”), or
* is an Optional requirement and is not included.

1. The Developer fills the assessment information part in Section 3 and submits the applicable questionnaire(s), according to the selected scope of evaluation, to an Evaluation Laboratory.
2. The Evaluation Laboratory performs the technical review by checking that the rationale given for each requirement is consistent with the statement of the requirement. The Evaluation Laboratory may ask for clarification. The Evaluation Laboratory submits an application to the PSA Certification Body on behalf of the Developer. The Evaluation Laboratory also confirms the unique 5 digit reference to append to the EAN-13 certificate number that will be issued by the PSA Certification Body.
3. The PSA Certification Body will provide an EAN-13 for the relevant Chip, System Software or Device certification (see section 2.4).
4. The PSA Certification Body proceeds to the certification of the product and the EAN-13 is published along with product reference on the Certification Body website.

The pass threshold for each section of Chip, System Software or Device is at most one (1) question not answered in conformance with the “Expected answer” on the marking sheet of Appendix D with a rationale of why security is unaffected. Requirements marked as Optional must not be considered in the count.

For a variant of an existing certified product, the Developer can reuse the questionnaire that was reviewed by the Evaluation Laboratory provided exactly the same answers and declarations apply (see section 3.7). In that case, no action from an Evaluation Laboratory is required and the Developer only has to submit an application to the PSA Certification Body and outline how the changes do not impact the security relative to the original certified product. The EAN-13 for the new product will differ from the product already certified.

## Operational Environment Assumptions

The following assumptions hold regarding the operational environment of the device target of the evaluation:

* The device manufacturing process ensures integrity and authenticity of the hardware design and any software components.
* Generation, storage, distribution, destruction, injection of secret data in the device enforces integrity and confidentiality of these data. In particular, private and symmetric keys are not shared among devices.
* The device and related software, including third-party libraries, is subject to a vulnerability watch and a responsible disclosure program. Vulnerabilities are subject to timely security patches and customers notified.
* The OEM has performed a risk assessment for the applications supported by the device to identify and protect assets used by the device, has followed coding best practices, and has performed functional testing.

# Content of Evaluation Technical Report (ETR)

## The Evaluator shall provide content in the ETR for all the applicable parts of this section.Evaluation Identification

|  |  |
| --- | --- |
| **RTE reference:** | *(Unique reference)* |
| **RTE version:** |  |
| **Authors:** | *(Name of the evaluators involved for this product)* |
| **Approved by:** |  |
| **Last update:** |  |
| **Notes:** | *(optional notes)* |

## TOE Identification

|  |  |
| --- | --- |
| **Commercial name:** | *(e.g. Product family)* |
| **Chip part number:** |  |
| **Chip version:** | *(e.g. Chip silicon revision)* |
| **SPE name:** | *(e.g. Trusted Firmware-M)* |
| **SPE version:** |  |

The Evaluator shall verify that the identification of the TOE as specified in the Questionnaire JASDEN0001 [4] is non ambiguous.

The Evaluation Technical Report (ETR) shall also include:

* Unique report reference: A combination of alphanumeric characters that make the report identifiable in the Evaluator organisation
* Date of report
* Page numbers including identification of the total number of pages.

## Conformity Analysis

For L1 evaluation a single evaluation review phase is performed in which the evaluator assesses the information provided in the completed questionnaire. The Evaluator writes a short ETR to show their assessment of the Vendor’s questionnaire answers against the L1 requirements**.**

For each requirement in the questionnaire the Evaluator will provide:

* Indication of whether the requirement is met, partially met or is not applicable.
* An adequate description of why the Evaluator has indicated the result for each requirement based on the information provided in the questionnaire.

The Evaluator shall check the developer answers against the requirements in the developer-provided, completed Questionnaire JASDEN0001 [4]. The evaluator shall provide an assessment for each developer response and confirm that it meets or does not meet the questionnaire requirement. The Evaluator shall provide a reason for any positive or negative assurance made about the Developer Questionnaire responses.

The marking scheme for section 7 requires all mandatory requirements in any completed subsection (e.g. 7.1 “PSTI”, 7.2 “CRA” or 7.3 “RED”) to be answered “Yes” with a description of how the requirements are met or N/A with a description of why the requirement is not applicable to the TOE. The Evaluator shall also check that the completed JASDEN0001 [4] Questionnaire includes a reference to evidence showing how the requirement is met or is not applicable. This could be a reference in a technical manual, design spec or similar. This will assist in demonstrating the sufficiency of the response to a Notified Body.

For each completed section in the questionnaire (Chip, Software Platform, Device) the Evaluator will provide:

* A marking sheet showing the level of conformance to the expected criteria in Appendix D of JASDEN0001 [4].
* For each section in Appendix D of JASDEN0001 [4], all answers to “Supported: Yes, Partial, N/A” must be as expected, according to the marking sheet. The developer can answer one question per section that deviates from this rule if a rationale is supplied of why security is unaffected for the product under evaluation.

There is no product testing required as part of the L1 assurance activities. As such, no testing of the product is planned. The only intended work is the assessment of the documentation evidence (completed JASDEN0001 [4] Questionnaire) provided by the Developer.

1. <https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/> [↑](#footnote-ref-2)
2. <https://developer.arm.com/architectures/security-architectures/platform-security-architecture> [↑](#footnote-ref-3)
3. The isolation between the Non-Secure Processing Environment and the Secure Processing Environment can be implemented using, for example, TrustZone, using dual cores, or via processor privilege levels. [↑](#footnote-ref-4)
4. The Updateable Platform Root of Trust may also execute any Application specific Root-of-Trust services, but these are not in the scope of a Chip certification. [↑](#footnote-ref-5)
5. A System Software certificate is only applicable with a valid PSA Certified chip, or the chip named in the certificate. [↑](#footnote-ref-6)