# PSA Certified™ Level 1 Questionnaire



psacertified™
level one

| | | | |
|---|---|---|---|
| Document number: | JSADEN0001 | Version: | 1.2 |
| Date of Issue: | 30/10/2019 | | |
| Author: | PSA JSA Members:<br>Arm Limited<br>Brightsight B.V.<br>CAICT<br>Prove & Run S.A.S.<br>Riscure B.V.<br>Trust CB B.V.<br>UL TS B.V. | | |
| Authorized by: | PSA JSA Members | | |

## 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. This document covers PSA Certified™ Level 1 which builds on the PSA Security Model goals, generic IoT threat models and industry best practice to provide a set of critical security questions for the chip vendor, RTOS supplier and OEM. Use this form to fill in the questionnaire for your product and review it with one of the JSA member Evaluation Laboratories. Products that become PSA Certified will be showcased on www.psacertified.org website. PSA and PSA Certified are architecture neutral.

## Keywords

PSA Certified, Level 1, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

# 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 PSA CERTIFIED OVERVIEW 9

2.1 PSA Overview 9

2.2 Scope for Security Evaluation 9

2.3 Roles for PSA Certified Level 1 11

2.4 Options for Evaluation 11

2.5 Process for PSA Certified Level 1 11

2.6 Assumptions for the Operational Environment 12

3 ASSESSMENT INFORMATION 13

3.1 Contact 13

3.2 Scope of Evaluation 13

3.3 Product Reference 13

3.4 Product Description 14

3.5 PSA Implementation 14

3.6 Declaration for new questionnaire 15

3.7 Declaration for reuse of an existing certificate 16

4 CHIP ASSESSMENT QUESTIONNAIRE 17

4.1 Hardware 17

4.2 PSA-RoT 18

5 RTOS ASSESSMENT QUESTIONNAIRE 20
5.1 Code Integrity 20
5.2 Data Assets 21
5.3 Communication 21
5.4 Hardening 22
5.5 Passwords 22
5.6 Privacy 23
6 DEVICE ASSESSMENT QUESTIONNAIRE 24
6.1 Code Integrity 24
6.2 Communication 24
6.3 Hardening 25
6.4 Passwords 25
6.5 Privacy 26

# 1 About this document

## 1.1 Current status and anticipated changes

Current Status: Final

## 1.2 Change history

| Release Date | Version | Comments |
|---|---|---|
| 30/10/2019 | 1.2 | Clarifications for possible evaluation scopes and alignments with PSA Certified Level 2. |
| 01/04/2019 | 1.1 | Clarifications on PSA Functional Certification and PSA Developer APIs |
| 13/02/2019 | 1.0 | Public release based on BET03 version |

## 1.3 References

This document refers to the following documents.

| Ref | Doc No | Author(s) | Title |
|---|---|---|---|
| [PSA-FF] | ARM DEN 0063 | ARM | ARM® Platform Security Architecture Firmware Framework |
| [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 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 |
| 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 Developer 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 Developer APIs and passed the PSA Functional certification Test Suites. |
| PSA Immutable Root of Trust | The hardware and code and data that cannot be modified following manufacturing. See *PSA Security Model* [PSA-SM] for details |
| PSA Root of Trust | This defines the most trusted security domain within a PSA system. See *PSA Security Model* [PSA-SM] for details |
| PSA Root of Trust Service | This is a Root of Trust Service within the PSA Root of Trust domain |
| 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 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. |
| 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 |
| 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 |

## 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 1 Questionnaire).
- The number (JSADEN-001) 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.

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 PSA Certified Overview

## 2.1 PSA Overview

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

The terms PSA Functional Certification and PSA Certified are used here with the following meanings:

- *PSA Functional API Certification*

  PSA Functional API Certification means that a device has implemented the **PSA Developer APIs**[1] and passed the PSA Functional API Certification Test Suites. The PSA Developer APIs cover three security functions: Attestation, Cryptography and Secure Storage. A step by step guide for getting a product PSA Functional API certified is available on the resources page of **www.psacertified.org**

- *PSA Certified*

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

The PSA Certified scheme 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 range of *assurance levels*.

PSA Certified Level 1 assurance[2], the target of this document, relies on a questionnaire filled out by the chip vendor, RTOS vendor or OEM. The questionnaire defined in the present document aims at covering baseline IoT security requirements to mitigate common IoT threats and security requirements for PSA products.

Questionnaire assessment is performed by an Evaluation Laboratory and if the device passes, a digital certificate is issued and published on **www.psacertified.org**. The certificate number is a globally unique EAN-13 number that can be supplied by the Evaluation Laboratory or by the company seeking certification.

PSA devices support an Entity Attestation Token that can include the EAN-13 to inform relying parties that the chip, RTOS or device has been evaluated and PSA certified.

## 2.2 Scope for Security Evaluation

The scope for security evaluation is the combination of the hardware and software components supporting a device. There are three evaluation scopes, the Chip, the RTOS and the Device. Figure 1 illustrates the components in the PSA architecture and the related security certification scopes.

The isolation between the Non-Secure Processing Environment and the Secure Processing Environment (for PSA Updateable Root of Trust and Application Root of Trust) can be implemented for instance relying on Cortex-v8M with TrustZone or using dual cores on Cortex-v7M.

[1] https://pages.arm.com/psa-apis.html

[2] PSA Certified security assurance levels are a distinct concept from SPM isolation levels defined in PSA specification, which characterize different types of software isolation.

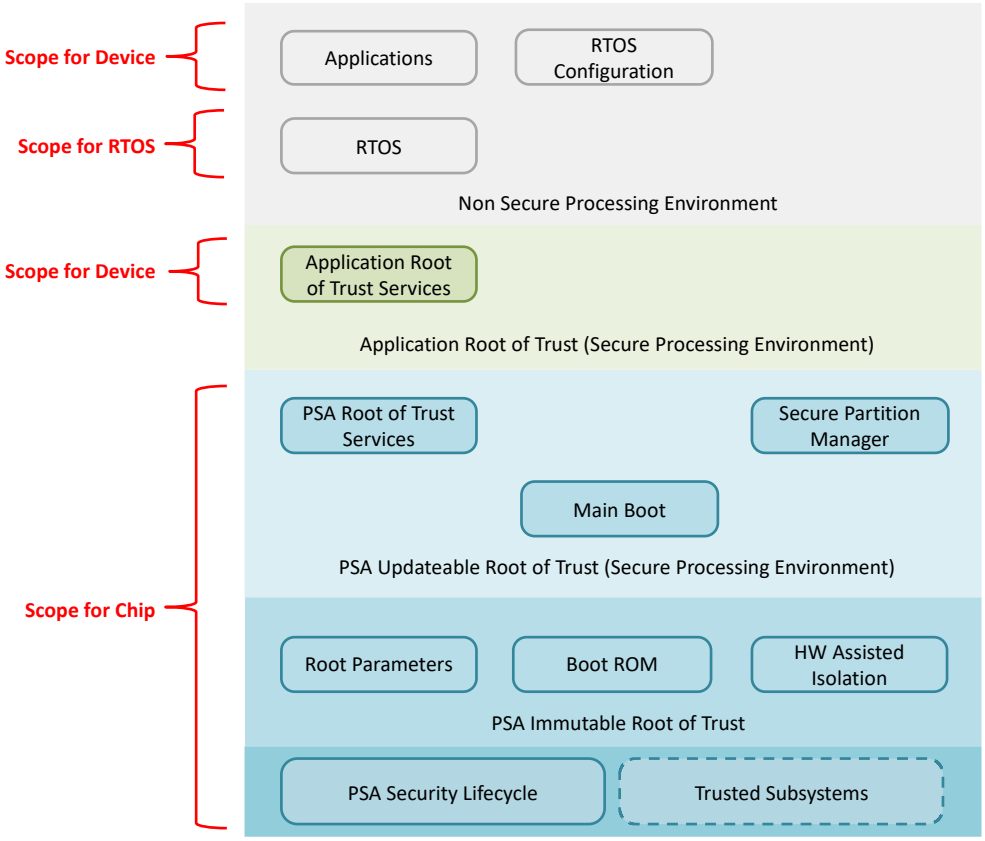


Figure 1: Logical Scope of PSA Certified Level 1

The Chip provides security features such as immutable storage or protection of debug features, which are essential for ensuring the security of the PSA device. The hardware may be a System-in-Package (SiP) or a System-on-Chip (SoC) integrated on a board. The Chip evaluation scope includes the following components from the PSA platform, as described in [PSA-FF]:

- PSA immutable root of trust, for example the Boot ROM, any root parameters, the isolation hardware, security lifecycle management and enforcement.
- Trusted subsystems used by the PSA root of trust, such as any security subsystems, trusted peripherals, SIM or SE, which can include hardware and software.
- PSA updateable root of trust, such as the secure partition manager and generic PSA Root of Trust Services such as attestation, secure storage, crypto and firmware update validation.

For the RTOS, the only software component in scope of the security evaluation is the RTOS for the Non-Secure Processing Environment and any related libraries.
RTOS evaluation must rely on an evaluated Chip (See Section 2.4).

For the Device, the scope includes the following software components:

- Applications and libraries developed by the OEM. These may execute in the Non-Secure Processing Environment or as Application Root of Trust Services executed in the Secure Processing Environment.
- Configuration of the RTOS for the device.

Device evaluation must rely on an evaluated Chip and RTOS (See Section 2.4).

## 2.3 Roles for PSA Certified Level 1

PSA Certified Level 1 involves the following roles:

- Chip Vendor: Develops the chip, the PSA Immutable Root of Trust (and possibly Trusted Subsystems) and the components of the updateable PSA Root of Trust (possibly based on Trusted Firmware-M).
- RTOS Vendor: Develops OS and related libraries for the Non-Secure Processing Environment.
- OEM: Conceives and develops a device based on the PSA specifications.
- Evaluation Laboratory: Proceeds to technical review of questionnaires submitted for PSA Certified Level 1 and if successful provides a digital certificate reference number (EAN-13) for the scope under evaluation.
- Certification Secretariat: Receives applications for PSA security certification, issues certificates, updates security certification scheme.

## 2.4 Options for Evaluation

The purpose of PSA Certified Level 1 is to assess the security foundation of a device. The certification is organised in layers: device on top of RTOS on top of Chip. The certificate for a given layer ensures that lower layers, if any, have also been evaluated, either in a previous evaluation (certificates for these lower layers are then reused for composition) or in the evaluation that lead to the considered certificate.

The Chip evaluation can proceed independently, with related PSA Immutable and Updateable Root of Trust and possibly Trusted Subsystems.

The RTOS evaluation can proceed:

- Either on an already certified chip,
- Or on an uncertified chip (no independent certificate will be issued for the chip).

The RTOS certificate is only valid for the selected RTOS and chip combination.

The Device evaluation can proceed:

- Either on an already certified RTOS and chip combination,
- Or on an uncertified RTOS on certified chip (no independent certificate will be issued for the RTOS), or
- Or on an uncertified RTOS and uncertified chip (no independent certificates will be issued for the RTOS and the chip).

The Device certificate is only valid for the selected Device, RTOS and chip combination.

## 2.5 Process for PSA Certified Level 1

The process for level 1 certification of devices based on PSA is the following:

1. The Chip Vendor, the RTOS Vendor or the OEM (all named Developer below) complete the relevant questionnaire provided in Section 4, 5 or 6.
2. For each requirement, the box corresponding to the fulfilment of the requirement is ticked.

- Yes: for fully complies with the requirement.

- Part.: for partially compliance with the requirement (a grey box means not relevant).
- N/A: If the requirement is not applicable.

For fully fulfilled requirement, the Developer has to describe on the line following the statement of the requirement how this requirement is implemented, according to the instructions given *in italic*, or otherwise he has to provide a rationale explaining why this requirement is not fully fulfilled or is not applicable.

3. The Developer submits an application to the PSA Certification Secretariat.
4. The Developer fills the assessment information part in Section 3 and submits the applicable questionnaire(s), according to the selected scope of evaluation, to an Evaluation Lab.
5. The Evaluation Laboratory provides a technical review by checking that the rationale given for each requirement is consistent with the statement of the requirement. The Evaluation Laboratory may ask for clarifications.
6. If the result of the review by the Evaluation Laboratory is Pass, the Evaluation Laboratory will provide an EAN-13 for the chip, RTOS or device, if not already provided by the Developer.
7. The PSA Certification Secretariat proceeds to the certification of the product and the EAN-13 is published along with product or chip reference on the Secretariat's website.

The pass threshold for each of Chip, RTOS or Device is 1 (one) "Part." or "N/A", and the rest "Yes".

For a new product or a variant of an existing product, the Developer can also reuse a questionnaire that has already been reviewed by an Evaluation Laboratory provided the same answers exactly apply. In that case, no action from an Evaluation Laboratory is required and the Developer only has to submit an application to the PSA Certification Secretariat. The EAN-13 for the new product will differ from the product already certified.

## 2.6 Assumptions for the Operational Environment

This document assumes the following assumptions hold regarding the operational environment of the device target of the PSA evaluation:

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

# 3 Assessment Information

The Vendor applying for PSA certification shall fill this section.

## 3.1 Contact

| | |
|---|---|
| **Company activity:** | *(State whether OEM, RTOS Vendor or Chip Vendor)* |
| **Company name:** | |
| **Contact name:** | |
| **Contact title:** | |
| **Contact email:** | |
| **Contact address:** | |
| **Contact phone:** | |

## 3.2 Scope of Evaluation

Check the expected scope for the evaluation and related evaluation option (See Section 2.4):

- ☐ Chip only *(Fill Section 4 only)*
- ☐ RTOS on uncertified chip *(Fill Sections 4 and 5)*
- ☐ RTOS on certified chip *(Fill Section 5 only and provide in Section 3.3 the EAN-13 of the PSA Certified chip)*
- ☐ Device and RTOS on certified chip *(Fill Sections 5 and 6 and provide in Section 3.3 the EAN-13 of the PSA Certified chip)*
- ☐ Device on certified RTOS and certified chip (*Fill Section 6 only and provide in Section 3.3 the EAN-13 of the chip and RTOS that passed PSA Certified. NB: The RTOS must have been certified on the same chip used for this evaluation)*
- ☐ Device, on uncertified RTOS and uncertified chip *(Fill Sections 4, 5 and 6)*

## 3.3 Product Reference

| | |
|---|---|
| **Commercial name:** | |
| **HW reference:** | *(For RTOS and Device, use the reference of the Chip that passed PSA Certified)* |
| **HW version:** | |
| **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)* |
| **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)* |

*For RTOS or Device evaluation:*

| | |
|---|---|
| **RTOS name:** | *(e.g. Mbed OS)* |
| **RTOS version:** | |
| **RTOS EAN-13:** | *(If this version of the RTOS has already passed PSA Certified, specify the EAN-13 of the certificate)* |
| **Reference documentation:** | *(If this version of the RTOS has not yet passed PSA Certified, provide identification of the reference documentation used to fill the questionnaire. It may be requested by the Evaluation Laboratory)* |

## 3.4 Product 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 external resources required for operation of the product, and the related security assumptions)* |

## 3.5 PSA Implementation

*For Chip or RTOS evaluation*:

| | |
|---|---|
| **PSA functional API certified:** | *(For Chip evaluation, PSA Functional API certification is required. Provide the output report from PSA API tests.*<br>*For RTOS evaluation: Yes/No. PSA Functional API certification for RTOS is currently not mandatory but will become a requirement in future revisions of this document.*<br>*If Yes, 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, or declare 'none' if no trusted subsystem is used)* |

## 3.6 Declaration for new questionnaire

This declaration applies for a questionnaire that has not yet been reviewed by an Evaluation Laboratory.

As an authorised representative of the organisation stated in Section 3.1 of this document, I declare that:

1. The information provided in the relevant Section 4, 5, or 6 of this questionnaire is valid and correct for the product/service stated in Section 3.3

and

2. I acknowledge and accept the instructions, exclusions and other provisions set out in this document.

| | |
|---|---|
| **Name:** | |
| **Date:** | |
| **Signature:** | |

## 3.7 Declaration for reuse of an existing certificate

This declaration applies for a product that can reuse the exact same answers to a questionnaire that has already been reviewed by an Evaluation Laboratory and for which related product has passed PSA Certified. In that case, the Vendor does not have to fill again the relevant Section 4, 5, or 6 of this questionnaire and no action from an Evaluation Laboratory is required.

| | |
|---|---|
| **EAN-13 of the product that passed PSA Certified:** | |

As an authorised representative of the organisation stated in Section 3.1 of this document, I declare that:

1. The information provided in the questionnaire for the product referenced above and that is PSA Certified is also valid and correct for the product/service stated in Section 3.2

and

2. I acknowledge and accept the instructions, exclusions and other provisions set out in this document.

| | |
|---|---|
| **Name:** | |
| **Date:** | |
| **Signature:** | |

# 4 Chip Assessment Questionnaire

Skip this section if the version of the chip referenced in Section 3.3 is already PSA-Certified.

## 4.1 Hardware

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| C1.1 | The chip has a hardware mechanism to isolate the Secure Processing Environment (SPE) and related assets from the Non-Secure Processing Environment (NSPE). | | | |
| | *(Describe how isolation is implemented, typically through TrustZone on Cortex-v8M or dual cores on Cortex-v7M)*<br>*Example of response for Yes: The Cortex-M33 (ARMv8-M architecture) supports TrustZone. The Secure Processing Environment is executed in secure mode.* | | | |
| C1.2 | The chip supports secure boot, initiated from immutable code.<br>*NB: Immutable code can be for instance ROM, or EEPROM or FLASH memory that is locked before device delivery.* | | | |
| | *(Describe which cryptographic functions and key sizes are used for secure boot, and how cryptography is implemented, such as hardware cryptographic accelerator or software in immutable code. Also describe how locking is performed if boot code is stored in mutable memory such as EEPROM or FLASH)*<br>*Example of response for Part: The initial Bootloader is run from Boot ROM in secure mode but without prior validation. This Bootloader authenticates the SPE image by hash (SHA-256) and digital signature (RSA-2048) validation. Public key is built into the bootloader image. Metadata of the image is delivered together with the image itself in a header and trailer section. In case of successful authentication, bootloader passes execution to the secure image.* | | | |
| C1.3 | The chip supports security lifecycle, i.e. protect a lifecycle state for the device and enforce transition rules between states.<br>The supported lifecycle states should include at least Device assembly and Test, Factory provisioning, Provisioned and a Debug mode.<br>*NB: Security lifecycle is currently not mandatory but will become a requirement in future revisions of this document.* | | | |
| | *(Describe supported lifecycle states and transition rules)*<br>*Example of response for Yes: The chip supports security lifecycle as defined in [PSA-SM], Section 3.4 - Generic PSA security lifecycle.* | | | |
| C1.4 | The chip supports the secure storage of following keys and ID:<br>• Hardware Unique Key (HUK), with at least with 128-bits of entropy, used for deriving other per device secrets<br>• ROT Public Key (ROTPK), used for authenticating the first stage of SPE code during trusted boot<br>• Unique attestation key (see requirement below)<br>• Instance ID that uniquely identifies the attestation key | | | |

| | | | | |
|---|---|---|---|---|
| | • Implementation ID uniquely identifies the Immutable PSA RoT.<br>These keys and IDs may be injected during initial manufacturing of the silicon or during the final manufacturing of a product or also be derived from a Physically Unique Function (PUF).<br>*NB: The Attestation Key can be derived from the HUK.* | | | |
| | *(Describe key size for each key, and if applicable the key derivation method for the Attestation Key. If HUK is derived from a PUF, provide a rationale of key uniqueness and describe the protection of the function to read the key value)* | | | |

## 4.2 PSA-RoT

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| C2.1 | The updateable PSA-RoT supports firmware update, either from local connectivity (such as USB or removable media) or from remote servers.<br>*NB: Verification of integrity and authenticity for local update currently not mandatory but will become a requirement in future revisions of this document.* | | | |
| | *(Describe how updates are validated, including the cryptographic algorithms used, and where the cryptographic keys used for validation are stored.)* | | | |
| C2.2 | The update mechanism shall prevent firmware downgrade and protect current firmware version in a secure storage, such as anti-rollback counter in protected flash or OTP.<br>*NB: Prevention of firmware downgrade is currently not mandatory but will become a requirement in future revisions of this document.* | | | |
| | *(Describe the firmware versioning information used to detect firmware downgrade and how it is protected in integrity and against decrease and overflow)* | | | |
| C2.3 | The PSA-RoT performs access control for RTOS access, modification and usage of PSA-RoT data and secrets. | | | |
| | *(Describe the subjects concerned by access control and how they are identified or authenticated)* | | | |
| C2.4 | The PSA-RoT uses state of the art cryptography for protection of its assets, as recommended for instance by national security agencies, and does not rely on proprietary cryptographic algorithms or customization of standard cryptographic algorithms.<br>While most implementations will use ECDSA and AES, other cryptographic algorithms can also be used, for instance EdDSA and ChaCha, or Camelia in Japan, or KCDSA in Korea or also SM2, SM3 or SM4 in China.<br>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. | | | |

| | |
|---|---|
| | *(Describe cryptographic algorithms provided by PSA-RoT and supported key sizes. Also describe how random number generation is performed)* |

# 5 RTOS Assessment Questionnaire

Skip this section:

- if the evaluation applies to the Chip only, or
- if the version of the RTOS on the chip referenced in Section 3.3 is already PSA-Certified.

## 5.1 Code Integrity

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| R1.1 | The RTOS supports firmware update, either from local connectivity (such as USB or removable media) or from remote servers.<br>*NB: Verification of integrity and authenticity for local update is currently not mandatory but will become a requirement in future revisions of this document.*<br>If the RTOS supports updates from remote servers, all updates received from remote servers are validated locally to check integrity and authenticity prior installation. This includes manifest, executable code and any related data, such as configuration data. | | | |
| | *(Describe how updates are validated, including the cryptographic algorithms used, and where the cryptographic keys used for validation are stored.)*<br>*Example of response for Yes: The RTOS relies on TF-M firmware upgrade based on swapping method. The new firmware image is downloaded from RTOS and stored in bootloader slot 1 (slot 0 is the active firmware) and marked for update. At the next boot, the bootloader measures and validates the update and swaps slot 1 and slot 0.* | | | |
| R1.2 | The update mechanism shall prevent firmware downgrade and protect current firmware version in a secure storage, such as anti-rollback counter in protected flash or OTP.<br>*NB: Prevention of firmware downgrade is currently not mandatory but will become a requirement in future revisions of this document.* | | | |
| | *(Describe the firmware versioning information used to detect firmware downgrade and how it is protected in integrity and against decrease and overflow)*<br>*Example of response for Yes: In the process described in answer for R1.1, the RTOS verifies firmware version before storing the new image in slot 1. The current version of firmware is stored using secure storage service from TF-M.* | | | |

## 5.2 Data Assets

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| R2.1 | The RTOS relies on PSA-RoT for Device ID queries. | | | |
| | *(Optional notes)* | | | |
| R2.2 | The RTOS makes use of secure storage to protect sensitive application data and secrets and additionally binds the data to a specific device instance. | | | |
| | *(Describe how secure storage is implemented e.g. uses TF-M secure storage)*<br>*Example of response for Yes: The RTOS relies on TF-M (SPE) that supports a secure storage service implementing an AES-GCM based AEAD encryption policy to protect data integrity and authenticity. It uses the flash filesystem and relies on a secret hardware unique key (HUK) per device.* | | | |
| R2.3 | The RTOS uses cryptography as recommended, for instance, by national security agencies, and does not rely on proprietary cryptographic algorithms or customization of standard cryptographic algorithms.<br>In particular the RTOS uses the platform provided cryptographic primitives, including random number generation and key generation, wherever possible.<br>PSA requires 128-bit security.<br>While most implementations will use ECDSA and AES, other cryptographic algorithms can also be used, for instance EdDSA and ChaCha, or Camelia in Japan, or KCDSA in Korea or also SM2, SM3 or SM4 in China. | | | |
| | *(Describe cryptographic algorithms provided by the RTOS, supported key sizes and how the library that provide them, e.g. TF-M crypto libraries)* | | | |

## 5.3 Communication

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| R3.1 | For two-way communication protocols, the RTOS provides the ability to authenticate remote servers before establishing a connection. | | | |
| | *(Optional notes)* | | | |
| R3.2 | The RTOS provides the ability to encrypt data exchanged with remote servers. | | | |
| | *(Optional notes)* | | | |
| R3.3 | For authentication and encryption of two-way communication protocols, the RTOS relies on TLS version 1.2 or later, e.g. Mbed TLS Long Term Support branch. It forbids the fall-back to legacy cipher suite publicly known to be unsecure (such as cipher suites with 3DES, DES, IDEA, RC4, or Null). | | | |

| | | | | |
|---|---|---|---|---|
| | *(Optional notes)* | | | |
| R3.4 | Data input via network protocols is validated defensively against malformed input. | | | |
| | *(Optional notes)* | | | |

## 5.4 Hardening

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| R4.1 | The RTOS provides an attestation token for the current security lifecycle state of the device. | | | |
| | *(Optional notes)* | | | |
| R4.2 | Functionalities that are not needed for the intended usage of the RTOS are disabled or not installed. | | | |
| | *(Optional notes)* | | | |
| R4.3 | The RTOS supports logging of security relevant events and errors and auditing function.<br>Log files protected against tampering.<br>*NB: All devices may not support logging, due to constrained resources for instance.*<br>*Logging is currently not mandatory but will become a requirement in future revisions of this document.* | | | |
| | *(Describe how logs are protected and how they can be retrieved if necessary)* | | | |

## 5.5 Passwords

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| R5.1 | The RTOS does not make use of default password or hardcoded credentials. | | | |
| | *(Optional notes)* | | | |
| R5.2 | The RTOS does not make use of passwords or if it does, it enforces choice of passwords according to security best practices, in particular regarding password length and complexity and number of failed authentication attempts (refer for instance to NIST SP 800-63B-3 guidelines). | | | |
| | *(Optional notes)*<br>*Example of response for Yes: The RTOS does not make use of passwords.* | | | |

## 5.6 Privacy

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| R6.1 | The RTOS does not allow persistent storage of personal data and configuration, or if it does it allows the user to reset the device to erase all this data.<br>*NB: This statement is currently not mandatory but will become a requirement in future revisions of this document.* | | | |
| | *(Optional notes)*<br>*Example of response for Yes: The RTOS does not allow persistent storage of personal data or configuration.* | | | |

# 6 Device Assessment Questionnaire

Skip this section if the scope of evaluation does not include the device.

## 6.1 Code Integrity

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| D1.1 | The device is configured to enforce secure boot for the RTOS and updateable PSA-RoT. Each updatable component is measured and validated prior execution.<br>*NB: Secure boot can rely on chip proprietary mechanisms or on TF-M.* | | | |
| | *(Optional notes)*<br>*Example of response for Yes: The device is configured to rely on TF-M and primitives of Boot ROM for measuring and validating TF-M image prior execution. Then the RTOS relies on the bootloader from Secure Processing Environment (TF-M) for measuring and validating the RTOS image prior to execution.* | | | |

## 6.2 Communication

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| D2.1 | The device does not expose unnecessary communication ports or communication protocol stacks. | | | |
| | *(Optional notes)* | | | |
| D2.2 | The device authenticates remote servers before establishing a connection. | | | |
| | *(Optional notes)* | | | |
| D2.3 | The device encrypts by default all data exchanged with remote servers. | | | |
| | *(Optional notes)*<br>*Example of response for N/A: The device only sends non-confidential information, such as external temperature.* | | | |
| D2.4 | For authentication and encryption, if the device relies on TLS, it should be version 1.2 or later, e.g. Mbed TLS Long Term Support branch. | | | |
| | *(Optional notes)* | | | |

## 6.3 Hardening

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| D3.1 | The device is protected in production against unauthorized use of debug or test features, possibly with rules depending on device lifecycle state.<br>The device erases sensitive user assets and credentials on access to these features. | | | |
| | *(Describe which technical measures disable or deactivate debug)* | | | |
| D3.2 | The current security lifecycle state of the device is attestable through an attestation token. | | | |
| | *(Optional notes)* | | | |
| D3.3 | Functionalities that are not needed for the intended usage of the device are disabled or not installed. | | | |
| | *(Optional notes)* | | | |
| D3.4 | The device supports logging of security relevant events and errors and auditing function.<br>Log files are protected against tampering. | | | |
| | *(Optional notes)* | | | |

## 6.4 Passwords

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| D4.1 | The device does not make use of default passwords or hardcoded credentials. | | | |
| | *(Optional notes)* | | | |
| D4.2 | The device enforces choice of password according to security best practices, in particular regarding password length and complexity and number of failed authentication attempts (refer for instance to NIST SP 800-63B-3 guidelines). | | | |
| | *(Optional notes)* | | | |
| D4.3 | After a fixed threshold of unsuccessful authentications against a password, the password is either disabled or a timeout is applied before another authentication attempt is allowed. | | | |
| | *(Optional notes)* | | | |
| D4.4 | The device implements an inactivity time-out or other appropriate mechanism to prevent perpetual authorization. | | | |
| | *(Optional notes)* | | | |
| D4.5 | Passwords, and other credentials, are stored on secure storage. | | | |
| | *(Optional notes)* | | | |

## 6.5 Privacy

| ID | Requirement | Response | | |
|---|---|---|---|---|
| | | Yes | Part. | N/A |
| D5.1 | Personal data, including in log files, is protected by access controls means. | | | |
| | *(Optional notes)* | | | |
| D5.2 | Personal data is stored on a secure storage. | | | |
| | *(Optional notes)* | | | |