PSA Certified™ Level 1 Questionnaire

Document number:	JSADEN0001	Version:	1.0
Date of Issue:	25/02/2019		
Author:	PSA JSA Members: Arm Limited Brightsight B.V. CAICT Prove & Run S.A.S. Riscure B.V. UL TS B.V.		
Authorized by:	PSA JSA Members		

Abstract

PSA Certified is the independent security evaluation scheme for 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 test labs. 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

1.1 Current status and anticipated changes

Current Status: Final

1.2 Change history

Release Date	Version	Comments
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 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 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 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
Trusted boot	Trusted Boot is technology to provide a chain of trust for all the components during boot

1.5 Feedback

Arm welcomes feedback on its documentation.

If you have comments on the content of this documentation, send an e-mail to psacertified@arm.com. Give:

- The title (PSA Certified Level 1 Questionnaire).
- The number (JSADEN-001).
- 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 and allowing secure products and features to be developed on top. It is expected that PSA API compliance (functional certification) will be an initial step in achieving secure products that are later evaluated by test labs as part of the PSA Certified scheme.

The terms 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 PSA functional security APIs and has passed a test suite provided by Arm. Arm supplies a reference implementation as open source software – Trusted Firmware-M

- *PSA Certified*

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

The PSA 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*.

Level 1 for assurance (not to be confused with SPM isolation levels), which is the target of this document, relies on a questionnaire assessment filled out by the semiconductor manufacturer, OS vendor or OEM on the security of its device with respect to baseline IoT security requirements to mitigate common IoT threats and the expected security requirements for PSA products. This assessment is checked 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 test lab or by the company seeking certification. PSA devices support Entity Attestation Token that can use the EAN-13 as an identifier of the chip type to inform relying parties that the chip PSA-RoT has been evaluated using the questionnaire provided in the following sections.

2.2 Scope for Security Evaluation

The scope for security evaluation is the combination of the hardware and software components supporting a device. The considered hardware may be a System-in-Package (SiP) or a System-on-Chip (SoC) integrated on a board.

For Chip Vendors, the hardware is in scope of the security evaluation as it provides security features, such as immutable storage or protection of debug features, which are essential for ensuring the security of the PSA implementation. The scope also includes, the following software components from the PSA platform, as described in [PSA-FF]:

- PSA immutable root of trust, for example Boot ROM, Root secrets and IDs, Isolation hardware, Security lifecycle management and enforcement.
- 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.

- PSA updateable root of trust, such as Software isolation framework, protecting more trusted software from less trusted software, Generic services such as Entity Attestation Token (EAT) generation, secure storage, generic crypto services, FW update validation.

For RTOS and integrated PSA-RoT Vendors, the software components in the scope of security evaluation are:

- OS for the Non-Secure Processing Environment.

For OEMs, the software components in the scope of security evaluation are:

- Applications and libraries developed by the OEM. They may be split between parts executed on the Non-Secure Processing Environment and on the Secure Processing Environment.

Figure 1 below illustrates the components of a PSA architecture with related scopes of evaluation. 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.

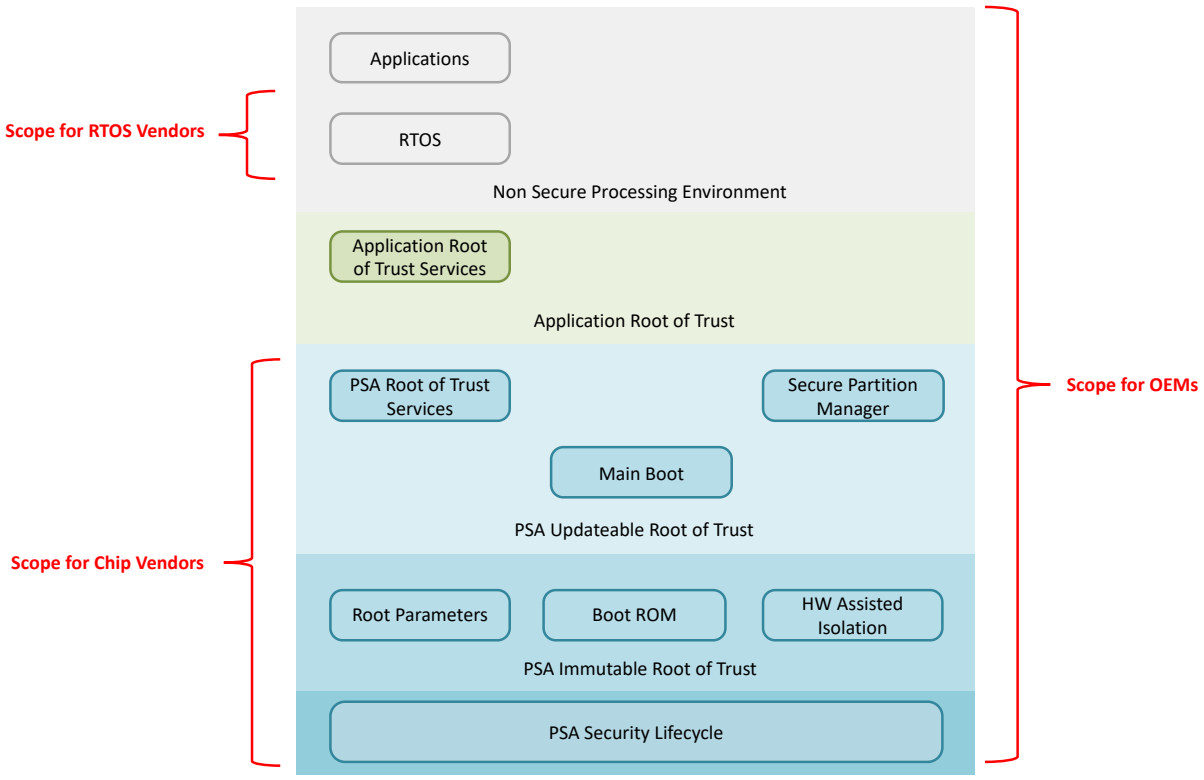

Figure 1: Scope of PSA Certified Level

2.3 Roles for PSA Certified Level 1

PSA Certified Level 1 for devices based on the PSA architecture involves the following roles:

- Arm: Issues PSA functional and security specification.

- OEM: Conceives and develops a device based on PSA specification, i.e., integrates a PSA platform on the device, develops applications or libraries on top of the platform.
- Chip Vendor: Develops the chip, the PSA Immutable Root of Trust and possibly Trusted Subsystems, and the updateable PSA components for the Secure Processing Environment, e.g. integrating Trusted Firmware-M.
- RTOS Vendor: Develops OS and related libraries for the Non-Secure Processing Environment.
- Certification Secretariat: Receives applications for PSA security certification, issues certificates, updates security certification scheme.
- 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 a SoC or product.

2.4 Process for PSA Certified Level 1

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

1. The Chip Vendor, the RTOS Vendor or the OEM (for short, the Developer below) proceeds to the self-assessment of its product (chip, RTOS and integrated device respectively) using the dedicated questionnaires provided in Section 4, 5 or 6 respectively.
2. For each requirement, the Developer shall check the box corresponding to the fulfilment of the requirement by its product:

- Yes: If the product fully complies with the requirement.
- Part.: If the product partially complies with the requirement (box greyed for requirements "Part." is not relevant).
- N/A: If the requirement is not applicable for the product.

For a product fully compliant with the requirement, the Developer may also have to describe on the line following the statement of the requirement how this requirement is implemented, according to the instructions given *in italic*.

For a product not fully compliant with the requirement (box "Part". or "N/A" checked), the Developer has to provide on the line following the statement of the requirement a rationale explaining why this requirement is not fulfilled.

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 full questionnaire to a test 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 clarifications.
6. If the result of the review by the Evaluation Laboratory is Pass, the test lab will provide a PSA_ID for the chip or device.
7. The PSA Certification Secretariat proceeds to the certification of the product and the PSA_ID is published along with product or chip reference on the Secretariat's website.

The pass threshold for each of the 3 sections (Chip Vendor, RTOS Vendor or OEM) 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 have to submit an application to the PSA Certification Secretariat.

2.5 Use of PSA Certified Level 1 Security Certificates

The purpose of PSA Certified Level 1 is to assess the security foundation of a device. The certification is organised in layers (chip, RTOS, device), each one associated to a role (Chip Vendor, RTOS Vendor, OEM) during the development of a device.

The Chip Vendor can proceed independently to certification of its chip, with related PSA Immutable Root of Trust and possibly Trusted Subsystems.

The RTOS Vendor has to use an already certified chip. Reuse of an existing RTOS certificate on a different chip requires another evaluation, but it should be a straightforward step if the new chip complies similarly to the Chip Vendors requirements for the other chip (i.e. same requirements fulfilled, with a similar implementation).

The OEM has to use an already certified RTOS (and thus on an already certified chip). The certificate is only valid for the device composed of the selected chip, RTOS and integrated OEM software.

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 Product Reference

Product name:	
EAN-13:	*(As used in the HW version claim of the chip attestation token)*
HW reference:	*(For RTOS Vendors and OEM, use the reference that passed PSA Certified for Chip Vendors)*
HW version:	
SPE name:	*(e.g. Trusted Firmware-M)*
SPE version:	
NSPE name:	*(e.g. Mbed OS)*
NSPE version:	

3.3 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)*

3.4 PSA Implementation

For Chip Vendors and RTOS Vendors:

PSA functional API certified:	*(For Chip vendors, PSA Functional API certification is required. Provide the output report from PSA API tests.*

	For RTOS vendors: Yes/No. This requirement is not mandatory for the first products that will be evaluated in 2019 *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)*

3.5 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 3.2

and

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

Name:	
Date:	
Signature:	

3.6 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 passed PSA Certified. In that case, the Vendor does have 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 passed 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 Assessment Questionnaire – For Chip Vendors

For RTOS Vendor or OEMs, skip this Section and proceed respectively to Section 5 or 6.

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.			
	(Describe how isolation is implemented, typically through TrustZone on Cortex-v8M or dual cores on Cortex-v7M) *Example of response for Yes: The Cortex-M33 (ARMv8-M architecture) supports TrustZone. The Secure Processing Environment is executed in the Secure mode.*			
C1.2	The chip provides trusted boot support, initiated from immutable code. *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 trusted 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) *Example of response for Part: The Boot ROM runs the Bootloader in secure mode but without prior validation. The 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. The supported lifecycle states should include at least Device assembly and Test, Factory provisioning, Provisioned and a Debug mode. *NB: This requirement is not mandatory for the first products that will be evaluated in 2019.*			
	(Describe supported lifecycle states and transition rules) *Example of response for Yes: The chip supports security lifecycle as defined in [PSA-SM], §E - Generic PSA security lifecycle.*			
C1.4	The chip supports the secure storage of following keys: • Hardware Unique Key (HUK), with at least with 256-bits of entropy, used for deriving other per device secrets • RoT Public Key (RoTPK), used for authenticating the first stage of SPE code during trusted boot • Unique attestation key (see requirement below). These keys 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).			

	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)			

5 Assessment Questionnaire – For RTOS Vendors

For Chip Vendors or OEMs, skip this Section.

5.1 Code Integrity

ID	Requirement	Response		
		Yes	Part.	N/A
R1.1	The RTOS and updateable PSA-RoT supports firmware update, either from local connectivity (such as USB or removable media) or from remote servers. *NB: Verification of integrity and authenticity for local update is not mandatory for the first products that will be evaluated in 2019.* 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 are stored the cryptographic keys used for validation) *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 on 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. *NB: This requirement is not mandatory for the first products that will be evaluated in 2019.*			
	(Describe the firmware versioning information used to detect firmware downgrade and how it is protected in integrity and against decrease and overflow) *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 protects in integrity the Device ID.			
	(Optional notes) *Example of response for Yes: The RTOS uses the secure storage service provided by PSA-RoT to protect in integrity the Device ID.*			
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) *Example of response for Yes: The RTOS relies on SPE (TF-M) 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 PSA-RoT performs access control from RTOS for access, modification and usage of PSA-RoT data and secrets.			
	(Describe the subjects concerned by access control and how they are identified or authenticated)			
R2.4	The RTOS uses state of the art cryptography, as recommended for instance by national security agencies, and does not rely on proprietary cryptographic algorithms or customization of standard cryptographic algorithms. In particular the RTOS uses the platform provided cryptographic primitives, including for random number generation and key generation, wherever possible. PSA requires 128-bit security. However, you may choose an appropriate cipher suite. While we expect most implementations will use ECDSA and AES, you do not have to use this suite. You may use for instance EdDSA and ChaCha, or Camelia in Japan, or KCDSA in Korea or also SM2, SM3 or SM4 in China.			
	(Describe cryptographic algorithms used on the device, related 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 authenticates remote servers before establishing a connection.			
	(Optional notes)			
R3.2	The RTOS encrypts by default all 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.			
	(Optional notes)			
R3.4	The network protocols provided by the RTOS are programmed defensively against malformed inputs.			
	(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. Log files protected against tampering. *NB: All devices may not support logging, due to constrained resources for instance.* *This requirement is not mandatory for the first products that will be evaluated in 2019.*			
	(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) *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. *NB: This requirement is not mandatory for the first products that will be evaluated in 2019.*			
	(Optional notes) *Example of response for Yes: The RTOS does not allow persistent storage of personal data or configuration.*			

6 Assessment Questionnaire – For OEM

For Chip Vendors or RTOS Vendors, skip this Section.

6.1 Code Integrity

ID	Requirement	Response		
		Yes	Part.	N/A
D1.1	The device is configured to enforce trusted boot for RTOS and updateable PSA-RoT. Each updatable component is measured and validated prior execution. *NB: The trusted boot can rely on chip proprietary mechanisms or on TFM.*			
	(Optional notes) *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 execution.*			

6.2 Communication

ID	Requirement	Response		
		Yes	Part.	N/A
D2.1	The device does not expose unnecessary communication ports or communication protocol stack.			
	(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) *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. 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. 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)			