PSA Certified™ Lightweight Protection Profile Version 1.2

psacertified™

psacertified™
level two

Document number:	JSADEN002
Version:	1.2
Release Number:	01
Authors:	PSA JSA Members: Applus+, S.L Arm Limited CAICT ECSEC Laboratory Inc Prove & Run S.A.S. Riscure B.V. SGS Brightsight B.V. Trust CB B.V. UL TS B.V.
Authorized by:	PSA JSA Members
Date of Issue:	04/04/2022

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

Non-Confidential Proprietary Notice

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

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
04/04/2022	1.2	Non-confidential	Clarification of definitions and update of TOE figure. Addition of L2+SE level.
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-EM]	JSADEN003	PSA JSA	PSA Certified: Evaluation Methodology
[PSA-L1]	JSADEN001	PSA JSA	PSA Certified: Level 1 Questionnaire
[PSA-AM]	JSADEN004	PSA JSA	PSA Certified: Attack Method
[PSA-Comp]		PSA JSA	PSA Certified Security Evaluation for RoT Components **https://www.psacertified.org/getting-certified/ip-provider/rot-component-evaluation/**

1.3.2 Informative references

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

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 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. They are termed Application Root-of-Trust (ARoT) services.
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.
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
Hardware Unique Key (HUK)	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust.
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.
JTAG	Joint Test Action Group
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 Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.

PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
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 considered to be the most trusted security component on the device. See [PSA-SM].
PSA Root of Trust Service	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 Functional APIs.
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.
Secure Partition	A Partition in the Secure Processing Environment.
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)	The processing environment that executes the PSA-RoT, the PSA-RoT Services and any Application RoT Service(s).
SiP	System in Package
SoC	System on Chip
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.
Trusted Subsystem	A security subsystem that the PSA-RoT relies on for protection of its assets, or that implement some of its services.
Updateable Platform Root of Trust	The firmware, software and data of the PSA-RoT that can be securely updated following manufacture.

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 Lightweight Protection Profile).
- The number (JSADEN-002) 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

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 of this TOE. The evaluation laboratory examines measures and processes to ensure that a functional TOE is not vulnerable to the identified threats to the levels defined in this document.

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, and SPE Developers.
- 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 PSA Certified Level 2 Ready Evaluation

The PSA Certified scheme allows for 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 PSA Certified 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 PSA Certified Level 2+SE

The PSA Certified scheme also considers a PSA Certified Level 2 certification where the product architecture, as illustrated in Figure 1, includes a trusted subsystem, typically a Secure Element, that is certified for the

considered security functions for protection against hardware attacks and at least at AVA_VAN.3 (with Common Criteria, PSA Certified Level 3 RoT components [PSA-Comp] or SESIP3).

The Developer can obtain the rights to use a specific "PSA Certified Level 2+SE" logo and showcase its solution on **www.psacertified.org**. Such a logo could be used to demonstrate, for example, the benefit of protection against hardware attacks for the most sensitive assets of the product.

2.5 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 to mitigate the identified threats.

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

SPE Developer can also apply for evaluation of their code, but they must choose a specific hardware implementation to perform the first evaluation.

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.

2.6 Process for PSA Certified Level 2

The process for certification of devices based on the PSA architecture according to PSA Certified Level 2 (including PSA Certified Level 2+SE) 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 and PSA root of trust implementation according to the security problem and security functions described in this document. He considers the Attack methods document [PSA-AM] to understand how its chip will be assessed by the Evaluation Laboratory.
2. The Chip Vendor submits its chip, which may already be integrated on a device, and related documentation to an Evaluation Laboratory.
3. 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.
4. If the result of the review by the Evaluation Laboratory is Pass, the Evaluation Laboratory will provide a EAN-13 for the chip or device.

5. The PSA Certification Secretariat reviews the Evaluation Technical Report from the Evaluation Laboratory and proceeds to the certification of the TOE. The EAN-13 is published along with device or chip reference on the Secretariat's website.

2.7 Resistance to Attacks

PSA certification is designed for IoT devices which will be deployed at scale. To meet PSA Certified Level 2 there shall be no attacks that can be remotely applied to a class of devices. It is not required to protect against physical attacks on an individual device, as it is assumed the attacker will not be able to repeat the attack on sufficient devices before being detected.

Therefore, for the purposes of PSA Level 2 certification, attacks that require physical access for the exploitation phase are excluded. Physical attacks are only considered valid in the identification phase of the attack if they lead to scalable remote attacks (for example revealing a class key shared by all devices).

2.8 Product Identification

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

2.8.1 Contact

Company activity:	*(State whether OEM, System software Vendor or Chip Vendor)*
Company name:	
Contact name:	
Contact title:	
Contact email:	
Contact address:	
Contact phone:	

2.8.2 Chip Reference

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:	
Chip EAN-13:	*(If this version of the chip has already passed PSA Certified, specify the EAN-13 of the certificate)*
Chip reference documentation:	*(If this version of the chip has not yet passed PSA Certified, provide identification of the reference documentation used to fill the questionnaire, such as chip datasheet, detailed fact sheet or reference manual. It may be requested by the Evaluation Laboratory)*
Vulnerability disclosure policy:	*(If a vulnerability disclosure policy is available for this product, provide the URL it can be retrieved. See Appendix A.3 of [PSA-L1] for more information)*

2.8.3 Chip Description

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

operational environment:	

2.8.4 PSA RoT Implementation

PSA functional API certified:	*(PSA Functional API Certification is optional.* *If PSA API tests have been performed, then provide the output reports to the Evaluation Laboratory.)*
Isolation boundary level:	*(Isolation of the Secure Processing Environment (SPE) from the Non-secure Processing Environment (NSPE) is a mandatory PSA Certified requirement. The PSA Security Model [PSA-SM] defines two incremental isolation boundaries; please indicate if these are deployed:* ☐ *The PSA-RoT is isolated from the Application RoT Service(s).* ☐ *In addition to PSA-RoT isolation from Application RoT Service(s), Application RoT Services are isolated from each other.)*
PSA RoT services:	*(Describe RoT services part of the PSA Root of Trust)*
Trusted subsystem:	*(Identify trusted subsystems relied upon for operation of PSA Root of Trust, such as an on-chip security subsystem or off-chip Secure Element.* *Provide trusted subsystems reference, such as related chip name, part number and version, and reference to an existing security certification, such as Common Criteria, FIPS-140 or SESIP, or PSA Certified RoT Component.* *If this existing security certification is not sufficient to cover the trusted subsystems security functions relied upon to establish the PSA Root of Trust, the Vendor can pre-certify these security functions using a PSA Certified Level 2 security certification for RoT components [PSA-Comp] (or a PSA Certified Level 3 security certification for RoT components if the product applies for PSA Certified Level 2+SE certification). Otherwise, these security functions will be evaluated as part of the currently applied PSA Certified Level 2 security evaluation.* *Describe usage of the trusted subsystems, such as: Cryptographic provider for the Platform Root-of-Trust and Application Root-of-Trust.* *Declare 'none' if no trusted subsystem is used.)*

3 TOE Description

3.1 Scope

The scope for a PSA Certified Level 2 Security evaluation, or Target of Evaluation (TOE), is the combination of the trusted hardware and firmware components implementing a PSA-RoT with the Security Functional Requirements stated in this document. PSA Certified Level 2 scope is identical to PSA Certified Level 3.

The Chip security evaluation scope includes the following Secure Processing Environment PSA-RoT elements, as described in [PSA-SM]:

- 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 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 TOE 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.

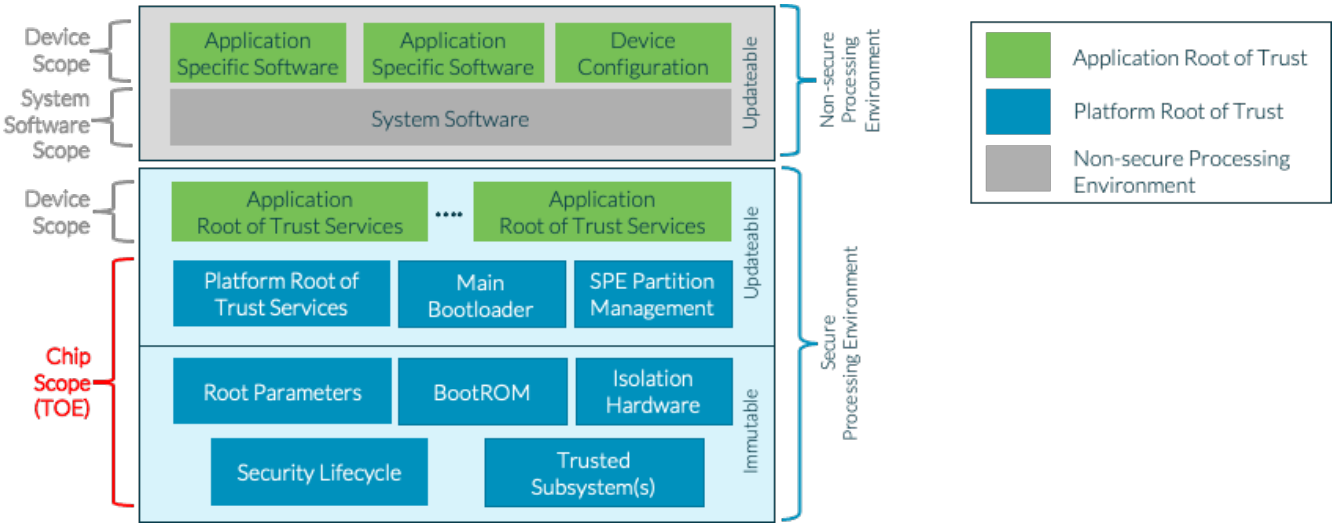

Figure 1: TOE Scope of PSA Certified Level 2

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

3.1.1 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).

3.1.2 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 (for instance remote servers, administrators, users), in charge of personalizing the TOE, managing firmware update or interacting with the TOE.

The Chip Vendor shall provide a clear description of the operational environment of the TOE for its expected usage.

3.2 Assumptions

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

- Cryptographic keys and certificates outside of the TOE are subject to secure key management procedures.
- Actors in charge of TOE management, for instance for signature of firmware update, are trusted.
- Each TOE has a unique identifier, provisioned during manufacturing.
- Integrity of immutable code is ensured by hardware mechanism such as ROM, or EEPROM or FLASH memory that is locked before device delivery.

For its Security Target, the Chip Vendor may describe additional assumptions on the operational environment of the TOE. This should also be reflected in the user guidance documentation for the TOE.

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

4.2 Threat Agents

The threat agents which may attack the TOE are remote hackers, with access to a remote connection to the TOE.

During the identification phase of the attack, it is assumed that threat agents can have remote and local physical access to the TOE for analysis purposes. By this, attackers could identify vulnerabilities which can be remotely exploited to break any of the security functions of Section 5.

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 in the 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.

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 entities recognize a rogue device under its control as a valid TOE.

4.3.8 T.ILLEGAL_ACCESS

An attacker manages to access or modify data used by the TOE in system memory or exchanged with any trusted subsystems.

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 shall provide additional information on how each of 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 and T.ILLEGAL_ACCESS by preventing software outside of the TOE from tampering with TOE assets.

When a trusted subsystem is used by the TOE, the Chip Vendor shall describe which mechanism is used to protect in confidentiality and integrity the communication between the SPE and the trusted subsystem. This mechanism will be part of the evaluation.

5.3 F.SECURE_STORAGE

The TOE protects the confidentiality and integrity of assets in 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.

When a trusted subsystem is used for some or all of this function, the Chip Vendor shall describe which set of assets is managed by the trusted subsystem.

5.4 F.FIRMWARE_UPDATE

The TOE verifies the integrity and authenticity of the TOE update prior installation of 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 from SPE or NSPE.
- 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 (including any trusted subsystems) or software failure detection, without exposure of any sensitive data.

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

5.6 F.CRYPTO

The TOE implements state-of-the-art cryptographic algorithms and key sizes for protection of TOE assets. Recommendations may come from national security agencies (such NIST for U.S., BSI for Germany, CESG for U.K., ANSSI for France) or from academia. Weak cryptographic algorithms or key sizes may be available for specific usages and with specific guidance, but they shall not reduce security of provided state-of-the-art cryptography.

This security function mitigates T.WEAK_CRYPTO by preventing exploitation of cryptographic weaknesses to target TOE assets.

The Chip Vendor shall provide cryptographic algorithms and key sizes in scope for the evaluation. He may provide additional information on how these security functions are implemented, for instance with support of cryptographic accelerators.

When a trusted subsystem is used for some or all of this function, the Chip Vendor shall describe which set of cryptographic operations is performed by the trusted subsystem.

5.7 F.ATTESTATION

The TOE provides an attestation service which reports on the device identity, firmware measurements of the TOE and security lifecycle state of the TOE.

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 other information to be included or provide a mechanism for application specific information to be include in the device attestation report, such as such as measurements of other components, further information as to the state of the device, and any measurements made by the application as in [PSA-SM].

When a trusted subsystem is used for this function, the Chip Vendor shall describe how attestation is performed and which information is exchanged with trusted subsystem.

5.8 F.AUDIT

The TOE maintains log of all significant security events and allows 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 it is discarded.

5.9 F.DEBUG

The TOE restricts access to debug features by 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.

Appendix A: Developer Evidence

The Developer (Chip Vendor or the SPE Developer) shall provide the following documentation to the Evaluation Laboratory:

- Security Target based on this Protection Profile.
    - Developer shall reuse the contents of the PP and fill parts in <orange> in its Security Target.
    - Developer documentation referenced in the Security Target shall also be provided.
- 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.
- If available, answers to PSA Certified Level 1 Questionnaire [PSA-L1] for the TOE (Chip Vendor Section).
- Test results for PSA Functional Certification or otherwise test results from Developer functional tests of TOE APIs, including TOE setup for these tests.
- Vendor user guidance for any Trusted Subsystems used.
- If available, evidence of a security certification for any Trusted Subsystems used.

Additionally, the Developer shall provide:

- The TOE, in its manufactured and finalized state. In this state, it shall only permit configuration operations that support the required use cases and accesses to the security functions. The TOE 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.
- The source code for the components in scope of the TOE (see Section 3.1, hardware design is not required). This shall include drivers for Trusted Subsystems if used.
- The functional testing environment for TOE APIs.
- The TOE test equipment if they are specific or dedicated.

Appendix B: Reference Lifecycle

The TOE only provides the root of trust and that this must be integrated into a device that will include other components and functions not covered by the PSA certification. The TOE typical lifecycle 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: 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 (enables, sets or seeds the Hardware Unique Key).
4: Software integration	The OEM is responsible for the integration, validation and preparation of the software to load in the product that will include the RoT, any pre-installed Applications Root of Trust, and additional software required to use the product (e.g., NSPE, Client Applications).
5: Device manufacturing	The OEM 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 access to the security functions. The TOE 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.