PSA Certified™ Level 1 Questionnaire Version 2.0

psacertified™

psacertified™
level one

Document number:	JSADEN001
Version:	2.0 Beta
Release Number:	01
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:	10/02/2020

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, System software 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

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

Contents

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Final

1.2 Release Information

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

Date	Version	Confidentiality	Change
10/02/2020	2.0	Non-confidential	Updates and alignment with ETSI 303 645, NISTIR 8259 and SB-327 standards
30/10/2019	1.2	Non-confidential	Clarifications for possible evaluation scopes and alignments with PSA Certified Level 2
01/04/2019	1.1	Non-confidential	Clarifications on PSA Functional API Certification and PSA Functional APIs
13/02/2019	1.0	Non-confidential	Public release based on BET03 version

1.3 References

This document refers to the following informative 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
[SP800-63B]	ETSI EN 303 645	ETSI	Cyber Security for Consumer Internet of Things; Draft V2.0.0 (2019-11)
[8259]	NISTIR 8259	NIST	Core Cybersecurity Feature Baseline for Securable Manufacturers; Draft (2nd) January 2020
[SB-327]	Bill No. 327; Chapter 886.	California State Senate	Information privacy: connected devices

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations

Term	Meaning
Application firmware	The main application firmware for the platform, typically comprising a System software and application tasks. PSA provides no isolation services for this firmware, although the System software may make use of available hardware support to provide internal isolation of operation
Application Root of Trust	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
Critical Security Parameter	Secret information, with integrity and confidentiality needs, used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic key
Evaluation laboratory	Laboratory or facility that performs the technical review of questionnaires submitted for PSA Certified Level 1. The list of evaluation laboratories participating to PSA Certified can be found on www.psacertified.org
Hardware Unique Key (HUK)	Secret and unique to the device – 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 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 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
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 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 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 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.

PSA JSA Members also welcome general suggestions for additions and improvements.

Note

PDFs are tested only in Adobe Acrobat and Acrobat Reader and cannot guarantee the appearance or behaviour of any document when viewed with any other PDF reader.

2 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 Certified, and PSA Functional API Certification are used here with the following meanings:

- *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 Body (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 device, including its critical assets, is not vulnerable to identified threats. 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, System software or device has been evaluated and PSA Certified.

- *PSA Functional API Certification*

  PSA Functional API Certification means that a device has implemented the PSA Functional APIs[1] and passed the PSA Functional API Certification test suites. The PSA Functional 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 www.psacertified.org/resources.

The PSA Certified scheme 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*.

PSA Certified Level 1 assurance[2], the target of this document, relies on questionnaires filled out by the chip vendor, the System software vendor or the OEM. The questionnaire defined in this document covers the baseline IoT security requirements to mitigate common IoT threats and security requirements for PSA products. The Evaluation Laboratory rely on this questionnaire to examine the device security measures.

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 System software and the Device. Figure 1 illustrates the components in the PSA architecture and the related security certification scopes. This figure

[1] https://pages.arm.com/psa-apis.html
[2] PSA Certified security assurance levels are distinct from the isolation levels, which characterize different types of software isolation, defined in the PSA specifications.

distinguishes a Non-secure Processing Environment (NSPE) and a Secure Processing Environment (SPE), for which the chip shall provide isolation[1].

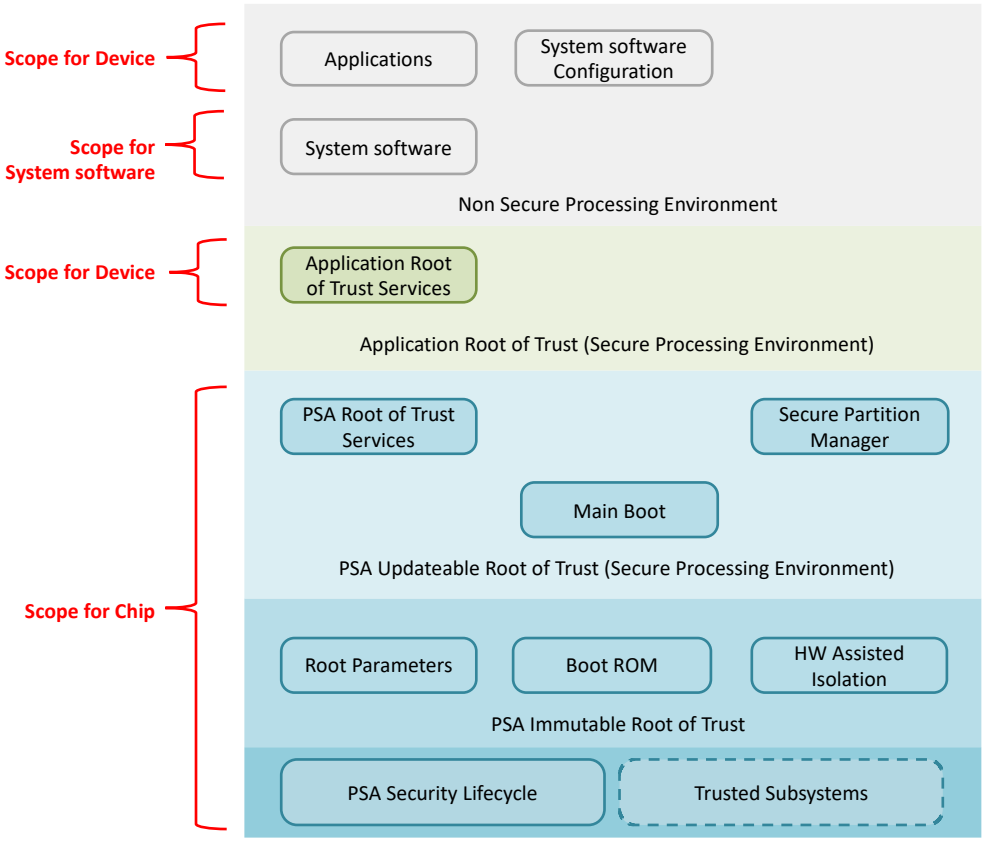

Figure 1: Logical Scope of PSA Certified Level 1

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.

[1] 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.

For the System software, the scope of the security evaluation is the System software for the Non-secure Processing Environment and any related libraries. System software 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 System software for the device.

Device evaluation must rely on an evaluated Chip and System software (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)
- System software 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: Performs the 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 Body: 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 the System software, on top of the Chip. The certificate for a given layer ensures that lower layers have either been separately evaluated (the certificates for which are then referenced) or are covered in the evaluation that lead to the considered certificate.

1. The Chip evaluation can proceed independently

2. The System software evaluation can proceed either;
   - on an already certified chip,
   - or on an uncertified chip (no independent certificate will be issued for the chip).

   The System software Certificate is only valid for the selected System software and chip combination.

3. The Device evaluation can proceed either;
   - on an already certified System software and chip combination,

- or on an uncertified System software on a certified chip (no independent certificate will be issued for the System software),
- or on an uncertified System software and uncertified chip (no independent certificates will be issued for the System software and the chip).

The Device Certificate is only valid for the selected Device, System software and chip combination.

2.5 Process for PSA Certified Level 1

The process for Level 1 certification is the following:

1. The Chip Vendor, the System software Vendor or the OEM (all named Developer below) complete the relevant questionnaire provided in sections 4, 5 or 6 respectively.
2. For each requirement, the box corresponding to the fulfilment of the requirement is ticked as follows:
   - Yes: for full compliance with the requirement
   - Part.: for partial compliance with the requirement (a grey box means not relevant)
   - N/A: if the requirement is not applicable.

For a 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 guidance given *in italic*, or otherwise has to provide a rationale explaining why this requirement is not fully fulfilled or is not applicable.

3. 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 Laboratory.
4. The Evaluation Laboratory performs the 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 clarification. The Evaluation Laboratory submits an application to the PSA Certification Body on behalf of the Developer.
5. If the result of the review by the Evaluation Laboratory is Pass, the Evaluation Laboratory will provide an EAN-13 for the Chip, System software or Device, if not already provided by the Developer.
6. The PSA Certification Body proceeds to the certification of the product and the EAN-13 is published along with product reference on the Body's website.

The pass threshold for each section of Chip, System software or Device is at most 1 (one) question not answered in conformance with the "Expected answer" on the marking sheet of Appendix D with a rationale of why security is unaffected. Requirements marked as Optional must not be considered in the count.

For a new product or a variant of an existing product, the Developer can reuse a questionnaire that has already been reviewed by an Evaluation Laboratory provided exactly the same answers 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 Body. The EAN-13 for the new product will differ from the product already certified.

2.6 Operational Environment Assumptions

The following assumptions hold regarding the operational environment of the device target of the evaluation:

- The device manufacturing process ensures integrity and authenticity of the hardware design and any 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 all applicable parts of this section.

3.1 Contact

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

3.2 Scope of Evaluation

Check the box for the scope for this evaluation (see section 2.4):

- ☐ Chip only; fill in section 4.
- ☐ System software on an uncertified chip; fill *in sections 4 and 5*.
- ☐ System software on a certified chip; fill in section 5 and provide in section 3.3 the EAN-13 of the PSA Certified chip.
- ☐ Device and System software on a certified chip, fill in sections 5 and 6 and provide in section 3.3 the EAN-13 of the PSA Certified chip.
- ☐ Device on certified System software and certified chip; fill section 6 and provide in section 3.3 the EAN-13 of the Chip and System software that passed PSA Certified. NB: The System software must have been certified on the same chip used for this evaluation)
- ☐ Device on an uncertified System software and an uncertified chip; *fill in sections 4, 5 and 6*.

3.3 Product Reference

This declaration is applicable to Chip, System software or Device evaluation.

Commercial name:	*(e.g. Product family)*
Chip part number:	
Chip version:	*(e.g. Chip silicon revision)*
SPE name:	*(e.g. Trusted Firmware-M)*
SPE version:	
Chip EAN-13:	*(If this version of the chip has already passed PSA Certified, specify the EAN-13 of the certificate)*
Chip reference documentation:	*(If this version of the chip has not yet passed PSA Certified, provide identification of the reference documentation used to fill the questionnaire, such as chip datasheet, detailed fact sheet or reference manual. It may be requested by the Evaluation Laboratory)*
Vulnerability disclosure policy:	*(If a vulnerability disclosure policy is available for this product, provide the URL it can be retrieved. See Appendix A.2 for more information)*

Additionally, for System software or Device evaluation this declaration is required.

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

3.4 Product Description

This declaration applies for a Device evaluation.

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

3.5 PSA Implementation

For Chip or System software evaluation:

PSA Functional API certified:	*PSA Functional API Certification is optional.* *If PSA API tests have been performed, then provide the output reports to the Evaluation Laboratory.*
Isolation boundary level:	*As described in [PSA-FF]:* ☐ *Isolation level 1: isolation boundary between the SPE and the NSPE* ☐ *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)*

3.6 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 sections 4, 5, or 6, as required, 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 reuses the exact same answers to a questionnaire that has already been reviewed by an Evaluation Laboratory and for which the 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 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 referred in Section 3.3 is already PSA Certified.

NB: When this section is filled by the System software Vendor or OEM, he may provide answers that apply only to the context in which the chip is used. For instance, he may only provide in C2.4 the cryptographic algorithms he is relying on, not all the algorithms supported by the chip.

4.1 Hardware

ID	Requirement	Supported?		
		Yes	Part.	N/A
C1.1	The chip shall rely on 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, for example through TrustZone or dual cores.) *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 shall support secure boot, 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 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.) *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 SPE image.*			
C1.3 (Optional)	The chip shall support security lifecycle, i.e. protecting sensitive data based on device lifecycle state and enforcing the rules for transition between states. The supported lifecycle states should include at least Device assembly and test, Factory provisioning, Provisioned and a Debug mode. *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) *Example of response for Yes: The chip supports security lifecycle as defined in [PSA-SM].*			
C1.4	The chip shall support the storage of following keys and IDs, in such a way that it resists tampering by means such as physical, electrical or software (such as external probing of the chip for confidential data): • Hardware Unique Key (HUK), with at least with 128-bits of entropy, used for deriving other per device secrets • RoT Public Key (ROTPK), used for authenticating the first stage of SPE code during secure boot • Unique attestation key (see requirement below) • Instance ID that uniquely identifies the attestation key • Implementation ID uniquely identifies the Immutable PSA-RoT. These keys and IDs may be injected during initial manufacturing of the silicon or during the final manufacturing of a product. They can also be derived from a Physically Unique Function (PUF) or 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. Describe the protection of the functions to read the keys. *Also describe how the chip data is protected from tampering.)*			

4.2 PSA-RoT

ID	Requirement	Supported?		
		Yes	Part.	N/A
C2.1	The PSA-RoT shall support firmware update, either from local connectivity (such as USB or removable media) or from remote servers. Updates shall be validated locally to check integrity and authenticity prior installation. This includes manifest, executable code and any related data, such as configuration data. The cryptography used for firmware update shall comply to requirement C2.4.			
	(Describe how updates are validated, including the cryptographic algorithms used, and where the cryptographic keys used for validation are stored.			

ID	Requirement	Supported?		
		Yes	Part.	N/A
	NB: Justification is required if local validation of update from remote servers prior to installation cannot be supported, typically due to resource constraints.)			
C2.2	The update mechanism shall allow to prevent unauthorized firmware rollback and protect current firmware version number in secure storage, such as anti-rollback counter in protected flash or OTP. This feature can be activated or deactivated before device delivery, or after delivery using device configuration (see R6.1).			
	(Describe the firmware versioning information used to detect firmware rollback and how it is protected in integrity and against decrease and overflow)			
C2.3	The PSA-RoT shall perform access control for modification and use of PSA-RoT data and secrets by System software.			
	(Describe the System software subjects concerned by access control and how they are identified or authenticated)			
C2.4	The PSA-RoT shall use best practice cryptography for protection of its assets, as recommended for instance by national security agencies, and not rely on proprietary cryptographic algorithms or customization of standard cryptographic algorithms. PSA requires equivalence of at least 128-bit security. *NB: While most implementations will use ECDSA and AES, other cryptographic algorithms can be used, for instance EdDSA and ChaCha, or Camelia in Japan, or KCDSA in Korea or SM2, SM3 or SM4 in China.* *Weak cryptographic algorithms or key sizes may be available for specific uses (e.g. legacy) and with specific guidance. They shall not be used in any way that reduces the security of the best practice cryptography.*			
	(List the cryptographic algorithms provided by PSA-RoT and supported key sizes. Also describe how random number generation is performed.)			

5 System Software Assessment Questionnaire

Skip this section:

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

NB: When this section is filled by the OEM, he can provide answers that apply only to the context in which the System software is used. For instance, the OEM may only provide in R2.3 the cryptographic algorithms he is relying on, not all the algorithms supported by the System software.

5.1 Code Integrity

ID	Requirement	Supported?		
		Yes	Part.	N/A
R1.1	The System software shall support firmware update, either from local connectivity (such as USB or removable media) or from remote servers. Updates shall be validated locally to check integrity and authenticity prior installation. This includes manifest, executable code and any related data, such as configuration data. The cryptography used for firmware update shall comply with requirement R2.3.			
	(Describe how updates are validated, including the cryptographic algorithms used, and where the cryptographic keys used for validation are stored. *NB: Justification is required if local validation of update from remote servers prior to installation cannot be supported, typically due to resource constraints.)* *Example of response for Yes: The System software relies on TF-M firmware upgrade based on swapping method. The new firmware image is downloaded by the System software 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 allow to prevent unauthorized firmware rollback and protect current firmware version number in a secure storage, such as anti-rollback counter in protected flash or OTP. This feature can be activated or deactivated before device delivery, or after delivery using device configuration (see R6.1).			
	(Describe the firmware versioning information used to detect firmware rollback and how it is protected in integrity and against decrease and overflow)			

ID	Requirement	Supported?		
		Yes	Part.	N/A
	Example of response for Yes: In the process described in answer for R1.1, the System software verifies firmware version in secure storage 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	Supported?		
		Yes	Part.	N/A
R2.1	The System software shall rely only on PSA-RoT for Device ID queries.			
	(Optional notes)			
R2.2	The System software shall use of secure storage to protect sensitive critical security parameters and also provide this functionality for application data. It shall additionally bind the data to a specific device instance and, if supported, security lifecycle state (refer to requirement C1.3). The cryptography used for secure storage shall comply to requirement R2.3.			
	(Describe how secure storage is implemented e.g. uses TF-M secure storage) *Example of response for Yes: The System software 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 System software shall use best practice 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 System software shall use the PSA-RoT provided cryptographic primitives, including random number generation and key generation, wherever possible. PSA requires equivalence of at least 128-bit security. *NB: While most implementations will use ECDSA and AES, other cryptographic algorithms can be used, for instance EdDSA and*			

ID	Requirement	Supported?		
		Yes	Part.	N/A
	ChaCha, or Camelia in Japan, or KCDSA in Korea or SM2, SM3 or SM4 in China.			
	(Describe cryptographic algorithms provided by the System software, supported key sizes and how the library that provide them, e.g. TF-M crypto libraries)			
R2.4	The System software shall support update of cryptographic algorithms and primitives.			
	(Optional notes)			

5.3 Communication

ID	Requirement	Supported?		
		Yes	Part.	N/A
R3.1	For two-way communication protocols and for each network interface, the System software shall provide the ability to authenticate remote servers or users in the act of establishing a connection.			
	(Optional notes)			
R3.2	The System software shall provide the ability to encrypt data exchanged with remote servers.			
	(Optional notes)			
R3.3	The System software shall use secure protocols, compliant to requirement R2.3, for authentication and encryption of two-way communication. If the System software relies on TLS, the version shall be 1.2 or later, and it shall forbid the fall-back to legacy cipher suite publicly known to be unsecure (such as cipher suites with 3DES, DES, IDEA, RC4, or Null).@ *NB: This can be met with actively supported versions of Mbed TLS Long Term Support branch.*			
	(Optional notes)			

5.4 Hardening

ID	Requirement	Supported?		
		Yes	Part.	N/A
R4.1	The System software shall provide 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 System software shall be disabled or not installed.			
	(Optional notes)			
R4.3 (Optional)	The System software should provide logging of security relevant events and errors and auditing function. The log should include sufficient details to determine what happened. *NB: Not all devices may support logging, due to constrained resources for instance. 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)			
R4.4	If the System software supports logging, it shall restrict access to log files to authorised users only (refer to R5.3).			
	(Optional notes)			
R4.5	Data input from user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated defensively against malformed input.			
	(Optional notes)			

5.5 Passwords

ID	Requirement	Supported?		
		Yes	Part.	N/A
R5.1	If the System software makes use of critical security parameters (including passwords), they shall be unique per device or defined by the user. They shall not be resettable to any universal factory default value.			
	(Optional notes)			

ID	Requirement	Supported?		
		Yes	Part.	N/A
R5.2	If the System software makes use of passwords, it shall enforce 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 guidelines for memorized secrets).			
	(Optional notes) *Example of response for Yes: The System software requires passwords of at least 8 characters in length, not in dictionary words or with repetitive or sequential characters. Additionally, the System software implements a rate-limiting mechanism (applying an increasing timeout) that limits the number of failed authentication attempts.* *Example of response for Yes: The System software does not make use of passwords.*			
R5.3	If the System software makes use of critical security parameters for user authentication, the cryptography used for that feature shall comply with requirement R2.3.			
	(Describe the cryptography used for user authentication)			

5.6 Configuration

ID	Requirement	Supported?		
		Yes	Part.	N/A
R6.1	If the System software allows security-relevant configuration changes via a network interface, the related configuration shall only be accepted after authentication (refer to R3.1, R3.3 and R5.3). *NB: Security-relevant changes include:* • *access control management for remote or local users,* • *configuration of network keys,* • *passwords policy (such as changes or thresholds),* • *update policy (such as query frequency, automatic installation, server address, rollback),* • *configuration of cryptography (such as default key length),* • *access to network interfaces and authentication policy (such as account lock thresholds after failed authentication attempts).*			

	Example of response for Yes: The System software allows security-relevant configuration changes after the administrator has been successfully authenticated in a local interface through the mechanism described in R5.3. *Other example of response for Yes: The System software does not allow security-relevant configuration changes.*

5.7 Privacy

ID	Requirement	Supported?		
		Yes	Part.	N/A
R7.1	If the System software allows persistent storage of personal data and configuration, it shall allow the user to erase all this data.			
	(Optional notes) *Example of response for Yes: The System software does not allow persistent storage of personal data or configuration.* *Other example of response for Yes: The System software erases all data and resets to factory settings.*			

6 Device Assessment Questionnaire

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

6.1 Code Integrity

ID	Requirement	Supported?		
		Yes	Part.	N/A
D1.1	The device shall be configured to enforce secure boot for the System software and updateable PSA-RoT. Each updatable component shall be measured and validated prior to execution.			
	(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 to execution. Then the System software relies on the bootloader from the Secure Processing Environment (TF-M) for measuring and validating the System software image prior to execution.*			

6.2 Communication

ID	Requirement	Supported?		
		Yes	Part.	N/A
D2.1	The device shall close unused network ports and logical interfaces.			
	(Optional notes)			
D2.2	For two-way communication protocols, the device shall provide the ability to authenticate remote servers in the act of establishing a connection.			
	(Optional notes)			
D2.3	The device shall encrypt by default all data exchanged with remote servers. In particular critical security parameters shall always be encrypted			
	(Optional notes) *Example of response for N/A: The device only sends non-confidential information, such as external temperature. This information does not need to be encrypted.*			

ID	Requirement	Supported?		
		Yes	Part.	N/A
D2.4	The device shall use secure protocols, compliant to requirement R2.3, for authentication and encryption of two-way communication. If the device relies on TLS, the version shall be 1.2 or later, and it shall forbid the fall-back to legacy cipher suite publicly known to be unsecure (such as cipher suites with 3DES, DES, IDEA, RC4, or Null). NB: This can be met with actively supported versions of Mbed TLS Long Term Support branch.			
	(Optional notes)			

6.3 Hardening

ID	Requirement	Supported?		
		Yes	Part.	N/A
D3.1	The device shall be protected in production against unauthorised use of debug or test features, possibly with rules depending on device lifecycle state. The device shall erase 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 shall be attestable through an attestation token.			
	(Optional notes)			
D3.3	Functionalities that are not needed for the intended usage of the device shall be disabled or not installed.			
	(Optional notes)			
D3.4 (Optional)	The device should support logging of security relevant events and errors and auditing function. The log should include sufficient details to determine what happened.			

ID	Requirement	Supported?		
		Yes	Part.	N/A
	NB: Not all devices may support logging, due to constrained resources for instance. 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)			
D3.5	If the device supports logging, it shall restrict access to log files to authorised users only.			
	(Optional notes)			

6.4 Passwords

ID	Requirement	Supported?		
		Yes	Part.	N/A
D4.1	If the device makes use of critical security parameters (including passwords), they shall be unique per device or defined by the user. They shall not be resettable to any universal factory default value.			
	(Optional notes)			
D4.2	If the device makes use of passwords, it shall enforce choice of these passwords according to security best practices, in particular regarding password length and complexity (refer for instance to NIST SP 800-63B guidelines).			
	(Optional notes)			
D4.3	If the device makes use of passwords, and after a fixed threshold of unsuccessful authentications against a password, the device shall either disable password or apply a timeout before another authentication attempt is allowed.			
	(Optional notes)			
D4.4	If the device makes use of critical security parameters for authorisation, it shall implement an inactivity time-out or other appropriate mechanism to prevent perpetual authorisation.			
	(Optional notes)			
D4.5	If the device makes use of critical security parameters, it shall use secure storage to protect them.			
	(Optional notes)			

6.5 Privacy

ID	Requirement	Supported?		
		Yes	Part.	N/A
D5.1	The device shall restrict access to log personal data, including in log files, to authorised users only			
	(Optional notes)			
D5.2	The device shall store personal data on a secure storage.			
	(Optional notes)			

6.6 Organizational

ID	Requirement	Supported?		
		Yes	Part.	N/A
D6.1 (Optional)	The Developer should provide a public point of contact as part of its vulnerability disclosure policy.			
	(Optional notes)			
D6.2 (Optional)	The Developer should explicitly state the minimum length of time for which the device will receive security updates.			
	(Optional notes)			

Appendix A Organisational Best Practices

In addition to the technical security measures that are in the scope of PSA Certified Level 1 through the requirements expressed in sections 4 to 6, this appendix provides organizational best practices that contribute to comprehensive device security.

Verification of compliance to these organizational security best practices is **not** part of the tasks performed by Evaluation Laboratories during the course of a PSA Certified Level 1 evaluation.

A.1 Device Identification

ID	Best practice
BP1.1	The device model designation should be easily visible to the end-user.
BP1.2	The device identification number should be easily visible to the end-user.

A.2 Vulnerability Disclosure

ID	Best practice
BP2.1	The Developer should publish a vulnerability disclosure policy, easily accessible from its website.
BP2.2	The Developer should provide a public point of contact as part of its vulnerability disclosure policy.
BP2.3	The Developer should act on a timely manner after knowledge of a vulnerability and provide security updates.
BP2.4	The Developer should actively monitor for vulnerabilities likely to affect security of its devices.
BP2.5	The Developer should notify the end-user of known vulnerabilities and possible mitigations.

A.3 Update

ID	Best practice
BP3.1	The device should install by default available updates.
BP3.2	The device should check after initialization for available updates.
BP3.3	The Developer should explicitly state the minimum length of time for which the device will receive security updates.

A.4 Critical Security Parameters

ID	Best practice
BP4.1	The Developer should ensure uniqueness for pre-installed Critical Security Parameters.
BP4.2	The Developer should that pre-installed Critical Security Parameters are generated with sufficient entropy.
BP4.3	The Developer should follow a secure management process for the protection of Critical Security Parameters stored outside the device.

A.5 Installation and Maintenance

ID	Best practice
BP5.1	The Developer should design device installation and maintenance processes to employ minimal steps while ensuring security.
BP5.2	The Developer should provide clear guidance to the end-user for device installation and maintenance.

A.6 Privacy

ID	Best practice
BP6.1	The Developer should inform the end-user when personal data is processed, by who and for which purpose and obtain clear consent.
BP6.2	The Developer should allow the end-user to withdraw at any time its content for processing of its personal data
BP6.3	The Developer should provide clear instructions to the end-user on how to delete its personal data.
BP6.4	The Developer should minimize and anonymize whenever possible the data collected from end-user logs.

Appendix B Mapping of PSA Certified to Other Standards

The domain of IoT is subject to several initiatives to improve device cybersecurity, from industry guidance to national regulation. While the scope of these initiatives is different from the one targeted for PSA Certified Level 1, this appendix aims at building a bridge between them.

More precisely, for initiatives deemed relevant for PSA Certified Level 1, this appendix provides a mapping between other standards requirements and corresponding PSA Certified Level 1 requirements.

B.1 ETSI EN 303 645

The following table only considers the mandatory requirements from ETSI EN 303 645 standard, as per Table B.1 of ETSI standard [303645], that have to be enforced by the device. Requirements that have be enforced by the environment of the device are not in the scope of PSA Certified Level 1.

Draft ETSI EN 303 645 V2.0 (2019-09)	PSA Certified Level 1 Requirements
Provision 4.1-1	D4.1 No default password R4.1 No default password
Provision 4.1-3	R5.3 User authentication
Provision 4.1-5	D4.2 Password best practices D4.3 Password threshold
Provision 4.3-2	R1.1 Firmware update
Provision 4.3-4	R1.1 Firmware update
Provision 4.4-1	R2.2 Secure storage D4.5 Secure storage
Provision 4.4-2	C1.4 ID storage
Provision 4.4-3	D4.1 Critical security parameter
Provision 4.5-1	R3.3 TLS
Provision 4.5-3	R2.4 Cryptography update
Provision 4.5-5	R6.1 Configuration
Provision 4.5-7	D2.3 Communication encryption
Provision 4.6-1	D2.1 No unused port
Provision 4.8-5	R3.3 TLS
Provision 4.11-1	R7.1 Erase user data

Draft ETSI EN 303 645 V2.0 (2019-09)	PSA Certified Level 1 Requirements
Provision 4.13-1	R4.5 Input validation

B.2 NISTIR 8259

The following table considers the NIST cybersecurity baseline [8259].

Draft NISTIR 8259 (January 2020) Capabilities	PSA Certified Level 1 Requirements
Device identification	C1.4 ID storage R2.1 Device ID
Device configuration	C2.3 Access control PSA-RoT R6.1 Configuration R7.1 Factory settings
Data protection	C1.1 Isolation C1.4 Secure storage C2.4 Cryptography R2.2 Secure storage R2.3 Cryptography R6.1 Configuration R7.1 Erase user data D5.2 Personal data
Logical access to interfaces	C2.3 Access control PSA-RoT R3.1 Connection authentication R3.2 Communication encryption R3.3 TLS R4.2 Unneeded functionalities R4.5 Input validation R6.1 Configuration D2.1 No unused port D2.2 Communication authentication D2.3 Communication encryption D2.4 TLS D3.1 Debug D3.3 Unneeded functionalities

Draft NISTIR 8259 (January 2020) Capabilities	PSA Certified Level 1 Requirements
Software and firmware update	C2.1 Firmware update C2.2 Rollback R1.1 Firmware update R1.2 Rollback R6.1 Configuration
Cybersecurity state awareness	C1.3 Security lifecycle R4.1 Attestation R4.3 Log R4.4 Log protection D1.1 Secure boot D3.2 Security lifecycle D3.4 Log D3.5 Log protection D5.1 Access control

B.3 SB-327

The following table considers the requirements of California law [SB-327] on cybersecurity of IoT devices.

SB-327, SECTION 1, Title 1.81.26, 1798.91.04.	PSA Certified Level 1 Requirements
(a)(1) Appropriate to the nature and function of the device.	PSA Certified requirements are targeted to IoT devices.
(a)(2) Appropriate to the information it may collect, contain, or transmit.	PSA Certified requirements on Code Integrity, Data Assets, Communication.
(a)(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.	PSA Certified requirements on Code Integrity, Data Assets, Communication, Passwords, Hardening, Privacy.
(b)(1) or (b)(2)	D4.1 No default password

Appendix C Transition Guide from PSA Certified Level 1 version 1.2

This appendix summarizes the changes introduced on requirements between this revision PSA Certified Level 1 and version 1.2.

PSA Certified L1 v.2.0	Changes from v1.2	Corresponding requirement from PSA Certified L1 v1.2
C1.1	Unchanged	C1.1
C1.2	Unchanged	C1.2
C1.3	Unchanged	C1.3
C1.4	Added "in such a way that it resists tampering by means such as physical, electrical or software (such as external probing of the chip for confidential data)"	C1.4
C2.1	Verification or integrity and authenticity is now mandatory for all updates. Also compliance to C2.4 for cryptography	C2.1
C2.2	Support of rollback is now mandatory but it can be deactivated.	C2.2
C2.3	Unchanged	C2.3
C2.4	Added "PSA requires equivalence of at least 128-bit security."	C2.4
R1.1	Verification or integrity and authenticity is now mandatory for all updates. Also compliance to R2.3 for cryptography	R1.1
R1.2	Support of rollback is now mandatory but it can be deactivated.	R1.2
R2.1	Unchanged	R2.1
R2.2	Rewording	R2.2
R2.3	Unchanged	R2.3
R2.4	New	
R3.1	Rewording	R3.1
R3.2	Rewording	R3.2
R3.3	TLS is not mandatory, but use of secure protocols is.	R3.3
R4.1	Unchanged	R4.1

PSA Certified L1 v.2.0	Changes from v1.2	Corresponding requirement from PSA Certified L1 v1.2
R4.2	Unchanged	R4.2
R4.3	Added "The developer shall include sufficient details to determine what happened."	R4.3
R4.4	New, but replaces "Log files should be protected against tampering." from R4.3 v1.2	
R4.5	Rewording from R3.4 v1.2. Also added data validation through APIs	R3.4
R5.1	Rewording. Also added no reset to universal default value	R5.1
R5.2	Rewording	R5.2
R5.3	New	
R6.1	New	
R7.1	Rewording. Now mandatory.	R6.1
D1.1	Unchanged	D1.1
D2.1	Rewording	D2.1
D2.2	Rewording	D2.2
D2.3	Rewording. Also CSP shall always be encrypted.	D2.3
D2.4	Rewording	D2.4
D3.1	Unchanged	D3.1
D3.2	Unchanged	D3.2
D3.3	Unchanged	D3.3
D3.4	Added "The developer shall include sufficient details to determine what happened."	D3.4
D3.5	New, but replaces "Log files should be protected against tampering." from R3.4 v1.2	
D4.1	Rewording. Also added no reset to universal default value	D4.1
D4.2	Rewording	D4.2
D4.3	Rewording	D4.3

PSA Certified L1 v.2.0	Changes from v1.2	Corresponding requirement from PSA Certified L1 v1.2
D4.4	Rewording	D4.4
D4.5	Rewording	D4.5
D5.1	Unchanged	D5.1
D5.2	Unchanged	D5.2
D5.1	New	
D5.2	New	

Appendix D Marking Sheet

This appendix summarizes the expected answers for each requirement in the Chip, System software and Device questionnaires for compliance to PSA Certified Level 1 and also for additional compliance to the other standards considered in the document.

D.1 Chip Assessment Questionnaire

D.1.1 PSA Certified Level 1

Exceptionally, one question answered not in conformance with "Expected answer" with rationale of why security is unaffected.

PSA Certified L1 v.2.0	Expected answer
C1.1 Hardware isolation of SPE	"Yes"
C1.2 Secure Boot	"Yes"
C1.4 ID Storage	"Yes"
C2.1 Firmware update	"Yes"
C2.2 Rollback protection	"Yes"
C2.3 Access control for modifications to PSA-RoT	"Yes"
C2.4 Best Practice Crypto	"Yes"

D.1.2 NISTIR 8259 Mapping

PSA Certified L1 v.2.0	Expected answer
C1.1 Hardware isolation of SPE	"Yes"
C1.3 Security lifecycle	"Yes"
C1.4 ID Storage	"Yes"
C2.1 Firmware update	"Yes"
C2.2 Rollback protection	"Yes"
C2.3 Access control for modifications to PSA-RoT	"Yes"
C2.4 Best Practice Crypto	"Yes"

D.2 System Software Assessment Questionnaire

D.2.1 PSA Certified Level 1

Exceptionally: One question answered not in conformance with "Expected answer" with rationale of why security is unaffected.

PSA Certified L1 v.2.0	Expected answer
R1.1 Firmware update	"Yes"
R1.2 Prevent rollback	"Yes"
R2.1 Use PSA-RoT for ID queries	"Yes"
R2.2 Use secure storage	"Yes"
R2.3 Best practice crypto	"Yes"
R2.4 Updateable crypto	"Yes"
R3.1 Authenticate remote servers	"Yes"
R3.2 Ability to encrypt data exchanged	"Yes"
R3.3 Two-way comms use secure protocols for auth and encryption e.g. TLS >= v1.2	"Yes"
R4.1 Attestation token of lifecycle state	"Yes"
R4.2 Disable/not install unused functionality	"Yes"
R4.3 System software should log security events	Any answer
R4.4 ***If*** logging enabled, restrict access of log files to auth users only	"Yes" or "N/A"
R4.5 Input protected against malformed input	"Yes"
R5.1 ***If*** *using* critical security parameters they are unique per device	"Yes" or "N/A"
R5.2 ***If*** *using* passwords then best practice	"Yes" or "N/A"
R5.3 ***If*** *using* user auth then crypto is best practice	"Yes" or "N/A"
R6.1 ***If*** security config changeable – auth first	"Yes" or "N/A"
R7.1 ***If*** personal data stored it should be erasable /device reset	"Yes" or "N/A"

D.2.2 ETSI Mapping

PSA Certified L1 v.2.0	Expected answer
R1.1 Firmware update	"Yes"
R2.2 Secure Storage	"Yes"
R2.3 Communication Encryption	"Yes"
R3.3 Two-way comms use secure protocols for auth and encryption e.g. TLS >= v1.2	"Yes"
R4.5 Input validation	"Yes"
R5.3 User Auth	"Yes"
R6.1 Configuration	"Yes"
R7.1 Erase user data	"Yes"

D.2.3 NISTIR 8259 Mapping

PSA Certified L1 v.2.0	Expected answer
R1.1 Firmware update	"Yes"
R1.2 Prevent rollback	"Yes"
R2.1 Use PSA-RoT for ID queries	"Yes"
R2.2 Use secure storage	"Yes"
R2.3 Best practice crypto	"Yes"
R3.1 Authenticate remote servers	"Yes"
R3.2 Ability to encrypt data exchanged	"Yes"
R3.3 Two-way comms use secure protocols for auth and encryption e.g. TLS >= v1.2	"Yes"
R4.1 Attestation token of lifecycle state	"Yes"
R4.2 Disable/not install unused functionality	"Yes"
R4.3 System software should log security events	"Yes"
R4.4 Restrict access of log files to auth users only	"Yes"
R4.5 Input protected against malformed input	"Yes"
R5.2 Passwords best practice	"Yes"
R6.1 Security config changeable – auth first	"Yes"
R7.1 Personal data erasable /device reset	"Yes"

D.3 Device Assessment Questionnaire

D.3.1 PSA Certified Level 1

Exceptionally: One question answered not in conformance with "Expected answer" with rationale of why security is unaffected.

PSA Certified L1 v.2.0	Expected answer
D1.1 Secure boot with validated software	"Yes"
D2.1 Close unused network ports/ interfaces	"Yes"
D2.2 Ability to auth remote servers	"Yes"
D2.3 Encrypt by default data exchanged	"Yes"
D2.4 The device shall use secure protocols for authentication and encryption of two-way communication	"Yes"
D3.1 Protect against unauth use of debug	"Yes"
D3.2 Security lifecycle attestable	"Yes"
D3.3 Functionalities not needed disabled or not installed	"Yes"
D3.4 Log security events *(OPT)*	Any answer
D3.5 *If* log, restrict log files to auth users	"Yes" or "N/A"
D4.1 *If* critical security params then unique per device	"Yes" or "N/A"
D4.2 *If* passwords, device uses password best practice	"Yes" or "N/A"
D4.3 *If* passwords, ability to disable passwords or apply time out after unsuccessful auth against a password	"Yes" or "N/A"
D4.4 *If* auth, time-out against perpetual auth	"Yes" or "N/A"
D4.5 *If* critical security params then secure storage	"Yes" or "N/A"
D5.1 Restrict access to personal data/logs to auth users	"Yes"
D5.2 Personal data stored on secure storage	"Yes"
D6.1 Public point of contact	Any answer

D6.2 Minimum length of time for updates	Any answer

D.3.2 ETSI Mapping

PSA Certified L1 v.2.0	Expected answer
D2.1 Close unused network ports/ interfaces	"Yes"
D4.1 Critical security params unique per device	"Yes"
D4.2 Device uses password best practice	"Yes"
D4.3 Ability to disable passwords or apply time out after unsuccessful auth against a password	"Yes"

D.3.3 NISTIR 8259 Mapping

PSA Certified L1 v.2.0	Expected answer
D1.1 Secure boot with validated software	"Yes"
D2.1 Close unused network ports/ interfaces	"Yes"
D2.2 Ability to auth remote servers	"Yes"
D2.3 Encrypt by default data exchanged	"Yes"
D2.4 The device shall use secure protocols for authentication and encryption of two-way communication	"Yes"
D3.1 Protect against unauth use of debug	"Yes"
D3.2 Security lifecycle attestable	"Yes"
D3.3 Functionalities not needed disabled or not installed	"Yes"
D3.4 Log security events	"Yes"
D3.5 Restrict log files to auth users	"Yes"
D5.1 Restrict access to personal data/logs to auth users	"Yes"
D5.2 Personal data stored on secure storage	"Yes"

D.3.4 SB-327 Mapping

PSA Certified L1 v.2.0	Expected answer
D4.2 Device uses password best practice	"Yes"

D.3.5 Draft UK Government Basic Security Requirement Mapping

PSA Certified L1 v.2.0	Expected answer
D4.1 Critical security params (including passwords) are unique per device not resettable to universal factory default	"Yes"
D6.1 Public point of contact	"Yes"
D6.2 Minimum length of time for updates	"Yes"

D.3.6 Marking Sheet Summary

PSA Level 1 pass?	Answer
ETSI 303 645 device mapping complete?	
NISTIR 8259 mapping complete?	
SB-327 mapping complete?	
Draft UK Government basic security requirement complete?	