PSA Certified™ Level 2 Lightweight Protection Profile

Document number:	JSADEN0002	Version:	BET02
Date of Issue:	25/02/2019		
Author:	PSA JSA Members: Arm Limited Brightsight B.V. CAICT Prove & Run S.A.S. Riscure B.V. UL TS B.V.		
Authorized by:	PSA JSA Members		

Abstract

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 multi-level assurance program for chips containing a security domain called a Root of Trust (PSA-RoT) that provides trusted functionality to the platform. This document describes the PSA Certified Level 2 scheme for chip vendors. It defines the scope and security requirements for test lab based evaluation of a TOE implementing the PSA architecture.

Keywords

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

Non-Confidential Proprietary Notice

Contents

1 ABOUT THIS DOCUMENT 6

1.1 Current status and anticipated changes 6

1.2 Change history 6

1.3 References 6

1.4 Terms and abbreviations 6

1.5 Feedback 7

2 INTRODUCTION 9

2.1 Document Context 9

2.2 Targeted Audience 9

2.3 How to Use this Document 9

2.4 Process for PSA Certified Level 2 10

2.5 Product Identification 10
2.5.1 Contact 10
2.5.2 Chip Reference 10
2.5.3 Chip Description 11
2.5.4 PSA Implementation 11

3 TOE DESCRIPTION 12

3.1 Scope 12

3.2 Major Security Features 13

3.3 Operational Environment 13

3.4 Life-cycle 13

3.5 Assumptions 14

4 SECURITY PROBLEM DEFINITION 15

4.1 Assets 15

4.2 Threat Agents 15

4.3 Threats 15
4.3.1 T.ROGUE_CODE 15

4.3.2 T.FIRMWARE_ABUSE 15
4.3.3 T.UPDATE_ABUSE 15
4.3.4 T.STORAGE 15
4.3.5 T.DEBUG 16
4.3.6 T.WEAK_CRYPTO 16
4.3.7 T.IMPERSONATION 16

5 SECURITY FUNCTIONS 17

5.1 F.INITIALIZATION 17

5.2 F.SOFTWARE_ISOLATION 17

5.3 F.SECURE_STORAGE 17

5.4 F.FIRMWARE_UPDATE 17

5.5 F.SECURE_STATE 17

5.6 F.CRYPTO 18

5.7 F.ATTESTATION 18

5.8 F.AUDIT 18

5.9 F.DEBUG 18

6 DEVELOPER EVIDENCES 19

1 About this document

1.1 Current status and anticipated changes

Current Status: Beta

1.2 Change history

Release Date	Version	Comments
8/01/2019	BET00	Use of JSA template
17/01/2019	BET01	Integration of JSA F2F #3 comments
13/02/2019	BET02	Candidate for public release

1.3 References

This document refers to the following documents.

Ref	Doc No	Author(s)	Title
[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
[PSA-AM]	JSADEN004	ARM JSA	PSA Certified: Attack Method
[PSA-EM]	JSADEN003	ARM JSA	PSA Certified: Evaluation Methodology
[PSA-L1]	JSADEN001	ARM JSA	PSA Certified: Level 1 Questionnaire

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 an RTOS and application tasks. PSA provides no isolation services for this firmware, although the RTOS 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
JTAG	Joint Test Action Group
HUK	Hardware Unique Key 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 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
PSA Updateable Root of Trust	The Root of Trust firmware that can be updated following manufacturing. See *PSA Security Model* [PSA-SM] for details
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 may be present in a platform
Secure Processing Environment (SPE)	This is the security domain that includes the PSA Root of Trust and the Application Root of Trust domains
SiP	System in Package
SoC	System on Chip
SPE	Secure Processing Environment A platform's processing environment for software that provides confidentiality and integrity for its runtime state from software and hardware outside of the SPE. Contains the Secure Partition Manager, the Secure Partitions and the trusted hardware
SPM	Secure Partition Manager. 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
Trusted boot	Trusted Boot is technology to provide a chain of trust for all the components during boot

1.5 Feedback

Arm welcomes 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 Lightweight Protection Profile).
- The number (JSADEN-002).
- The page numbers to which your comments apply.
- The rule identifiers to which your comments apply, if applicable.
- A concise explanation of your comments.

Arm also welcomes general suggestions for additions and improvements.

Note

Arm tests PDFs 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

PSA defines a common hardware and software security platform, providing a generic security foundation and allowing secure products and features to be developed on top of this platform.

The PSA Certified scheme involves the evaluation by a laboratory of a device against a set of security requirements and, in case of a successful evaluation, the certification by the PSA Certified secretariat (or a third-party on behalf of the PSA Joint Stakeholder Members) of this TOE. The evaluation laboratory examines measures and processes to ensure that a functionally compliant TOE, including its critical assets, is not vulnerable to identified threats.

The PSA programme recognises that there will be different security requirements and different cost/security trade-offs for different applications and eco-systems. This is reflected in specifications by introducing a range of *assurance levels*.

This document describes PSA Certified Level 2 scheme. It defines the scope and security requirements for the evaluation of a TOE implementing the PSA architecture.

2.2 Targeted Audience

This document is directly aimed at:

- Chip Vendors, who develop the chip and the PSA components for the Secure Processing Environment, e.g. integrating Trusted Firmware-M.
- Evaluation Laboratories, who perform Level 2 evaluations according to the security requirements set in this document.

It can also be used by OEMs who conceive and develop platforms based on PSA specification in order to assess the robustness level of the security functions they rely on and to develop applications or libraries on top of the platform.

2.3 How to Use this Document

This document defines three important aspects of a security evaluation:

1. The scope of the evaluation, i.e. the part of the device that will be subject to the evaluation and the context the device and TOE is intended to be used.
2. The security problem considered in this scope, i.e. the actual threats on the TOE in its operational context.
3. The required security functions in the TOE in order to mitigate the identified threats.

The Chip Vendor will find here a description of the security functions to be implemented in order to pass the evaluation and an explanation (the security problem) of why they are required. For the purpose of the evaluation, the Chip Vendor will have to derive from this Protection Profile a Security Target (ST) that with chip-specific information relevant for the Evaluation Laboratory. He is expected to reuse the contents of this documents and fill parts in <orange>.

The Evaluation Laboratory will use this document as a reference of the security functions required for a PSA-compliant device. For the purpose of the evaluation, he will mainly consider the chip-specific Security Target provided by the Chip Vendor and derived from this PP.

2.4 Process for PSA Certified Level 2

The process for certification of devices based on the PSA architecture according to PSA Certified Level 2 scheme involves the role of a PSA Certification Secretariat. It receives applications for PSA Security certification, issues certificates and updates PSA Certified scheme.

The process is:

1. The Chip Vendor designs and implements its chip according to the security problem and security functions described in this document. He takes into account the Attack methods document [PSA-AM] to understand how its chip will be assessed by the Evaluation Laboratory.
2. The Chip Vendor submits an application to the PSA Certification Secretariat.
3. The Chip Vendor submits its chip, which may already be integrated on a device, and related documentation to an Evaluation Laboratory.
4. The Evaluation Laboratory performs the security evaluation of the TOE according to PSA Certified Evaluation Methodology [PSA-EM]. The Evaluation Laboratory may ask clarifications from the Chip Vendor.
5. If the result of the review by the Evaluation Laboratory is Pass, the Evaluation Laboratory will provide a PSA_ID for the chip or device.
6. The PSA Certification Secretariat proceeds to the certification of the TOE and the PSA_ID is published along with device or chip reference on the Secretariat's website.

2.5 Product Identification

For its Security Target, the Chip Vendor shall fill this part with product-related information.

2.5.1 Contact

Company name:	
Contact name:	
Contact title:	
Contact email:	
Contact address:	
Contact phone:	

2.5.2 Chip Reference

Commercial name:	
EAN-13:	*(As used in the HW version claim of the chip attestation token)*
HW reference:	
HW version:	
SPE name:	*(e.g. Trusted Firmware-M)*
SPE version:	

2.5.3 Chip Description

Expected usage:	
Features:	*(Describe the functional and security features marketed for the product)*
Description of expected operational environment:	*(Describe if any the actors and resources required for operation of the chip, and the related security assumptions)*

2.5.4 PSA Implementation

PSA functional API certified:	*(Provide the output report from PSA API tests.)*
Isolation boundary level:	*(May be 1, 2 or 3, as described in [PSA-FF])*
PSA RoT services:	*(Describe RoT services part of the PSA root of trust)*
Trusted subsystem:	*(Describe trusted subsystems relied upon for operation of PSA root of trust, such as a security subsystem, Secure Element, and their usage)*

3 TOE Description

3.1 Scope

The scope for a PSA Level 2 Security evaluation, or Target of Evaluation (TOE), is the combination of the hardware and firmware components supporting a device compliant with PSA specification. The considered hardware may be a System-in-Package (SiP), a System-on-Chip (SoC) integrated on a board, or similar set-up.

The hardware is in the scope of the security evaluation as it provides security features, such as immutable storage or protection of JTAG, which are essential for ensuring the security of the PSA implementation.

The PSA platform components that are in the scope of the security evaluation, as described in [PSA-FF], are:

- PSA updateable root of trust, such as Software isolation framework, protecting more trusted software from less trusted software, Generic services such as binding, initial attestation, generic crypto services, FW update validation.
- PSA immutable root of trust, for example Boot ROM, Root secrets and IDs, Isolation hardware, Security lifecycle management and enforcement. This component cannot be updated.
- Trusted Subsystems used by the PSA root of trust, such as security subsystems, trusted peripherals, SIM or SE, which include both hardware and software components are also in the scope of evaluation.

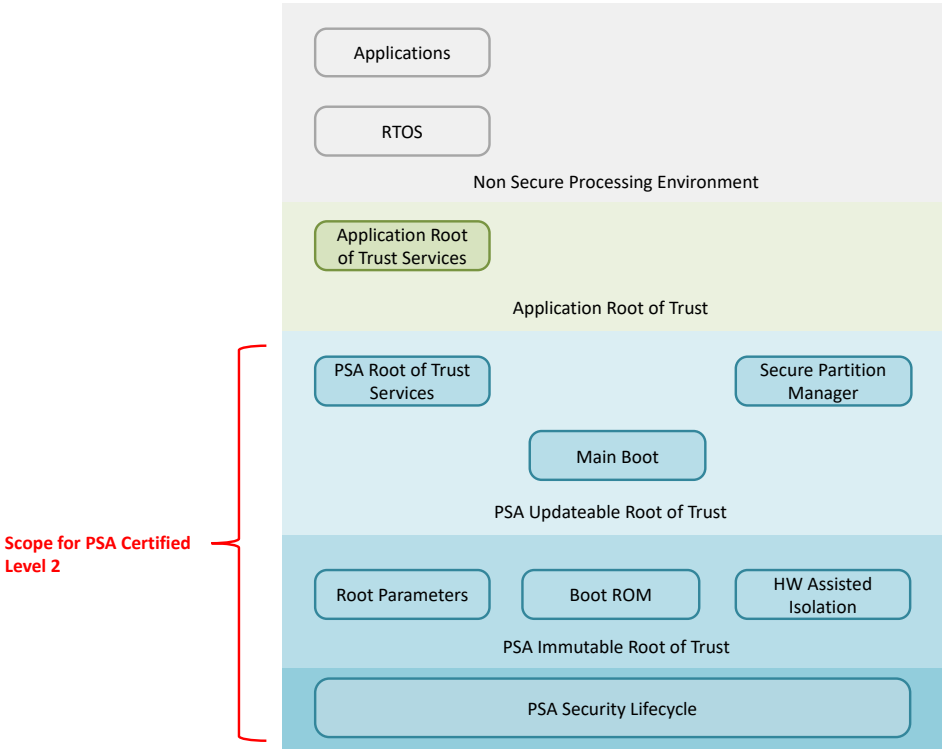

Figure 1: Scope of PSA Certified Level 2

For its Security Target, the Chip Vendor may provide the high-level HW and SW architecture of its product.

3.2 Major Security Features

The PP considers the following features for the purpose of PSA Level 2 security evaluation:

- A Secure Processing Environment (SPE) isolated by hardware mechanisms to protect critical services and related assets from the Non-Secure Processing Environment.
- A Secure Boot process to verify integrity and authenticity of executable code in a chain of trust starting from the Boot ROM. Related certificates are protected in integrity by hardware mechanisms.
- Support for Secure Storage, to protect in integrity and confidentiality sensitive assets for the SPE and related applications. These assets include at least the Hardware Unique Key (HUK), the ROT Public Key (ROTPK), the Attestation key.
- A Security Lifecycle for SPE, to protect the lifecycle state for the device and enforce the transition rules between states.
- Cryptographic functions services for SPE and SPE applications.
- Support for Entity Attestation Token (according to IETF specification).

For its Security Target, the Chip Vendor may provide additional features supported by its product or refine the provided ones.

3.3 Operational Environment

The TOE Operational Environment includes:

- other Applications Root of Trust or other Applications executed in the SPE environment
- alternate OS and applications executed in the Non-Secure Processing Environment (NSPE).
- remote entities (servers, Admin, users), in charge of personalizing the TOE, managing firmware update or interacting with the TOE.

3.4 Life-cycle

The TOE is aimed at being integrated in a device. Its typical life-cycle is as follows:

Phase	**Actors**
1 & 2: Firmware / Software / Hardware design	The Chip Vendor is in charge of designing (part of) the processor(s) where the TOE firmware runs and designing (part of) the TOE hardware security resources. The Chip Vendor designs the TOE ROM code and the secure portion of the device chipset.
3 & 4: Chip manufacturing	The Chip Vendor produces the chipset including the TOE. At this point, the TOE must be fully testable to permit checking for manufacturing defects. The TOE is then configured in multiple steps by the Chip Vendor and the purchasing OEM through the programming of fuses.
5: Device manufacturing	The device manufacturer is responsible for the device assembly, initialization, provisioning and any other operation on the TOE and device before delivery to the end user.
6: Deployed / Secure Enabled	The end user gets a device ready for use, including the TOE. This state only permits configuration operations that support the required use cases and has accesses to the

	security functions of the device. Its debugging and testing features are disabled and secure boot is mandatory. The TOE may be updated if it has not been designed to be immutable.
7: Return Material Authorization (RMA)	This is a terminal state used for devices that are returned to the manufacturer for failure analysis. When a device is put into the RMA state, it loses access to its secret keys and, with it, the ability to operate securely.

3.5 Assumptions

The following assumptions hold on the operational environment of the TOE the following assumptions hold on the operational environment of the TOE:

- The TOE Admin in charge of personalizing the TOE and managing firmware update is assumed to be trusted.
- The TOE Admin is assumed to securely manage cryptographic keys and certificates outside of the TOE.
- The TOE Admin is in charge of providing a unique identifier to the TOE, either through external provisioning or using statistical uniqueness properties for identifier generated on the device.

4 Security Problem Definition

4.1 Assets

The TOE shall protect:

- The integrity of SPE updateable code.
- The integrity and confidentiality of root secrets: Initial Attestation Key (IAK), Hardware Unique Key (HUK) and, if supported, Boot encryption key.
- The integrity of root parameters: Instance ID and Boot validation key (ROTPK).
- The integrity of the lifecycle state

For its Security Target, the Chip Vendor may refine this list of assets.

4.2 Threat Agents

The threat agents which may attack the TOE are:

- Remote hackers, with access to a remote connection to the TOE
- Local hackers, with limited resources, knowledge or equipment.

If the device including the TOE is expected to always operate in secure environments, that provide a physical security against local hackers, this threat agent may be discarded in the Security Target. The Chip Vendor shall provide a clear description of the expected usage of the TOE in the description of the Operational environment section and add related assumptions on physical security in the Assumptions section.

4.3 Threats

This section identifies threats on the TOE.

4.3.1 T.ROGUE_CODE

An attacker succeeds in loading and executing rogue code on the device, either in the Secure Processing Environment or in the Non-Secure Processing Environment, and compromises the TOE assets.

4.3.2 T.FIRMWARE_ABUSE

An attacker exploits a flawed version of the PSA root of trust (including hardware), for instance by sending malformed parameters, and compromises the TOE assets.

4.3.3 T.UPDATE_ABUSE

An attacker exploits a flaw in the firmware update mechanisms of the TOE, for instance by sending malformed parameters, by altering an authentic firmware update, by installing an old version of the firmware or by bypassing security checks, and installs a flawed version of the PSA updateable root of trust.

4.3.4 T.STORAGE

An attacker succeeds in illegally modifying or accessing assets stored on the TOE, for instance by bypassing checks related to TOE lifecycle or by performing local probing.

4.3.5 T.DEBUG

An attacker succeeds in accessing TOE debug features and illegally modifies or accesses TOE assets.

4.3.6 T.WEAK_CRYPTO

An attacker exploits flaws in the use or implementation of cryptographic algorithms in the TOE and illegally modifies or accesses TOE assets.

4.3.7 T.IMPERSONATION

An attacker manages to make remote entites recognize a rogue device under its control as a valid TOE.

5 Security Functions

In order to mitigate the identified threats, the TOE shall support the following security functions.
This part is similar to the Security Functional Requirements (SFR) part of a Common Criteria Protection Profile, although written in an informal style.

For its Security Target, the Chip Vendor should provide additional information on how these security functions are implemented.

5.1 F.INITIALIZATION

The TOE is started through a secure initialization process that ensures the authenticity and integrity of the firmware.
This security function mitigates T.ROGUE_CODE by preventing the installation firmware or piece of firmware code from unknown sources.

5.2 F.SOFTWARE_ISOLATION

The TOE provides isolation between the Non-Secure Processing Environment and the Secure Processing Environment and also between PSA Root of Trust and other executable code (such as Application Root of Trust) of the Secure Processing Environment.
This corresponds to at least isolation level 2, as defined in PSA Firmware Framework [PSA-FF].
This security function mitigates T.ROGUE_CODE by preventing software outside of the TOE from tampering with TOE assets.

5.3 F.SECURE_STORAGE

The TOE protects the confidentiality and integrity of assets in a secure storage. The secure storage is bound to the platform. Only the TOE can retrieve and modify assets from this secure storage.
This security function mitigates T.STORAGE by preventing direct and unprotected access to assets.

5.4 F.FIRMWARE_UPDATE

The TOE verifies the integrity and authenticity of the TOE update prior to performing the update.
The TOE also rejects attempts of firmware downgrade.
This security function mitigates T.UPDATE_ABUSE by preventing installation of firmware from unknown sources or installation of obsolete firmware.

5.5 F.SECURE_STATE

The TOE ensures the correct operation of its security functions. In particular, the TOE:

- Protects itself against abnormal situations caused by programmer errors or violation of good practices from code executed outside of the TOE, either other applications from Secure Processing Environment or OS and applications from the Non-Secure Processing Environment
- Controls the access to its services by Applications and checks the validity of parameters of any operation requested from Applications
- Enters a secure state upon platform initialization error or software failure detection, without exposure of any sensitive data.

This security function mitigates T.FIRMWARE_ABUSE by preventing exploitation of abnormal situations.

5.6 F.CRYPTO

The TOE implements state-of-the-art cryptographic algorithms and key sizes, as recommended for instance by national security agencies (such NIST for U.S., BSI for Germany, CESG for U.K., ANSSI for France).
This security function mitigates T.WEAK_CRYPTO by preventing the use of weak cryptographic algorithms and key sizes. It does not prevent however from weaknesses on the implementation of cryptographic functions.

The Chip Vendor may provide additional information on how these security functions are implemented.

5.7 F.ATTESTATION

The TOE provides an attestation service which reports on the device identity, firmware measurements and runtime state of the device. The attestation can be verified by remote entities.
This security function mitigates T.IMPERSONATION by providing a cryptographic proof of identity.

The Chip Vendor may specify which other information is included in device attestation, such as firmware measurements and runtime state of the device as in [PSA-SM].

5.8 F.AUDIT

The TOE maintains log of all significant security events and allow access and analysis of these logs to authorized users only (such as TOE Admin).
This security function mitigates T.ROGUE_CODE, T.FIRMWARE_ABUSE, T.UPDATE_ABUSE, T.STORAGE, T.DEBUG and T.IMPERSONATION.

This security function is optional for resource-constrained devices. The Chip Vendor shall provide a rationale on why is it discarded.

5.9 F.DEBUG

The TOE restricts access to debug features by a deactivation or access control mechanism with the same level of security assurance as other security functions of this PP.
This security function mitigates T.DEBUG by preventing unauthorized access to debug features.

6 Developer Evidences

The Chip Vendor shall provide the following documentation to the Evaluation Laboratory:

- Security Target based on this Protection Profile.
  All assets, threats and security functions defined in the Protection Profile shall be included in the Security Target. The Developer may add other assets, threats and security functions.
  The Developer may also add assumptions, provided they do not mitigate threats meant to be addressed by security functions.
- 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.
- Answers to PSA Certified Level 1 Questionnaire [PSA-L1] for the TOE (RTOS Vendor Section).
- Test results for PSA Functional Certification, including TOE setup for these tests.

Additionally, the Chip Vendor shall provide the TOE, the source code for the TOE and the TOE test equipment if they are specific or dedicated.