PSA Certified™ Level 3 Lightweight Protection Profile

Document number:	JSADEN009
Version:	1.0
Release Number:	ALP02
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:	15/10/2020

© Copyright Arm Limited 2017-2020. All rights reserved.

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 PSA 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 3 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against hardware and software attacks. The PSA Certified Level 3 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 PSA Certified Level 3 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 3, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

Copyright ©2017-2020 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.

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

Contents

Non-Confidential Proprietary Notice **3**

1 About this document **6**

1.1 Current Status and Anticipated Changes **6**

1.2 Release Information **6**

1.3 References **6**
1.3.1 Normative references 6
1.3.2 Informative references 6

1.4 Terms and Abbreviations **7**

1.5 Feedback **8**

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 3 **10**

2.5 Resistance to Attacks **10**

2.6 Product Identification **11**
2.6.1 Contact 11
2.6.2 Chip Reference 11
2.6.3 Chip Description 11
2.6.4 PSA Implementation 12

3 TOE Description **13**

3.1 Scope **13**
3.1.1 Major Security Features 14
3.1.2 Operational Environment 14

3.2 Assumptions **14**

4 Security Problem Definition **16**

4.1 Assets 16

4.2 Threat Agents 16

4.3 Threats 16
4.3.1 T.ROGUE_CODE 16
4.3.2 T.FIRMWARE_ABUSE 16
4.3.3 T.UPDATE_ABUSE 16
4.3.4 T.STORAGE 16
4.3.5 T.DEBUG 16
4.3.6 T.WEAK_CRYPTO 17
4.3.7 T.IMPERSONATION 17
4.3.8 T.PHYSICAL 17
4.3.9 T.SIDE_CHANNEL 17

5 Security Functions 18

5.1 F.INITIALIZATION 18

5.2 F.SOFTWARE_ISOLATION 18

5.3 F.SECURE_STORAGE 18

5.4 F.FIRMWARE_UPDATE 18

5.5 F.SECURE_STATE 18

5.6 F.CRYPTO 19

5.7 F.ATTESTATION 19

5.8 F.AUDIT 19

5.9 F.DEBUG 20

5.10 F.PHYSICAL 20

Appendix A: Developer Evidences 21

Appendix B: Reference Lifecycle 22

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Alpha

1.2 Release Information

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

Date	Version	Confidentiality	Change
09/07/2020	1.0ALP01	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]	JSADEN010	JSA	PSA Certified Level 3: Evaluation Methodology
[PSA-L1]	JSADEN001	JSA	PSA Certified: Level 1 Questionnaire
[PSA-AM]	JSADEN008	JSA	PSA Certified Level 3: Attack Method

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 Certified 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
CMS	Configuration Management System
Evaluation laboratory	Laboratory or facility that performs the evaluation tasks on the TOE. 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 Certified 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 API 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 Certified 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 Certified 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 Certified 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 3 Lightweight Protection Profile).
- The number (JSADEN-009) 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 Certified 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 Certified 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 Certification Body 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 Certified program recognises that there will be different security requirements and different cost/security trade-offs for different applications and ecosystems. This is reflected in specifications by introducing a range of assurance levels.

This document describes PSA Certified Level 3 scheme. It defines the scope and security requirements for the evaluation of a TOE implementing the PSA Certified architecture.

2.2 Targeted Audience

This document is directly aimed at:

- Chip Vendors, who develop the chip and the PSA Certified components for the Secure Processing Environment, e.g. integrating Trusted Firmware-M, and SPE Developers.
- Evaluation Laboratories, who perform PSA Certified Level 3 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 Certified 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 Developer (Chip Vendor or SPE Developer) 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 Developer will have to derive from this lightweight Protection Profile a lightweight Security Target (ST) with chip-specific information relevant for the Evaluation Laboratory. The Developer 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 Certified device. For the purpose of the evaluation, the Evaluation Laboratory 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 3

The process for certification of devices based on the PSA Certified architecture according to PSA Certified Level 3 scheme involves the role of a PSA Certification Body. It receives applications for PSA Certified security certification, issues certificates and updates PSA Certified scheme.

The process is:

1. The Chip Vendor designs and implements his 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 an Evaluation Technical Report to the PSA Certification Body.
5. The PSA Certification Body reviews the Evaluation Technical Report, proceeds to the certification of the TOE and provide an EAN-13 for this certification. The EAN-13 is published along with device or chip reference on the Secretariat's website https://trustcb.com/iot/psa-certified/ and on PSA Certified website https://psacertified.org.

2.5 Resistance to Attacks

PSA Certified is designed for IoT devices which require protection against physical attacks. Contrarily to PSA Certified Level 2, for the purposes of PSA Certified Level 3 certification, attacks that require physical access for the exploitation phase are included in the scope.

2.6 Product Identification

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

2.6.1 Contact

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

2.6.2 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.)*

2.6.3 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:	

2.6.4 PSA Implementation

PSA Functional API Certified:	*PSA Functional API Certification is optional.* *If PSA Functional API tests have been performed, then provide the output reports to the Evaluation Laboratory.*
Isolation boundary level:	*As described in [PSA-FF]:* ☐ *Isolation level 2: additional isolation boundary between the PSA Root of Trust and the Application Root of Trust* ☐ *Isolation level 3: additional isolation boundaries between each of the Secure Partitions in the Application Root of Trust.*
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, or declare 'none' if no trusted subsystem is used)*

3 TOE Description

3.1 Scope

The scope for a PSA Certified Level 3 Security evaluation, or Target of Evaluation (TOE), is the combination of the hardware and firmware components supporting a device compliant with PSA Certified specification. The considered hardware may be a System-in-Package (SiP), a System-on-Chip (SoC) integrated on a board, or similar set-up. PSA Certified Level 3 scope is identical to PSA Certified Level 2.

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 Certified implementation.

The 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.

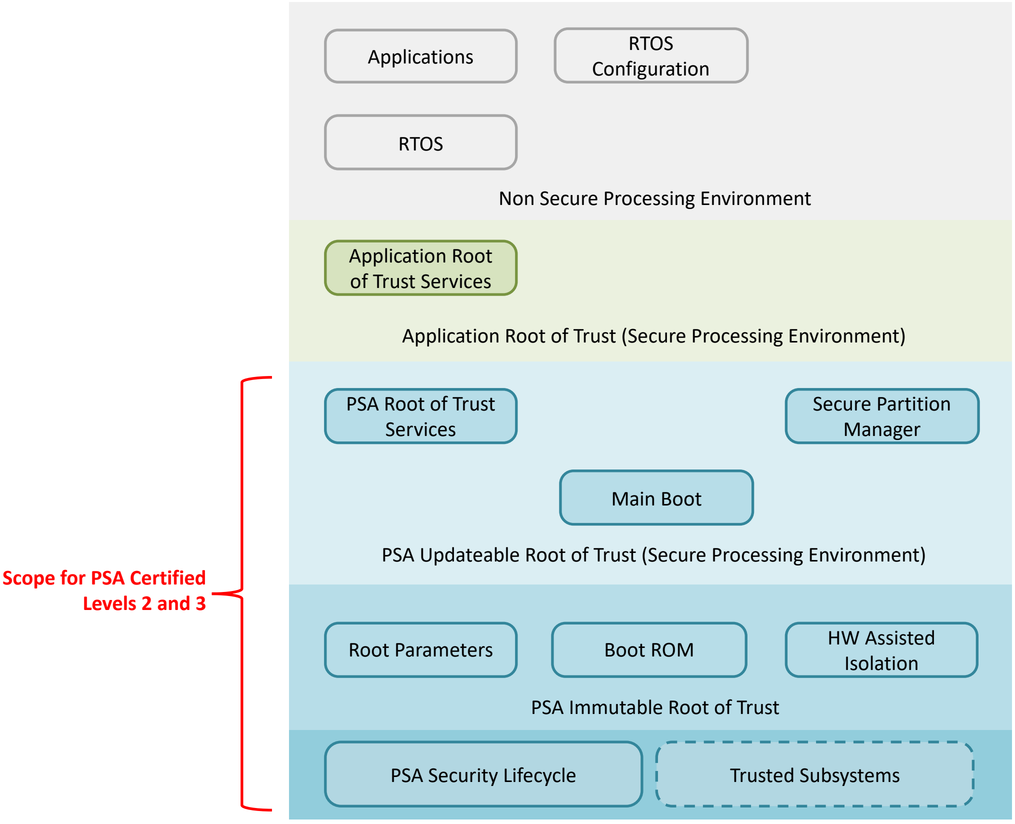
Applications
RTOS Configuration
RTOS
Non Secure Processing Environment
Application Root of Trust Services
Application Root of Trust (Secure Processing Environment)
PSA Root of Trust Services
Secure Partition Manager
Main Boot
PSA Updateable Root of Trust (Secure Processing Environment)
Scope for PSA Certified Levels 2 and 3
Root Parameters
Boot ROM
HW Assisted Isolation
PSA Immutable Root of Trust
PSA Security Lifecycle
Trusted Subsystems

Figure 1: Scope of PSA Certified Level 3

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 Certified Level 3 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 an attestion method, for example 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.
- The integrity and confidentiality of Application Root of Trust (ARoT) or the NSPE data managed by the TOE through the PSA Root of Trust Secure Storage service.

4.2 Threat Agents

The threat agents which may attack the TOE are local and remote hackers (i.e., with access to a remote connection to the TOE).

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.PHYSICAL

An attacker performs physical attacks, during the identification and/or the exploitation phase of an attack in order to illegally modify or access TOE assets

4.3.9 T.SIDE_CHANNEL

An attacker manages to compromise cryptographic assets by means of side-channel attacks.

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 of 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 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 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 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, random number generation and key sizes for protection of TOE assets. These algorithms must be designed and implemented in order to prevent side-channel and faults attacks.

Recommendations for state-of-the-art cryptography 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 and T.SIDE_CHANNEL 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.

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 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 is it 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.

5.10 F.PHYSICAL

The TOE protects the other security functions against physical manipulation of the TOE. This includes protection against manipulation of the hardware and any data, undetected manipulation of memory contents, physical probing on the chips surface. The RoT detects or prevents its operation outside the normal operating conditions (such as voltage, clock frequency, temperature, or external energy fields) where reliability and secure operation has not been proven or tested.

This security function mitigates T.PHYSICAL by preventing physical attacks.

Appendix A: Developer Evidences

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.
- Product data sheet, with specification of normal operating conditions.
- Functional specification, with a complete description of TOE interfaces (parameters, purpose, method of use, errors).
- 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.
- Test results for PSA Functional API Certification or otherwise test results from Developer functional tests of TOE APIs, including TOE setup for these tests.
- Statement of the configuration management system (CMS) used for TOE source code and a unique CMS revision identifier (or list of identifiers) for all files part of the TOE source code.
- Description of vulnerability remediation procedure, that explains how the Developer acts on timely manner after knowledge of a vulnerability to notify the end-user of known vulnerabilities and possible mitigations and provide security updates.

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.
- A mapping that relates the security functions of this ST to the files on the TOE source code that implement these security functions.
- The functional testing environment for TOE APIs.
- The TOE test equipment if it is specific or dedicated.

Appendix B: Reference Lifecycle

The TOE only provides the root of trust and this must be integrated into a device that will include other components and functions not covered by the PSA Certified evaluation. 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.

End of document