psacertified™

PSA Certified Level 2 Evaluation Methodology Version 1.1

psacertified™
level two

Document number:	JSADEN003
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:	18/02/2020

Abstract

PSA Certified is the independent security evaluation scheme for Platform Security Architecture (PSA) based IoT systems. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust (PSA-RoT) 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 2 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against scalable software attacks. The Level 2 documents include: a Protection Profile (PP) that describes the Target of Evaluation, its assets, the security objectives and security functions that will be evaluated; an Evaluation Methodology (EM) that details how the evaluation will be carried out, and an Attack Methods (AM) document describing the attacks in scope.

Developers submit their PSA-RoT to an approved test laboratory, listed on **www.psacertified.org**, for Level 2 evaluation and receive an Evaluation Technical Report. If the PSA-RoT is assessed as passing and approved by the independent Certification Body, a digital certificate will be issued on the PSA Certified website.

Keywords

PSA Certified Level 2, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

Contents

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Final

1.2 Release Information

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

Date	Version	Confidentiality	Change
18/02/2020	1.1	Non-confidential	Clarifications for PSA L2 Ready and new template
25/09/2019	1.0	Non-confidential	Initial version, approved by JSA members

1.3 References

This document refers to the following informative documents.

1.3.1 Normative references

Ref	Doc No	Author(s)	Title
[PSA-AM]	JSADEN004	ARM JSA	PSA Certified: Attack Method
[PSA-L1]	JSADEN001	ARM JSA	PSA Certified: Level 1 Questionnaire
[PSA-PP]	JSADEN002	ARM JSA	PSA Certified Level 2 Lightweight Protection Profile

1.3.2 Informative references

Ref	Doc No	Author(s)	Title
[GP-ROT]	GP_REQ_025	GlobalPlatform	Root of Trust Definitions and Requirements, Version 1.1, Public Release, June 2018
[PSA-FF]	ARM DEN 0063A	ARM	ARM® Platform Security Architecture Firmware Framework and RoT Services – M-profile
[PSA-SM]	ARM DEN 0079	ARM	PSA: Device Security Model

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations

Term	Meaning
Application firmware	The main application firmware for the platform, typically comprising a System software and application tasks. PSA provides no isolation services for this firmware, although the System software may make use of available hardware support to provide internal isolation of operation
Application Root of Trust	This is the security domain in which additional security services are implemented. See *PSA Security Model* [PSA-SM] for details
Application Root of Trust Service	This is a Root of Trust Service within the Application Root of Trust domain
Evaluation laboratory	Laboratory or facility that performs the technical review of questionnaires submitted for PSA Certified Level 1. The list of evaluation laboratories participating to PSA Certified can be found on www.psacertified.org
JTAG	Joint Test Action Group
Hardware Unique Key (HUK)	Secret and unique to the device – this symmetric key must not be accessible outside the PSA Root of Trust
Non-secure Processing Environment (NSPE)	This is the security domain outside of the SPE, the Application domain, typically containing the application firmware and hardware
PSA	Platform Security Architecture
PSA Certification Body	Entity that receives applications for PSA security certification, issues certificates, updates security certification scheme
PSA Functional APIs	Foundations from which security services are built, allowing devices to be secure by design. Three sets of APIs have been defined, so far, and include Crypto, Secure Storage and Attestation
PSA Functional API Certification	Functional certification for a device that ensures that the device has implemented PSA Functional APIs and passed the PSA Functional certification Test Suites
PSA Immutable Root of Trust	The hardware and code and data that cannot be modified following manufacturing. See *PSA Security Model* [PSA-SM] for details
PSA Root of Trust	This defines the most trusted security domain within a PSA system. See *PSA Security Model* [PSA-SM] for details
PSA Root of Trust Service	This is a Root of Trust Service within the PSA Root of Trust domain
Root of Trust (RoT)	This is the minimal set of software, hardware and data that is implicitly trusted in the platform – there is no software or hardware at a deeper level that can verify that the Root of Trust is authentic and unmodified. See *Root of Trust Definitions and Requirements* [GP-ROT]

Root of Trust Service (RoT Service)	A set of related security operations that are implemented in a Secure Partition. The server endpoint of a PSA IPC channel. Multiple RoT Services can co-exist in a single Secure Partition
Secure Partition	A thread of execution with protected runtime state within the Secure Processing Environment. Container for the implementation of one or more RoT Services. Multiple Secure Partitions are allowed in a platform
Secure Partition Manager (SPM)	The part of a PSA implementation that is responsible for isolating software in partitions, managing the execution of software within partitions, and providing IPC between partitions
Secure Processing Environment (SPE)	A platform's processing environment for software that provides confidentiality and integrity for its runtime state from software and hardware outside of the SPE
SiP	System in Package
SoC	System on Chip
Secure boot	Secure boot is technology to provide a chain of trust for all the components during boot
System software	NSPE software that may comprise a Real-Time Operating System (RTOS) or some other run-time executive, middleware, standard stacks, chip specific device drivers, etc., but not the application specific code
Trusted subsystem	Any trusted component outside of the functional scope of the PSA Root of Trust but within the trust boundary of the PSA Root of Trust. For example, DDR protection system, trusted peripherals, SIM or TPM

1.5 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 2 Evaluation Methodology).
- The number (JSADEN-003) 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 behaviour of any document when viewed with any other PDF reader.

2 Introduction

2.1 Document Context

This document is the result of the cooperation of PSA JSA group, comprising ARM and evaluation labs. It provides guidance on how to proceed to the evaluation of a TOE according to Level 2 or Level 2 Ready (see Section 2.3) of PSA Certified scheme. In particular, this document describes the elements that the Evaluator shall include in its Evaluation Technical Report (ETR).

2.2 Targeted Audience

This document is directly aimed at Evaluation Laboratories, who perform PSA Certified Level 2 or PSA Certified Level 2 Ready evaluations according to the security requirements set in [PSA-PP].

It can also be used by Chip Vendors, who develop the chip and the PSA components for the Secure Processing Environment, so as to understand the criteria used by Evaluation Laboratories to perform product evaluation.

2.3 PSA Certified Level 2 Ready Evaluation

This document considers a pre-certification evaluation of FPGA or development based systems, which provide reference designs for ASIC or custom chip but which may not be able to meet all nine security functions of the protection profile [PSA-PP]. In this case, only the claimed security functions are tested by the Evaluation Laboratory who issues the Evaluation Technical Report. No Level 2 certificate is generated for a Level 2 Ready evaluation but the Developer can obtain the rights to use a specific "PSA Certified Level 2 Ready" logo and showcase its solution on www.psacertified.org .

Such a logo could be used to demonstrate, for example, the benefit of software security assurance offered from an evaluated FPGA based system for development of secure AROTs, RTOS or device while maximizing chances of passing PSA Certified Level 2 certification for future ASIC or custom chips based on the FPGA reference design.

2.4 How to Use this Document

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

2.5 Input for Evaluation

According to Developer Evidences required in PSA Level 2 Protection Profile [PSA-PP], the expected input for Evaluation Laboratories to start and evaluation are:

- Security Target based on [PSA-PP].
- Functional specification and/or Operational guidance, explaining how to use functions and services provided by the TOE and describing all external interfaces or physical input or output of the TOE.
- Installation guidance, explaining how to prepare the TOE for operational phase, including how to personalize device prior use.
- User and security documentation of additional trusted subsystem, if used.

- Answers to PSA Certified Level 1 Questionnaire [PSA-L1] for the TOE (Chip Vendor Section).
- Test results for PSA Functional API Certification, including TOE setup for these tests.
- Source code for the components in scope of the TOE
- TOE test equipment if they are specific or dedicated.

2.6 Evaluation Workload

The workload for performing the evaluation of a TOE according to Level 2 of PSA Certified scheme is 25 man-days. It is assumed for this workload that no additional security function is added in the Protection Profile.

The workload for a PSA Certified Level 2 Ready evaluation, less that 25 man-days depending on the implemented security functions, has to be agreed between the Evaluation Laboratory and Certification Body prior the evaluation.

The Evaluation Laboratory can propose to reduce the workload in case of a re-evaluation or delta evaluation of a previously certified TOE. The Developer shall provide to the Evaluation Laboratory an *Impact Analysis Report* (IAR) that analyses of the impact of changes to the certified TOE. The resulting assurance for this TOE subject to re-evaluation or delta evaluation shall be the same as if the TOE had never been evaluated before and was subject to a complete evaluation.

3 Content of Evaluation Technical Report

3.1 Evaluation Identification

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

3.2 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 Security Target is non ambiguous and can be retrieved from the TOE.

3.3 Product Description

The Evaluator shall complete the following sub-sections based on the documentation provided by the Developer, as stated in Section 2.5.

3.3.1 Intended Usage

The Evaluator shall identify the intended usages for products including the TOE.

3.3.2 Operational Environment

The Evaluator shall identify:

- The context in which the TOE shall be used;
- The non-TOE Hardware, Software or Firmware required to operate the TOE. However, the TOE must be realized in a way such that TOE security functionalities do not rely on proper behavior of non-TOE hardware, software or firmware.

When the technical operational environment for the TOE as described in the Security Target is generic or covers different types of platforms for non-TOE Hardware, Software or Firmware, the Evaluator shall select one platform to perform testing of the TOE and identify it on the ETR.

3.3.3 Hardware and Software Interfaces

The Evaluator shall describe the hardware and software interfaces provided by the TOE and that can be used to interact with the TOE.

3.3.4 Security Features

The Evaluator shall describe the security features implemented by the TOE, and that will the subject of evaluation. He will rely on the product documentation, including the Security Target, and on source code of the TOE.

The security features shall be related to the intended usage of the TOE.

For evaluation of FPGA based system according to PSA Certified level 2 Ready evaluation, the Developer will describe precisely in the Security Target which hardware security features are absent or emulated, that will not be evaluated.

3.4 TOE Installation

The Evaluator shall describe the hardware and environment used to test installation of the TOE.

The Evaluator shall follow the installation guidance provided by the Developer and check that:

- It is clear and sufficient for installation for the TOE;
- Consistent with the intended usage and operational environment of the TOE;
- It does not contain or miss instructions that could lead to an insecure configuration of the TOE.

3.5 Conformity Analysis

The Evaluator shall check conformance of the Security Target (ST) with [PSA-PP]. In particular the ST shall include all assets, threats and security functions of the PP. If some of these elements are missing, the Evaluator shall check rationale provided by the Developer. If new elements are added, the Evaluator shall check consistency with the rest of the PP.

The Evaluator shall analyse the documentation provided by the Developer, in particular the one related to security functions included in the ST, and check that the description of the security functions is conformant with what is described in the ST and what is present in the source code of TOE.

The Evaluator shall review source code for the TOE and provide its expert opinion on the readability and structuration of the code (comments, modularity, portability, use of a type system…). The Evaluator may proceed by sampling, on a risk-based approach, if the volume of source code is too large for the allocated evaluation workload.

The Evaluator shall check that the product implements the security functions according to their description. He shall rely for this purpose on the output of the PSA Functional API Certification or on the Developer functional testing results.

For PSA Certified level 2 Ready evaluation, the Evaluator shall check that the guidance documentation clearly states the limitations due to not implemented or partially implemented security features, with considerations regarding the alternative implementation if provided (for instance, what is used instead of a boot ROM).

3.6 Vulnerability Analysis

The Evaluator shall perform vulnerability analysis on the TOE. He may rely for this purpose on the source code of the TOE. For the identification of the classes of attacks that can be performed on the TOE, the Evaluator shall refer to [PSA-AM].

For evaluation of FPGA based system according to PSA Certified Level 2 Ready evaluation, the Evaluator shall select, perform and declare in the ETR the applicable attack methods according to [PSA-AM] and the security features supported by the TOE. The missing security features due to limitation of FPGA based will be evaluated in the further PSA Certified level 2 evaluation.

3.6.1 Known or Potential Vulnerabilities

The Evaluator shall identify known or potential vulnerabilities applicable to the TOE. This can be for instance vulnerabilities already reported in public databases (such as CVE) for libraries included within the TOE, security updates for CPU or Hardware from Vendors, or vulnerabilities applicable to similar TOEs.

The Evaluator shall check for each known or potential vulnerability if it can be triggered from the TOE hardware and software interfaces.

3.6.2 Tested Vulnerabilities

The Evaluator shall proceed to penetration testing of the TOE based on the output of the vulnerability analysis. Considering that not all tests may be performed in the allocated workload for the evaluation, the Evaluator shall provide a rationale for the selected tests.

3.6.3 Scoring of Vulnerabilities

For the quotation of the vulnerabilities, the Evaluator shall refer to [PSA-AM].

The Evaluator may provide to the Developer observations or remarks on weaknesses of TOE security functions and possible options to consider to improve resistance to attacks.

3.7 Developers Interview

The Evaluator may contact Developers of TOE to obtain further information on the TOE, its usage and security functions if the Developer documentation is not detailed enough.

3.8 Summary

The Evaluator summarizes the output of its different evaluation tasks and provides its expert opinion on:

- The resistance to attacks of each TOE security function.
- The global resistance to attacks of the TOE with a judgement if the device should pass.

For the PSA Certified Level 2 Ready evaluation, the Evaluator shall clearly reminds all unavailable security features in the ETR as well as possible limitations of the evaluation due to the characteristics of the TOE. For reuse of evaluation results in a PSA Certified Level 2 evaluation of a full product based on the design of the FPGA system, the Evaluator will have to check that implementation of already evaluated security features are unchanged in the full product and to complete all remaining tasks for security features that were unimplemented or incomplete.

Non-Confidential Proprietary Notice

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