PSA Certified™
Level 1 Questionnaire
Version 2.1

Document number:	JSADEN001
Version:	2.1 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:	12/10/2020

Abstract

PSA Certified is an independent security evaluation scheme for Platform Security Architecture (PSA) based chips, system software and internet connected IoT and Edge devices. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust 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 and its goals, generic compute-based platform threat models and industry best practice to provide a set of critical security questions for the chip vendor, the system software supplier and the device 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, chip, connected device, internet, IoT, Platform Security Architecture, questionnaire, PSA, security, system software

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: Beta

1.2 Release Information

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

Date	Version	Confidentiality	Change
21/08/2020	2.1	Non-confidential	Updates and alignment with ETSI 303 645 and NISTIR 8259A. Addresses devices using application type processors. Change in compositional model for devices on system software on chips.
10/02/2020	2.0 Beta	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-SM]	DEN 0079	ARM	Device Security Model
[303645]	EN 303 645	ETSI	Cyber Security for Consumer Internet of Things; V2.1.0 (2020-04)
[8259]	NISTIR 8259A	NIST	IoT Device Cybersecurity Capability Core Baseline; May 2020
[SB-327]	Bill No. 327; Chapter 886.	California State Senate	Information privacy: connected devices
[UK DCMS]		UK Department for Digital, Culture & Sport	Proposals for regulating consumer smart product cyber security[1].

[1] https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations

Term	Meaning
Application Root of Trust Service(s)	Application specific security service(s) that are not defined by PSA. Such services execute in the Secure Processing Environment and are required to be in Secure Partitions.
Application Specific Software	Software that provides the functionality required of the specific device. This software runs in the Non-Secure Processing Environment, making use of the System software, Application RoT Services and PSA-RoT Services.
Critical Security Parameter	Secret information, with integrity and confidentiality requirements, used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc.. In some contexts these are classed as assets.
Evaluation Laboratory	Laboratory or facility that performs the technical review of questionnaires submitted for Level 1 PSA certification. The list of evaluation laboratories participating to PSA Certified can be found on www.psacertified.org
Hardware Unique Key (HUK)	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a critical security parameter.
Non-secure Processing Environment (NSPE)	The processing environment that hosts the non-secure System software and Application Specific Software. PSA requires the NSPE to be isolated from the SPE. Isolation between partitions within the NSPE is not required by PSA though is encouraged where supported.
Partition	The logical boundary of a software entity with intended interaction only via defined interfaces, but not necessarily isolated from software in other partitions. Note that both the NSPE and SPE may host partitions.
PSA	Platform Security Architecture
PSA Certification Body	The entity that receives applications for PSA security certification, issues certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories.
PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
PSA Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.

PSA Root of Trust (PSA-RoT)	The PSA defined combination of the Immutable Platform RooT of Trust and the Updateable Platform Root of Trust, and considered to be the most trusted security component on the device. See [PSA-SM].
Immutable Platform Root of Trust	The minimal set of hardware, firmware and data of the PSA-RoT, which is inherently trusted because it cannot be modified following manufacture. There is no software at a deeper level that can verify that it as authentic and unmodified.
Updateable Platform Root of Trust	The firmware, software and data of the PSA-RoT that can be securely updated following manufacture.
Platform Root of Trust Service(s)	PSA defined security services for use by PSA-RoT, Application RoT Service(s) and by the NSPE. Executes in the Secure Processing Environment and may use Trusted Subsystems. This includes the services offered by the PSA Functional APIs.
Secure Partition	A Partition in the Secure Processing Environment.
Secure Processing Environment Partition Management	Management of the execution of software in Secure Partitions. Typical implementations will provide scheduling and inter-partition communication mechanisms. Implementations may also enforce isolation between the managed Secure Partitions.
Secure Processing Environment (SPE)	The processing environment that hosts the PSA-RoT, and any Application RoT Service(s).
Secure Boot	The process of verifying and validating the integrity and authenticity of updateable firmware and software components as a pre-requisite to their execution. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded, which may extend the NSPE secure boot chain further.
System Software	NSPE software that may comprise an operating system or some run-time executive, together with any middleware, standard stacks and libraries, chip specific device drivers, etc., but not the application specific software.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its critical security parameters, or that implement some of its services.

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 behavior 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 of a device against a set of security requirements by an Evaluation Laboratory. The evaluation laboratory examines security measures to ensure that the device, including its critical security parameters, is not vulnerable to identified threats.

In the case of a successful evaluation a digital certificate is issued by the PSA Certification Body (or a third-party on behalf of the PSA Joint Stakeholder Members) for that device and can optionally be 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 that support, for example, an IETF Entity Attestation Token[2] can include the EAN-13 to inform relying parties that the chip, System software or device has been evaluated and is PSA Certified.

PSA Functional API Certification

PSA Functional API Certification means that a device has implemented the **PSA Functional APIs**[3] 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 recognizes that there will be different security requirements and different cost and 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, the target of this document, relies on questionnaires filled out by the Chip vendor, the System software vendor or the Device OEM. The questionnaires defined in this document cover the baseline security requirements to mitigate common threats and security requirements for PSA based products. The Evaluation Laboratory relies on this questionnaire to examine the device security measures.

2.2 Scope for Security Evaluation

There are three evaluation scopes: the chip, the system software and the device. The security evaluation covers the combination of the hardware and software components. Figure 1 illustrates the typical components in the PSA architecture and the related evaluation scopes. This figure distinguishes a Non-secure Processing Environment (NSPE) and a Secure Processing Environment (SPE), for which the Chip level shall provide isolation[4].

[2] https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/

[3] https://developer.arm.com/architectures/security-architectures/platform-security-architecture

[4] The isolation between the Non-Secure Processing Environment and the Secure Processing Environment can be implemented using, for example, TrustZone, using dual cores, or via processor privilege levels.

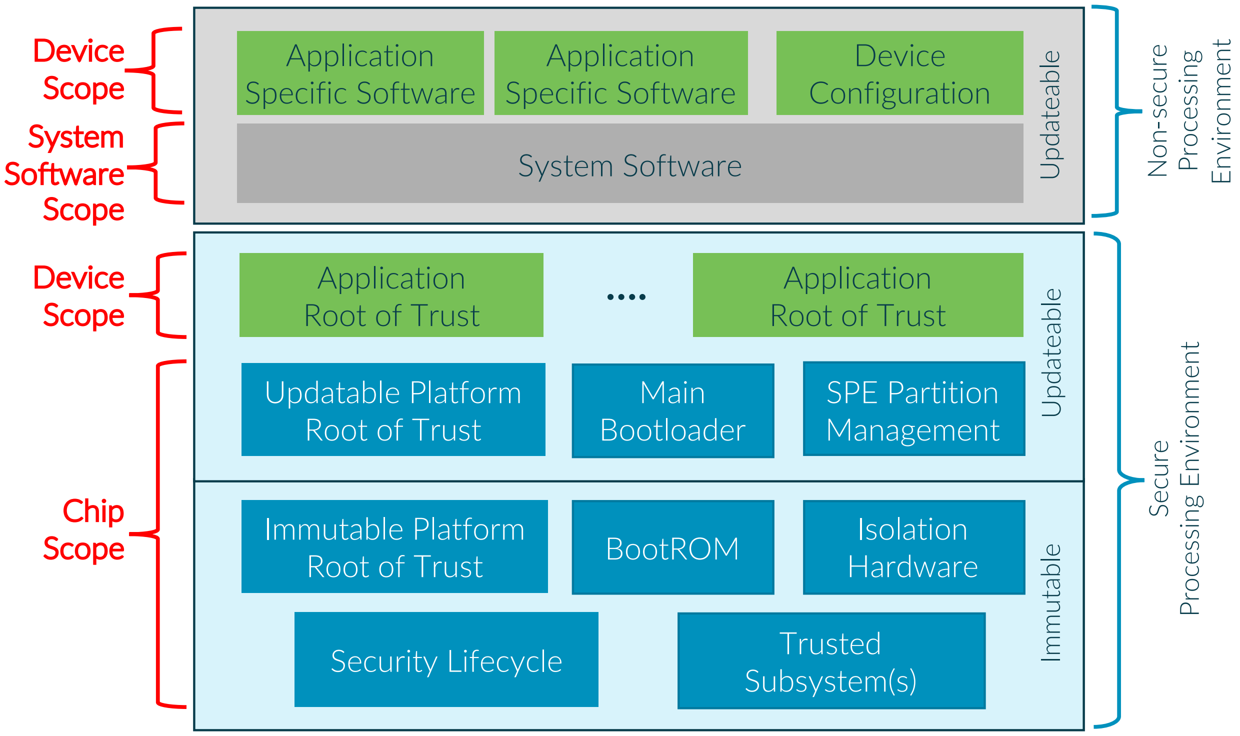
Device Scope
System Software Scope
Device Scope
Chip Scope
Application Specific Software
Application Specific Software
Device Configuration
System Software
Updateable
Non-secure Processing Environment
Application Root of Trust
....
Application Root of Trust
Updatable Platform Root of Trust
Main Bootloader
SPE Partition Management
Updateable
Immutable Platform Root of Trust
BootROM
Isolation Hardware
Security Lifecycle
Trusted Subsystem(s)
Immutable
Secure Processing Environment

Figure 1: Logical Scope of Chip, System Software and Device Levels

The Chip hardware may be a System-on-Chip or a System-in-Package, however, there may also be reliance on board level components. The Chip security evaluation scope includes the following components as described in [PSA-SM]:

- Immutable Platform Root of Trust, for example, the Boot ROM, any root parameters, the isolation hardware, and hardware based security lifecycle management and enforcement.
- Updateable Platform Root of Trust, for example, may include a main bootloader, code that implements the SPE Partition Management function, and code that implements the PSA defined services such as attestation, secure storage, and cryptography.
- Trusted subsystems are components that the PSA Root of Trust (PSA-RoT) relies on for protection of its assets, or that implement some of its services, for example, a Subscriber Identification Module or a Secure Element.

The System software in the scope of the security evaluation executes in the Non-secure Processing Environment. System software evaluation dependencies on the Chip layer are detailed in section 2.4.

For the Device, the scope of the security evaluation includes the following software components:

- Applications and any other software developed by the OEM. These may execute in the Non-Secure Processing Environment or as Application Root of Trust Services in the Secure Processing Environment
- Configuration of the System software for the device.

Device evaluation dependencies on the System software and Chip layers are detailed in 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 immutable and updateable parts of the PSA-RoT (including any trusted subsystems).
- System software Vendor: Develops the system software for the Non-secure Processing Environment.
- Device OEM: Conceives and develops a device based on the PSA specifications.
- Evaluation Laboratory: Performs the technical review of questionnaire(s) submitted for PSA Certified Level 1 and if successful provides a digital certificate reference number (EAN-13) for the applicable evaluation scope.
- Certification Body: The entity that receives applications for PSA certification, issues certificates, maintains the security certification scheme, and ensures consistency across the evaluation laboratories.

2.4 Options for Evaluation and Layer Composition

The purpose of PSA Certified Level 1 is to assess the security foundation of a device. The certification scheme is organized in layers: device, on top of the system software, on top of the chip. The certificate for a given layer is only applicable if the lower layers have either been separately evaluated and hold a PSA L1 certificate or, if not, are covered in the evaluation that lead to the considered certificate. The evaluation options are as follows;

1) Chip evaluation can proceed independently of the other layers. Section 4 must be filled in.
2) System software evaluation can proceed with one of the following;
    a) with a PSA Certified chip. Section 5 must be filled in and section 3.3 must give the chip EAN-13.
    b) with an uncertified chip the evaluation must also include the chip part. Sections 4 and 5 must be filled in. Note that an independent certificate for the chip will not be issued.
3) Device evaluation can proceed with one of the following;
    a) on PSA Certified system software with either;
        i) a valid PSA Certified chip other than that named in the system software certificate; see section 2.4.1 on validity. Section 6 must be filled in and section 3.3 must give the system software EAN-13 and the PSA Certified chip EAN-13. Section 3.8 also must be filled in.
        ii) the chip named in the system software certificate. Section 6 must be filled in and section 3.3 must give the system software EAN-13, and the named chip. If the named chip is PSA Certified, section 3.3 must give the chip EAN-13.
    b) on uncertified system software with a PSA Certified chip. The evaluation must include the system software part. Sections 5 and 6 must be filled in and section 3.3 must give the EAN-13 of the PSA Certified chip. An independent certificate for the system software will not be issued.
    c) if the chip is neither a valid PSA Certified chip (it does not have its own certificate) nor the chip named in any certificate for the System software[5] then the evaluation must include both the system software and the chip parts. Sections 4, 5 and 6 must be filled in. Note that independent certificates for the system software and for the chip will not be issued.

[5] A System software certificate is only applicable with a valid PSA Certified chip or the chip named in the certificate.

Certification of a device requires the device vendor to confirm that the device and any device vendor configuration of the system software results in the correct use of the PSA-RoT. Confirmation is accessed via the device Developer responses in section 6. PSA Functional API certification can help in this process.-Device evaluation is performed with a specific system software and chip combination, and the resulting device certificate is valid for that combination only.

2.4.1 Valid Alternative PSA Certified Chips

Flexible composition via 3)a)i) above relies on the interchangeability of the chip level PSA-RoT. Typically, this means that the alternate PSA Certified chip must support at least the same PSA-RoT functionality as the chip named in the System software certificate. In practice, this likely means that all the requirements in section 4 must be met. PSA API Functional API Certification can be used as evidence of interchangeability.

If the PSA Certified System software relies on chip-level security functionality in addition to that required for the PSA-RoT then the alternative chip must provide at least the same additional functionality. In practice, this is likely to mean that such compositions may be difficult.

The full rules on validity can be found **here**.

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 Device OEM (all named Developer below) complete the relevant questionnaire provided in sections 4, 5 or 6 as specified in section 2.4. It is recommended that the Developer also complete the assessible organisational best practices questions in Appendix A.1.
2. For each requirement in the relevant section, the box corresponding to the fulfilment of the requirement is ticked as follows, note that a gray box means that answer is not acceptable. All guidance given in italic should be deleted.
   - Yes: for full compliance with the requirement, the Developer describes how this requirement is met according to any guidance given *in italic*.
   - Partial: for partial compliance with the requirement, the Developer describes how the requirement is partially met according to any guidance given *in italic* and what impact that has on the security.
   - N/A: where the requirement is not applicable for one of the following reasons, the Developer must in all cases provide a rationale;
     - the required feature is not supported (typically those requirements that start with “if”), or
     - is an Optional requirement and is not included.
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 relevant Chip, System software or Device certification (see section 2.4), 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.

☐ System software on a PSA Certified chip.

☐ System software on an uncertified chip.

☐ Device on PSA Certified system software but with a valid PSA Certified chip other than that named in the system software certificate. The declaration in section 3.8 must be completed.

☐ Device on PSA Certified system software with the chip named in the system software certificate.

☐ Device on an uncertified system software on a PSA Certified chip.

☐ Device on system software and on an uncertified chip.

3.3 Product Reference

This declaration is applicable to the Chip;

Commercial name:	*(e.g. Product family)*
Chip part number:	
Chip version:	*(e.g. Chip silicon revision)*
SPE name:	*(e.g. Firmware Framework-M)*
SPE version:	
Chip EAN-13:	*(If this version of the chip is already PSA Certified, specify the EAN-13 of the certificate)*
Chip reference documentation:	*(If this version of the chip is not 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.1.)*

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

System software name:	*(e.g. Mbed OS, Linux)*
System software version:	The version number or an identifier for the build of the system software.
System software EAN-13:	*(If this version of the System software is already PSA Certified, specify the EAN-13 of the certificate)*
System software reference documentation:	*(If this version of the System software is not PSA Certified, provide identification of the reference documentation used to fill the System software questionnaire. It may be requested by the Evaluation Laboratory)*
System Software use of chip security features:	*(Please indicate what use, if any, is made of chip-level security functionality in addition to that required for the PSA-RoT. See section 2.4.1)*

3.4 Device 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 RoT 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.*
PSA Security Model Isolation Boundaries	Isolation of the Secure Processing Environment (SPE) from the Non-secure Processing Environment (NSPE) is a mandatory PSA Certified requirement. The PSA Security Model [PSA-SM] defines two incremental isolation boundaries; please indicate if these are deployed; ☐ The PSA-RoT is isolated from the Application RoT Service(s). ☐ In addition to PSA-RoT isolation from Application RoT Service(s), Application RoT Services are isolated from each other.
PSA-RoT Services:	*(Describe PSA-RoT services implementation)*
Trusted subsystem:	*(Describe any trusted subsystems relied upon for operation of PSA Root of Trust, such as a security subsystem or a Secure Element, and how they are used. Declare 'none' if no trusted subsystems are 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 authorized representative of the organization 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 authorized representative of the organization 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 3.3.

and

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

Name:	
Date:	
Signature:	

3.8 Declaration of conformance for a Device level certificate

If the Device developer is reusing a valid PSA Certified chip and PSA Certified system software for composition following 3)a)i) on page 13, the EAN-13 of the certificates should be declared below.

PSA Certified Chip EAN-13	
PSA Certified System Software EAN-13	

As an authorized representative of the organization stated in section 3.1 of this document, I declare that the information provided in this section is valid and correct for the product/service stated in section 3.3.

Name:	
Date:	
Signature:	

4 Chip Assessment Questionnaire

This section applies to the hardware and firmware that comprise the PSA-RoT that forms the Secure Processing Environment (SPE), see section 1.4. 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, the answers apply only to the context in which the chip is used. For example, the response to C2.4 need list only the cryptographic algorithms used, not all the algorithms supported by the chip.

4.1 Immutable Platform Root of Trust

ID	Requirement	Supported?		
		Yes	Partial	N/A
C1.1	The chip shall support a hardware mechanism(s) to isolate the Secure Processing Environment (SPE) 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 (see section 1.4), initiated from code in the immutable Platform Root of Trust. Note that asymmetric signing is expected, however, symmetric signing can be accepted if the requirement in C1.4 is met.			
	(Describe which cryptographic functions and key sizes are used for secure boot, and how the cryptography is implemented, such as use of a hardware cryptographic accelerator or software in immutable code. Also describe how the Immutable code is implemented and if in some form updateable on-chip memory (such as EEPROM or Flash) how that is locked.) *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-3076) 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.*			

ID	Requirement	Supported?		
		Yes	Partial	N/A
C1.3 (Optional)	The chip shall support a security lifecycle, i.e. protecting critical security parameters and sensitive data based on device lifecycle state and enforcing the rules for transition between states. Lifecycle states can typically be classed as follows, i) non-secure assembly and test, ii) provisioning, secured provisioned and operational, iii) decommissioned, and iv) debug, if debug of a secured provisioned device is supported. *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 or derivation of following minimum set (or equivalent) of critical security parameters, in such a way that prevents unauthorized reading and resists tampering by means such as physical, electrical or software (such as external probing of the chip for confidential data): • A secret Hardware Unique Key (HUK), with at least with 128-bits of entropy, used for deriving other device secrets • A PSA-RoT Public Key, or hash of, used for authenticating the first updateable firmware component code during secure boot. If symmetric signing is unavoidable, the key must be unique per device. • A secret attestation key and identifier that uniquely identifies the attestation key • An identifier that uniquely identifies the PSA-RoT on the chip. These keys and identifiers may be injected during chip manufacture or during the manufacture of the device, or derived from the HUK. They can also be derived from a Physically Unique Function (PUF).			
	(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 are protected from tampering.)*			

4.2 PSA RoT

ID	Requirement	Supported?		
		Yes	Partial	N/A
C2.1	The PSA-RoT shall support update of the PSA-RoT and any Application RoTs. Updates may be delivered either from locally connected devices (such as removable media) or from remote servers. Updates shall be validated by the PSA-RoT to check integrity and authenticity prior to execution (see C1.2) and, optionally, before installation. This includes the executable code and any related data, such as configuration data or a manifest. The cryptography used shall comply with requirement C2.4.			
	(Describe how updates are validated, including the cryptographic algorithms, the key size and where the keys used for validation are stored. 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 prevent unauthorized rollback of updates (see C2.1) and protect the current reference firmware version number in an anti-rollback counter, in secure storage (for example, protected flash or OTP). A mechanism may be provided to support authorized rollback for recovery reasons. Anti-rollback is strongly recommended but not mandatory in PSA Level 1 V2.			
	(Describe the versioning information used to detect rollback and how it is protected in integrity and against rollback and over or underflow. If supported, describe how authorized rollback is implemented.)			
C2.3	The PSA-RoT shall perform access control for modification and use of PSA-RoT critical security parameters and for System software or Device sensitive data managed by the PSA-RoT. For example, the PSA-RoT shall control access to any such data stored in a protected flash region or in OTP.			
	(Describe the System software subjects concerned by access control and how they are identified or authenticated)			

ID	Requirement	Supported?		
		Yes	Partial	N/A
C2.4	The PSA-RoT shall use best practice cryptography for protection of its assets, as recommended for instance by national security agencies. This includes the provision of a suitable source of random data. There should be no reliance on proprietary cryptographic algorithms or customization of standard cryptographic algorithms. PSA requires equivalence of at least 128-bit security. *NB: 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. A TRNG or a suitably seeded Deterministic Random Bit Generator can be used.*			
	(List the cryptographic algorithms provided by the PSA-RoT and the supported key sizes. Also describe how random number generation is performed.)			

5 System Software Assessment Questionnaire

This section applies to the software executing in the Non-secure Processing Environment (NSPE), see section 1.4. 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.

When this section is filled in by the System software vendor, it is acceptable to answer Yes to those requirements where the vendor provides the ability for the OEM to configure the device such that the OEM can meet the requirement. This situation arises where the system OEM, and not the software vendor, is not responsible for the deployed configuration. The System software vendor should state that this is the case as the answer to the requirement.

When this section is filled in by the OEM, the provided answers apply only to the context in which the System software is used. For instance, the OEM may only provide in S2.3 the cryptographic algorithms that are used, not all the algorithms supported by the System software.

5.1 Code Integrity

ID	**Requirement**	**Supported?**		
		Yes	**Partial**	**N/A**
S1.1	The System software shall support update of the system software and the application specific software, either from locally connected devices (such as removable media) or from remote servers. Updates shall be validated by the system software or the PSA-RoT to check the integrity and authenticity prior to execution and, optionally, installation. This includes the executable code and any related data, such as any manifest and configuration data. The cryptography used shall comply with requirement S2.3.			
	(Describe how updates are validated, including the cryptographic algorithms, the key sizes and where the keys used for validation are stored. Justification is required if local validation of an 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 validates the update and swaps slot 1 and slot 0.*			

ID	Requirement	Supported?		
		Yes	Partial	N/A
S1.2	The update mechanism shall prevent unauthorized rollback of system software, any applicable application software and authentication data. A mechanism may be provided to support authorized rollback for recovery reasons. Anti-rollback is strongly recommended but not mandatory in PSA Level 1 V2.			
	(Describe the versioning information used to detect rollback and how it is protected in integrity and against rollback and overflow. If supported, describe how authorized rollback is implemented. Note that use should be made of the PSA-RoT for the most secure solution.) *Example of response for Yes: In the process described in answer for S1.1, the System software verifies firmware version in PSA-RoT based secure storage before storing the new image in slot 1. The current version of firmware is stored using the PSA-RoT secure storage service.*			

5.2 Data Assets

ID	Requirement	Supported?		
		Yes	Partial	N/A
S2.1	The System software shall rely only on the PSA-RoT for all queries of the PSA-RoT (chip) identity (see C1.4).			
	(Describe how the PSA-RoT identity is used in preference to other identities that may exist.)			
S2.2	The System software shall use secure storage to protect sensitive data and provide this functionality for application data. It shall additionally bind the sensitive data to a specific device instance and, if supported, security lifecycle state (see C1.3). The cryptography used for secure storage shall comply with requirement S2.3.			
	(Describe how secure storage is implemented. Note that use should be made of the PSA-RoT secure storage service for the most secure solution.) *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 PSA-RoT secret hardware unique key (HUK) per device.*			

ID	Requirement	Supported?		
		Yes	Partial	N/A
S2.3	The System software shall use best practice cryptography as required by applicable standards or recommended by national security agencies, covering choice of algorithms and key lengths, and random number generation based on the identified threats. There should be no reliance on proprietary cryptographic algorithms or customization of standard cryptographic algorithms. This PSA Certified level requires equivalence of at least 128-bit security.			
	(Describe the cryptographic algorithms provided by the System software, supported key sizes and how they are implemented. Note that use should be made of the PSA-RoT cryptographic service for the most secure solution.)			

5.3 Communication

ID	Requirement	Supported?		
		Yes	Partial	N/A
S3.1	For two-way communication protocols and for each network interface, the System software shall provide the ability to authenticate remote devices and servers when establishing a connection.			
	(Describe how this requirement is met.)			
S3.2	The System software shall provide the ability to encrypt and integrity check data exchanged with remote devices and servers.			
	(Describe how this requirement is met.)			
S3.3	The System software shall use secure protocols, compliant with requirement S2.3, for authentication and encryption of two-way communication. The selected protocols shall not leak data that would lead to the identification of vulnerable devices. *NB: If the System software relies on TLS, the version shall be 1.2 or later, and it shall forbid the fallback to legacy cipher suites publicly known to be unsecure (such as 3DES, DES, IDEA, RC4, or Null).*			
	(Describe how this requirement is met.)			

5.4 Hardening

ID	Requirement	Supported?		
		Yes	Partial	N/A
S4.1	The System software shall support an attestation method that includes the current security lifecycle state of the device.			
	(Describe how this requirement is met. Note that use should be made of the PSA-RoT attestation service.) *Example of response for Yes: The system software generates an IETF Entity Attestation token, including the lifecycle state, and uses the PSA-RoT attestation service to sign the token.*			
S4.2	Functionality that is not needed for the intended use of the System software shall not be installed, or shall be disabled if non-installation is not practical.			
	(Describe how this requirement is met.)			
S4.3 (Optional)	The System software should provide logging of security relevant events and errors. The log should include sufficient details to determine what happened and should be integrity protected. *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)			
S4.4 (Optional)	If the System software supports logging, it shall restrict access to the log files to authorized users only (refer to S5.3).			
	(Describe how this requirement is met.)			
S4.5	Data input via network, local and user interfaces shall be validated defensively against malformed input. Data transferred via critical Application Programming Interfaces (API) shall also be validated defensively against malformed input.			
	(Describe how this requirement is met.)			

ID	Requirement	Supported?		
		Yes	Partial	N/A
S4.6	The System software shall enable the execution of application specific software and system software with the lowest level of privilege necessary for the intended function. Also, each authenticated user shall have limited privileges based on pre-determined and/or securely configurable access controls.			
	(Describe how this requirement is met.) *For example, this can be met by one or more of the following; processor privilege levels, memory access control, access control based on process identification and related permissions to system files, services, communication channels, etc.*			

5.5 Passwords and Critical Security Parameters

ID	Requirement	Supported?		
		Yes	Partial	N/A
S5.1	If the System software makes use of critical security parameters they shall be unique per device or defined by the user. They shall not be resettable to any universal factory default value and must not be easily determined by automated means or obtained from publicly available information.			
	(Describe how this requirement is met.)			
S5.2	If the System software makes use of passwords they should conform with security best practices, in particular, password length and complexity, and the number of failed authentication attempts (refer for instance to NIST SP 800-63B guidelines for memorized secrets). Where default passwords are used, they must be unique per device and must not be easily determined by automated means or obtained from publicly available information.			
	(Describe how this requirement is met.) *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.*			

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Requirement</th><th colspan="3">Supported?</th></tr>
<tr><th>Yes</th><th>Partial</th><th>N/A</th></tr>
<tr><td rowspan="2">S5.3</td><td>If the System software makes use of critical security parameters for user authentication, the cryptography used for that feature shall comply with requirement S2.3.</td><td></td><td></td><td></td></tr>
<tr><td colspan="4"><i>(Describe the cryptographic algorithms and key sizes used for user authentication)</i></td></tr>
</table>

5.6 Configuration

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Requirement</th><th colspan="3">Supported?</th></tr>
<tr><th>Yes</th><th>Partial</th><th>N/A</th></tr>
<tr><td rowspan="2">S6.1</td><td>If the System software allows security-relevant configuration changes via a user interface or a network interface, the related configuration change shall only be accepted after authentication (refer to S3.1, S3.3 and S5.3).
Examples of 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).</td><td></td><td></td><td></td></tr>
<tr><td colspan="4"><i>(Describe how this requirement is met.)</i>
<i>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 S5.3.</i>
<i>Other example of response for Yes: The System software does not allow security-relevant configuration changes.</i></td></tr>
</table>

5.7 Privacy

ID	Requirement	Supported?		
		Yes	Partial	N/A
S7.1	If the System software allows persistent storage of personal and configuration data, it shall allow only the owner or an authorized entity to erase this data.			
	(Describe how this requirement is met.) *Example of response for Yes: The System software does not allow persistent storage of personal data or configuration. Another example of response for Yes: The System software erases all data and resets to factory settings.*			

6 Device Assessment Questionnaire

This section applies to a device built on the System software (section 5) built on the Chip PSA-RoT (section 4). Skip this section if the scope of evaluation does not include the device.

6.1 Code Integrity

ID	Requirement	Supported?		
		Yes	Partial	N/A
D1.1	The device shall be configured to enforce Secure Boot for the PSA-RoT, any Application RoT Services and at least the first executable code of the NSPE System software.			
	(Describe how this requirement is met.) *Example of response for Yes: The device is configured to rely on TF-M and primitives of Boot ROM for validating TF-M image prior to execution. Then the bootloader from the Secure Processing Environment (TF-M) validates the System software image prior to its execution.*			
D1.2	The device shall be configured to ensure that PSA-RoT and any Application RoT Services updates are performed in accordance with C2.1, and that any anti-rollback checks are performed in accordance with C2.2. The device shall be configured to ensure that any system software and application software updates are performed, in accordance with see S1.1, and that any anti-rollback checks are performed in accordance with S1.2. Anti-rollback is strongly recommended but not mandatory in PSA Level 1 V2.			
	(Describe how this requirement is met.)			

6.2 Communication

ID	Requirement	Supported?		
		Yes	Partial	N/A
D2.1	The device shall close all logical interfaces not necessary for the intended use of the device. Examples include, network TCP/UDP ports and/or sockets relating to services not required.			
	(Describe how this requirement is met.)			

ID	Requirement	Supported?		
		Yes	Partial	N/A
D2.2	For two-way communication protocols, the device shall provide the ability to authenticate remote devices and servers when establishing a connection. *NB: Protocols should be selected such that the process of authentication does not leak data that would lead to the identification of vulnerable devices.*			
	(Describe how this requirement is met.)			
D2.3	The device shall encrypt by default all data exchanged with remote devices and servers. In particular, critical security parameters and any service or personal sensitive shall always be encrypted.			
	(Describe how this requirement is met.) *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.*			
D2.4	The device shall use secure protocols, compliant to requirement S2.3, for authentication and encryption of two-way communication. *NB: If the device relies on TLS, the version shall be 1.2 or later, and it shall forbid the fallback to legacy cipher suite publicly known to be unsecure (such as cipher suites with 3DES, DES, IDEA, RC4, or Null).*			
	(Describe how this requirement is met.)			

6.3 Hardening

ID	Requirement	Supported?		
		Yes	Partial	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. Where debug is not permitted, debug symbols shall not be present in the on the device code images. The device shall make inaccessible or erase sensitive user assets and credentials when these debug and test features are enabled.			
	(Describe which technical measures disable or deactivate debug)			

ID	Requirement	Supported?		
		Yes	Partial	N/A
D3.2	The current security lifecycle state of the device shall be attestable, using, for example, an entity attestation token.			
	(Describe how this requirement is met.)			
D3.3	Functionality that is not needed for the intended usage of the device shall not be installed or shall be disabled if non-installation is not practical.			
	(Describe how this requirement is met.)			
D3.4 (Optional)	The device should support audit logging of security relevant events and errors and ensure only authorised access to the logs. The log should include enough 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)			
D3.5 (Optional)	If the device supports logging, it shall restrict access to log files to authorized users only.			
	(Describe how this requirement is met.)			
D3.6	To ensure that the device has the necessary security properties, it and the System software shall make use of the PSA-RoT security functionality for at least one of the PSA-RoT secure storage, cryptography, and attestation services as necessary to meet the requirements in sections 4, 5 and 6. This is in addition to secure boot (see D1.1), and updates and anti-rollback (D1.2).			
	(Describe how the PSA-RoT functionality is used on this device.)			

6.4 Passwords

ID	Requirement	Supported?		
		Yes	Partial	N/A
D4.1	If the device makes use of critical security parameters, they shall be unique per device or defined by the user. They shall not be resettable to any universal factory default value and must not be easily determined by automated means or obtained from publicly available information.			
	(Describe how this requirement is met.)			
D4.2	If the device makes use of passwords, they should conform with security best practices, in particular, password length and complexity (refer for instance to NIST SP 800-63B guidelines for memorized secrets). Where default passwords are used, they must be unique per device and must not be easily determined by automated means or from publicly available information.			
	(Describe how this requirement is met.)			
D4.3	If the device makes use of passwords, the device shall either disable passwords or apply a timeout after a threshold of unsuccessful authentication attempts before another authentication attempt is allowed.			
	(Describe how this requirement is met.)			
D4.4	If the device makes use of critical security parameters for authorization, it shall implement an inactivity time-out or other appropriate mechanism to prevent perpetual authorization.			
	(Describe how this requirement is met.)			
D4.5	If the device makes use of critical security parameters, it shall use secure storage to protect them.			
	(Describe how this requirement is met. Note that use should be made of the PSA-RoT secure storage service for the most secure solution.)			

6.5 Privacy

ID	Requirement	Supported?		
		Yes	Partial	N/A
D5.1	The device shall restrict access to personal data, including that in any log files, to authorized users only.			
	(Describe how this requirement is met.)			
D5.2	The device shall store personal data on a secure storage.			
	(Describe how this requirement is met. Note that use should be made of the PSA-RoT secure storage service for the most secure solution.)			

Appendix A Organisational Best Practices

In addition to the technical security measures that are in the scope of Level 1 PSA certification covered in the requirements expressed in sections 4 to 6, this appendix lists many organizational best practices that contribute to comprehensive device security. These are collated from references [303645], [8259], [SB-327] and [UK DCMS].

The organizational best practices given in Appendix A.1 reflect common requirements that appear in many standards and are, or are likely to become, legal requirements in many territories. Verification of compliance to these organizational best practices by the Evaluation Laboratory during a PSA certification Level 1 evaluation is optional but recommended.

Appendices A.2 onwards categorise the organizational best practices. Other than those in Appendix A.1, assessment is not performed by the Evaluation Laboratory during a PSA certification Level 1 evaluation.

A.1 Assessable Organisational Best Practices

ID	Requirement	Supported?		
		Yes	Partial	N/A
BP2.2 (Optional)	The Developer should provide a public point of contact as part of its vulnerability disclosure policy.			
	(Optional notes)			
BP3.3 (Optional)	The Developer should explicitly state the minimum length of time for which the device will receive security updates.			
	(Optional notes)			

A.2 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.3 Vulnerability Disclosure

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

A.4 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. See Appendix A.1.

A.5 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.6 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.7 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 internet connected device and IoT domains are 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 v2.1.0 standard, as per Table B.1 of [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.

ETSI EN 303 645 V2.1.0 (2020-04) Provisions	PSA Level 1 Requirements
5.1-1: Unique per device passwords	D4.1: Critical Security Parameters
5.1.2: Automated password attacks	D4.2: Automated password attacks
5.1-3: Cryptography for user authentication	S5.3: User authentication
5.1-4: Change of authentication value	S6.1: Security configuration
5.1-5: Authentication mechanism attack resilience	D4.2: Password best practices D4.3: Password threshold
5.3-2: Mechanisms for secure updates	S1.1: Firmware update S1.2: Anti-rollback
5.3-7: Best practice cryptography for updates	S1.1: Firmware update
5.3-10: Trust relationship for updates	S1.1: Firmware update D2.2: Client-Server Authentication
5.4-1: Sensitive parameter secure storage	S2.2: Secure storage
5.4-2: Secure storage of ID	C1.4: ID storage
5.4-3: Configurable security parameters	D4.1: Critical security parameter
5.4-4: CSP unique per device resistant to automated attack	S5.1: CSP unique per device resistant to automated attack
5.5-1: Secure communication	S3.3: TLS
5.5-5: Authentication parameters configuration	S6.1: Configuration
5.5-7: Sensitive data encryption over network	D2.3: Communication encryption
5.6-1: Disable unused ports	D2.1: No unused port
5.6-2: Minimize unauth disclosure	S3.3: Secure protocols that do not leak
5.6-4: Software disable of debug interface	S4.2: Unneeded functionalities
5.11-1: User data erasure	S7.1: Erase user data

ETSI EN 303 645 V2.1.0 (2020-04) Provisions	PSA Level 1 Requirements
5.13-1: Input validation	S4.5: Input validation

B.2 NISTIR 8259A

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

NISTIR 8259A Capabilities	PSA Level 1 Requirements
Device identification	C1.4 ID storage S2.1 Device ID
Device configuration	C2.3 Access control PSA-RoT S6.1 Configuration S7.1 Factory settings
Data protection	C1.1 Isolation C1.4 Secure storage C2.4 Cryptography S2.2 Secure storage S2.3 Cryptography S6.1 Configuration S7.1 Erase user data D5.2 Personal data
Logical access to interfaces	C2.3 Access control PSA-RoT S3.1 Connection authentication S3.2 Communication encryption S3.3 TLS S4.2 Unneeded functionalities S4.5 Input validation S6.1 Configuration D2.1 No unused port D2.2 Communication authentication D2.3 Communication encryption D2.4 TLS D3.1 Debug D3.3 Unneeded functionalities
Software and firmware update	C2.1 Firmware update C2.2 Rollback S1.1 Firmware update S1.2 Rollback S6.1 Configuration

NISTIR 8259A Capabilities	PSA Level 1 Requirements
Cybersecurity state awareness	C1.3 Security lifecycle S4.1 Attestation S4.3 Log S4.4 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 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 2.0

This appendix summarizes the changes introduced on requirements between this revision of PSA Certified Level 1 and version 2.0.

PSA Certified L1 v.2.1	Changes from v2.0	PSA Certified L1 v2.0 requirement
C1.1	Unchanged	C1.1
C1.2	Clarification on use of symmetric signing.	C1.2
C1.3	Generalisation of lifecycle states and applicable data.	C1.3
C1.4	Clarification on data items.	C1.4
C2.1	Clarification on scope of update and checks prior to installation.	C2.1
C2.2	Clarification that anti-rollback is strongly recommended but not mandatory with V.2.	C2.2
C2.3	Broadened scope.	C2.3
C2.4	Added need to consider the source of random data.	C2.4
S1.1	Clarification on the scope of update and checks before installation.	R1.1
S1.2	Clarification that anti-rollback is strongly recommended but not mandatory with V.2.	R1.2
S2.1	Clarification on the use of PSA-RoT.	R2.1
S2.2	Reworded.	R2.2
S2.3	Rewording, and note about use of PSA-RoT moved to guidance.	R2.3
none	Removed requirement on update of cryptographic algorithms and primitives. Though recommended, this originated as a mandatory ETSI 303 645 requirement, but that is no longer the case.	R2.4
S3.1	Reworded.	R3.1
S3.2	Added integrity checks and scope extended to include remote devices.	R3.2
S3.3	Extended to include the possibility of a data leak leading to identification of a device that might be known to be vulnerable. This arises from an ETSI 303 645 requirement.	R3.3
S4.1	Unchanged.	R4.1
S4.2	Clarification to reflect that removal of some unwanted functionality may not be practical.	R4.2
S4.3	Added need for integrity protection to security logs.	R4.3
S4.4	Unchanged.	R4.4

PSA Certified L1 v.2.1	Changes from v2.0	PSA Certified L1 v2.0 requirement
S4.5	Reworded.	R4.5
S4.6	Added requirements related to the concept of least privilege.	none
S5.1	Added text about determining parameters via automated means or from published data. Removes applicability to passwords as that is covered in S5.2.	R5.1
S5.2	Added text about password uniqueness and determining passwords via automated means or from published data.	R5.2
S5.3	Unchanged.	R5.3
S6.1	Reworded.	R6.1
S7.1	Clarified scope.	R7.1
D1.1	Extended to cover any Application RoT(s) and recommends secure boot apply to at least first stage of NSPE code.	D1.1
D1.2	Clarification that anti-rollback is strongly recommended but not mandatory with V.2.	D1.2
D2.1	Clarified application to logical interfaces.	D2.1
D2.2	Broadened to cover remote devices as well as servers.	D2.2
D2.3	Broadened to cover remote devices as well as servers, and generalized data types.	D2.3
D2.4	Unchanged.	D2.4
D3.1	Extended to cover debug symbols.	D3.1
D3.2	Reworded.	D3.2
D3.3	Clarification to reflect that removal of some unwanted functionality may not be practical.	D3.3
D3.4	Added authorized access to security relevant logs.	D3.4
D3.5	Unchanged.	D3.5
D3.6	New to cover correct use of PSA-RoT in the composition process.	none
D4.1	Added text about determining parameters via automated means or from published data.	D4.1
D4.2	Added text about password uniqueness and determining passwords via automated means or from published data.	D4.2
D4.3	Reworded.	D4.3
D4.4	Reworded.	D4.4
D4.5	Reworded.	D4.5
D5.1	Unchanged.	D5.1

PSA Certified L1 v.2.1	Changes from v2.0	PSA Certified L1 v2.0 requirement
D5.2	Unchanged.	D5.2
none	Moved to Appendix A.1.	D6.1
none	Moved to Appendix A.1.	D6.1

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

PSA Certified L1 v.2.1	Expected answer
C1.1 Hardware isolation of SPE	Only "Yes"
C1.2 Secure Boot	"Yes"
C1.3 (Optional) Security lifecycle support	Any answer
C1.4 Secure storage of keys	"Yes"
C2.1 Firmware update	"Yes"
C2.2 Rollback protection	Any answer
C2.3 Access control for modifications to PSA-RoT	"Yes"
C2.4 Best Practice Crypto	"Yes"

D.1.2 ETSI EN 303 645 v2.1.0 Mapping

PSA Certified L1 v.2.1	Expected answer
C1.4 ID Storage	"Yes"

D.1.3 NISTIR 8259A Mapping

PSA Certified L1 v.2.1	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 mandatory question answered not in conformance with “Expected answer” with rationale of why security is unaffected.

PSA Certified L1 v.2.1	Expected answer
S1.1 Firmware update	“Yes”
S1.2 Prevent rollback	Any Answer
S2.1 Use PSA-RoT for ID queries	“Yes”
S2.2 Use secure storage	“Yes”
S2.3 Best practice crypto	“Yes”
S3.1 Authenticate remote servers	“Yes”
S3.2 Ability to encrypt data exchanged	“Yes”
S3.3 Two-way comms use secure protocols for auth and encryption e.g. TLS >= v1.2	“Yes”
S4.1 Attestation method of lifecycle state	“Yes”
S4.2 Disable/not install unused functionality	“Yes”
S4.3 (Optional) System software should log security events	Any Answer
S4.4 (Optional) If logging enabled, restrict access of log files to auth users only	Any Answer
S4.5 Input protected against malformed input	“Yes”
S4.6 Lowest privilege necessary	“Yes”
S5.1 If using critical security parameters they are unique per device	“Yes” or “N/A”
S5.2 If using passwords then best practice	“Yes” or “N/A”
S5.3 If using user auth then crypto is best practice	“Yes” or “N/A”
S6.1 If security config changeable – auth first	“Yes” or “N/A”
S7.1 If personal data stored it should be erasable /device reset	“Yes” or “N/A”

D.2.2 ETSI EN 303 645 v2.1.0 Mapping

PSA Certified L1 v.2.1	Expected answer
S1.1 Firmware update	“Yes”
S1.2 Prevent unauth rollback	“Yes”
S2.2 Secure Storage	“Yes”

PSA Certified L1 v.2.1	Expected answer
S3.3 Two-way comms use secure protocols for auth and encryption e.g. TLS >= v1.2	“Yes”
S4.2 Functionality not needed is not installed	“Yes”
S4.5 Input validation	“Yes”
S5.1 CSP Unique per Device	“Yes”
S5.3 User Auth	“Yes”
S6.1 Configuration	“Yes”
S7.1 Erase user data	“Yes”

D.2.3 NISTIR 8259A Mapping

PSA Certified L1 v.2.1	Expected answer
S1.1 Firmware update	“Yes”
S1.2 Prevent rollback	“Yes”
S2.1 Use PSA-RoT for ID queries	“Yes”
S2.2 Use secure storage	“Yes”
S2.3 Best practice crypto	“Yes”
S3.1 Authenticate remote servers	“Yes”
S3.2 Ability to encrypt data exchanged	“Yes”
S3.3 Two-way comms use secure protocols for auth and encryption e.g. TLS v1.2 or later	“Yes”
S4.1 Attestation token of lifecycle state	“Yes”
S4.2 Disable/not install unused functionality	“Yes”
S4.3 System software should log security events	“Yes”
S4.4 Restrict access of log files to auth users only	“Yes”
S4.5 Input protected against malformed input	“Yes”
S5.2 Passwords best practice	“Yes”
S6.1 Security config changeable – auth first	“Yes”
S7.1 Personal data erasable /device reset	“Yes”

D.3 Device Assessment Questionnaire

D.3.1 PSA Certified Level 1

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

PSA Certified L1 v.2.1	**Expected answer**
D1.1 Secure boot with validated software	“Yes”
D1.2 PSA-RoT is updateable	“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 unauthorized use of debug	“Yes”
D3.2 Security lifecycle attestable	“Yes”
D3.3 Functionalities not needed disabled or not installed	“Yes”
D3.4 (Optional) Log security events	Any answer
D3.5 (Optional) If log, restrict log files to auth users	Any answer
D3.6 Use of PSA-RoT Services	“Yes”
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”

D.3.2 ETSI EN 303 645 v2.1.0 Mapping

PSA Certified L1 v.2.1	**Expected answer**
D2.1 Close unused network ports/interfaces	“Yes”
D2.2 Ability to auth remote servers	“Yes”
D2.3 Encrypt by default data exchanged	“Yes”
D4.1 Critical security params unique per device	“Yes”

PSA Certified L1 v.2.1	Expected answer
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 8259A Mapping

PSA Certified L1 v.2.1	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 unauthorized 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.2.1	Expected answer
D4.2 Device uses password best practice	“Yes”

D.3.5 Marking Sheet Summary

PSA Level 1 pass?	Answer
PSA Certified Level 1 – Chip section pass achieved?	
PSA Certified Level 1 – System software pass achieved?	
PSA Certified Level 1 – Device pass achieved?	
ETSI EN 303 645 Chip section pass achieved?	
ETSI EN 303 645 System software section pass achieved?	
ETSI EN 303 645 Device pass achieved?	

PSA Level 1 pass?	**Answer**
NISTIR 8259A Chip section pass achieved?	
NISTIR 8259A System software section pass achieved?	
NISTIR 8259A Device section pass achieved?	
SB-327 mapping pass achieved?	