PSA Certified™ Level 1 Questionnaire Version 3.0 BETA 01

psacertified™

psacertified™
level one

Document number:	JSADEN001
Version:	3.0
Release Number:	BETA 01
Author	PSA JSA Members: Applus+ Laboratories Arm Limited CAICT DEKRA Testing and Certification ECSEC Laboratory Inc Prove & Run S.A.S. Riscure B.V. Serma Safety & Security S.A.S SGS Brightsight B.V. TrustCB B.V. UL TS B.V.
Authorized by:	PA JSA Members
Date of Issue:	10/11/2023

© Copyright Arm Limited 2017-2023. All rights reserved.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Abstract

PSA Certified is an independent security evaluation scheme for Platform Security Architecture (PSA) based chips, system software and for connected devices, including IoT, Edge devices, industrial and automotive applications. 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.

This version includes certification options covering the draft European Union Cyber Resiliency Act, the United Kingdom Product Security and Telecommunications Infrastructure Act, and the work in progress Radio Equipment Directive cyber-security requirements.

Keywords

PSA Certified Level 1, certification, chip, connected device, internet, IoT, Platform Security Architecture, questionnaire, PSA, security, system software, device, Cyber Resiliency Act, Product Security and Telecommunications Infrastructure Act, Radio Equipment Directive.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Copyright ©2017-2023 Arm Limited or its affiliates. All rights reserved. The copyright statement reflects the fact that some draft issues of this document have been released, to a limited circulation.

Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third-party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at http://www.arm.com/company/policies/trademarks.

Copyright © 2023 Arm Limited (or its affiliates). All rights reserved.

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

Contents

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: V3.0 BETA 01

1.2 Release Information

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

Date	Version	Confidentiality	Change
10/11/2023	3.0 BETA 01	Non-confidential	Update on the requirements due to regulations included in new section 7.
18/05/2022	2.2 REL01	Non-confidential	Clarifications and enhancements. Draft alignment with Matter and ioXt.
30/09/2021	2.1 REL02	Non-confidential	Clarification on questionnaire reuse, minor clarifications, some now optional, removal of examples, alignment with web version.
22/02/2021	2.1 REL01	Non-confidential	Minor refinements and clarifications based on evaluation submission feedback.
21/08/2020	2.1 Beta	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
[1]	DEN 0014	ARM	Platform Security Model
[2]	EN 303 645	ETSI	Cyber Security for Consumer Internet of Things; V2.1.1 (2020-06)
[3]	NISTIR 8259A	NIST	IoT Device Cybersecurity Capability Core Baseline; May 2020

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Ref	Doc No	Author(s)	Title
[4]	Bill No. 327; Chapter 886.	California State Senate	Security of Connected Devices
[5]		UK Department for Science, Innovation and Technology[1]	Proposals for regulating consumer smart product cyber security.
[6]	23-27349-003	Connectivity Standards Alliance	Matter 1.2 Core Specification
[7]		ioXt alliance	ioXt 2021 Base Profile, version 2
[8]	2022/0272 15.9.2022	European Commission (Cyber Resiliency Act)	Horizontal Cybersecurity Requirements for Products with Digital Elements and amending Regulation EU 2019/1020.
[9]	15.9.2022	European Commission	ANNEXES for [8]
[10]	13/7/2023	European Union	**Interinstitutional File: 2022/0272(COD) 11725/23**
[11]		UK Government	The Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable products) Regulations 2023.
[12]	Directive 2014/53/EU	European Union	**DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC**
[13]	29.10.2021 C(2021) 7672 final	European Union	**COMMISSION DELEGATED REGULATION (EU) .../... of 29.10.2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f),**
[14]	5.8.2022 C(2022) 5637 Final	European Union	**ANNEXES to the Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the**
[15]	SP800-57 Part 1 r5	NIST	Recommendation for Key Management: Part 1 – General

[1] Formerly the Department for Digital, Culture, Media & Sport

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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.
Best Practice Cryptography	Use of cryptographic algorithms, modes and protocols, key generation and random number generation approved by a government or by an industry body in the intended deployment market(s). Use of cryptographic algorithms with a cryptographic strength suitable for the expected lifetime of the device should be used. Where possible, the ability to change the algorithms in use should be considered.
Critical Security Parameter	Secret information, with integrity and confidentiality requirements, that is used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc. Critical Security parameters are considered to be Sensitive Data. In some contexts, these data 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
Factory Reset	Factory reset means reset to any state that might be as delivered from the manufacturer, for example, including any manufacturer provided updates after the initial delivery of the device.
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 executes 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 Certified API	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

PSA Certified API Certification	Functional certification confirms that the device implements the PSA Certified APIs correctly by passing the PSA Certified API 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 which is the most trusted security component on the device. See [1].
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.
Personally Identifiable Data	Information that relates to an identified or identifiable individual. Such data is considered to be Sensitive Data if disclosure or modification causes harm to the identified individual.
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 Certified 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 executes the PSA-RoT, the PSA-RoT Services, 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.
Sensitive Data	Any data that if, for example, is disclosed or modified, could result in a device vulnerability, jeopardize any service that relies on it, or cause harm to an identifiable individual.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its critical security parameters, or that implements some of its services.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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.

2.1.1 PSA Certified

The PSA Certified scheme involves the mandatory evaluation 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.

The 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 (section 4), the System Software vendor (section 5) or the Device OEM (section 6). 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 security measures.

Example answers for the questions can be found in the web-based version of this document, which can be found at **certify.psacertified.org**.

In the case of a successful evaluation a digital certificate is issued by the PSA Certification Body for that certification, which 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.

2.1.2 PSA Certified API Certification

PSA Certified API Certification, which is optional, means that a device has implemented the **PSA Certified API**[3] and passed the PSA Certified API Certification test suites. The PSA Certified APIs cover three security functions: Attestation, Cryptography and Secure Storage. A step-by-step guide for getting a product PSA Certified API certified is available on **www.psacertified.org/resources**.

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

[2] https://datatracker.ietf.org/doc/draft-tschofenig-rats-psa-token/
[3] https://developer.arm.com/architectures/security-architectures/platform-security-architecture

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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].

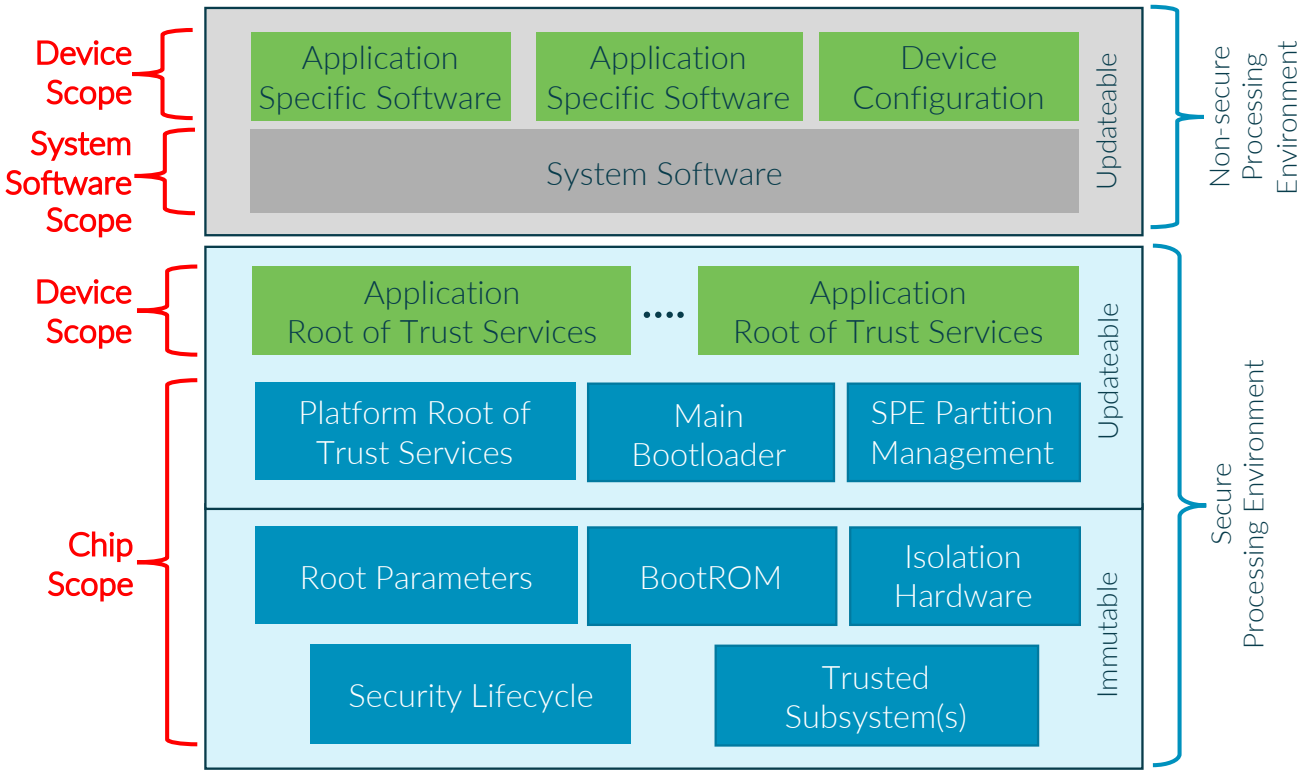

Figure 1: Logical Scope of Chip, System Software and Device Levels

The Chip security evaluation scope includes the following Secure Processing Environment PSA-RoT elements, see also [1]:

- Immutable Platform Root of Trust, for example, the Boot ROM, any root parameters, the NSPE/SPE isolation hardware, and any hardware-based security lifecycle management and enforcement.
- Updateable Platform Root of Trust, for example, a main bootloader, the code that implements the SPE Partition Management function, the code that implements the PSA defined services[5] such as attestation, secure storage, and cryptography.
- Any Trusted subsystems that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

The Chip scope hardware may be a System-on-Chip or a System-in-Package, possibly supported by board level trusted subsystem components, for example, a Secure Element or Subscriber Identification Module.

[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.
[5] The Updateable Platform Root of Trust may also execute any Application specific Root-of-Trust services, but these are not in the scope of a Chip certification.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 leads 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 declared in the system software certificate; see section 2.4.2 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 declared 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.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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[6] 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.

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. The optional PSA Certified 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.

From version 3.0, the vendor may choose to have their solution evaluated in the context of the regulations covered in section 7. In this case, the vendor must complete the required part or parts of section 7.

2.4.1 Options for submission directly to the PSA Certification Body

Where a product is developed from one already PSA Certified and the exact same questionnaire answers and declarations are applicable, then section 3.7 can be completed instead of the sections stated above and submitted directly to the PSA Certification Body. Checking for acceptability with the PSA Certification Body or chosen Evaluation Laboratory is recommended. Section 3.7 can be used in the following situations;

- a new Chip uses the same certified PSA-RoT implementation,
- updated certified System Software on the same Chip declared in the referenced certification,
- a new device using the same System Software and Chip declared in the referenced certification.

2.4.2 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 Certified 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 at **www.psacertified.org/getting-certified/silicon-vendor/overview/level-1/questionnaire-composition**.

[6] A System Software certificate is only applicable with a valid PSA Certified chip, or the chip named in the certificate.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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, 6 or 7 as specified in section 2.4. It is recommended that the Developer also complete the assessable organizational best practices questions in Appendix A.1.
2. For each requirement in the relevant section, a single box corresponding to the fulfilment of the requirement is ticked (or marked in an equivalent way) 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 Certification Body 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 variant of an existing certified product, the Developer can reuse the questionnaire that was reviewed by the Evaluation Laboratory provided exactly the same answers and declarations apply (see section 3.7). 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 and outline how the changes do not impact the security relative to the original certified product. The EAN-13 for the new product will differ from the product already certified.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

3 Assessment Information

The vendor applying for PSA certification shall fill all applicable parts of this section.

3.1 Contact

Company activity:	*(State whether Device (OEM) vendor, 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.

Check the boxes below if the scope of evaluation is to cover compliance with any of the regulations in section 7.

- ☐ EU Cyber Resiliency Act (section 7.1)
- ☐ UK Product Security and Telecommunications Infrastructure Act (section 7.2)
- ☐ Radio Equipment Directive (section 7.3)

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

3.3 Product Reference

This declaration is applicable for a Chip evaluation;

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 for retrieval. See Appendix A.1.)*

This declaration is applicable for a System Software evaluation;

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 is made of chip-level security functionality in addition to that required for the PSA-RoT. See section 2.4.2)*
Vulnerability disclosure policy:	*(If a vulnerability disclosure policy is available for this product, provide the URL for retrieval. See Appendix A.1.)*
Information and Instructions:	*(If user information and instructions are available for this product, provide the URL for retrieval.)*

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

This declaration is applicable for a Device evaluation;

Device name:	*(e.g., Smart Camera, Model123)*
Device version:	*(The version number or an identifier for the build of the device, including the software)*
Device EAN-13:	*(If this version of the Device is already PSA Certified, specify the EAN-13 of the certificate)*
Device reference documentation:	*(If this version of the Device is not PSA Certified, provide identification of the reference documentation used to fill the Device questionnaire. It may be requested by the Evaluation Laboratory)*
Device use of chip security features:	*(Please indicate what use is made of chip-level security functionality in addition to that required for the PSA-RoT. See section 2.4.2)*
Vulnerability disclosure policy:	*(If a vulnerability disclosure policy is available for this product, provide the URL for retrieval. See Appendix A.1.)*
Information and Instructions:	*(If user information and instructions are available for this product, provide the URL for retrieval.)*

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 evaluation:

PSA Certified API **certification:**	*PSA Certified 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 [1] defines two incremental isolation boundaries; please indicate if these are deployed;

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

	☐ 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)*
Entropy Source	*(List any applied random number specification or conformance tests of the entropy source. This information will be included in the certificate.)*

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 and selected in section 3.2, of this questionnaire is valid and correct for the product/service stated in Section 3.3.
2. The information provided in the applicable parts of section 7, as selected in section 3.2, of this questionnaire is valid and correct for the product stated in section 3.3.

and

3. 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 questionnaire

This declaration applies for a product that reuses the exact same questionnaire answers and any declarations that have 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. The vendor can apply directly to the PSA Certification Body. See section 2.4.1.

EAN-13 of the product that passed PSA Certified:	

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 14, 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:	

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 sections 1.4 and 2.2. Skip this section if the version of the chip referred in Section 3.3 is already PSA Certified. Instructions are given in section 2.5 on selection of one of “Yes”, “Partial” or “N/A” as the answer.

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.

Where cryptography is used to meet any of the requirements, then best practice cryptography shall be used, see section 1.4.

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.)			
C1.2	The chip shall support Secure Boot, initiated from code in the immutable Platform Root of Trust, and which ensures device security in the event of a failure. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded. 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. Describe how a Secure Boot failure is handled and how the security of the device is maintained.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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, including any factory reset. In all cases the requirements of BP5.3 must be considered. 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 PSA Certified.*			
	(Describe supported lifecycle states and transition rules, and for each state, which critical Security Parameters, and any other sensitive data, is protected and how it is protected.)			
C1.4	The chip shall support the secure storage or derivation of following minimum set, or equivalent, of critical security parameters: • 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. • An identifier or identifiers that uniquely identifies the Immutable PSA-RoT of the chip, for example, manufacturer, part number, revision number, and identifies the specific instance. If the chip supports attestation the chip shall also support the secure storage or derivation of the following, or equivalent, critical security parameters: • A secret attestation key. • An identifier that uniquely identifies the attestation key. The chip may support the secure storage of additional critical security parameters and sensitive data. All critical security parameters must be protected against unauthorized modification, and the secret parameters protected also against unauthorized reading. Protection is required against software attacks and basic physical attacks such as probing of the external interfaces of the chip. These keys and identifiers may be injected during chip manufacture, or during the manufacture of the device by the OEM			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
	(see C1.5), 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 and how the chip data are protected from modification.			
C1.5 Optional	The chip shall support the injection of keys and identifiers during the manufacture of the device by the OEM. A typical example is the key used for authenticating the first updateable firmware image.			
	(Describe the mechanisms available to an OEM to provision keys and identities and how to enforce modification and read rights (see C1.4).)			

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 immediately prior to execution (see C1.2) and, optionally, at the time of download. This includes the executable code and any related data, such as configuration data, and version numbering. 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 (Optional)	The PSA-RoT 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. *NB: Anti-rollback is strongly recommended but not mandatory in PSA Level 1 V3.0.*			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
	(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 authorized 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 using the PSA Secure Storage service (or equivalent).			
	(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 example, 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. This PSA Certified level requires a minimum security strength in line with the current version of NIST SP-800-57 [15] recommendations. RSA-2048 will not be accepted in products certified from 2027 onwards. *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.* *NB: A TRNG or a suitably seeded Deterministic Random Bit Generator can be used. The Developer should declare any conformance with random number specifications, for example NIST SP800-90B, for inclusion in the certificate.*			
	(List the cryptographic algorithms provided by the PSA-RoT and the supported key sizes. Also describe how random number generation is performed.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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. Instructions are given in section 2.5 on selection of one of "Yes", "Partial" or "N/A" as the answer.

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 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.

Where cryptography is used to meet any of the requirements, then best practice cryptography shall be used, see section 1.4.

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 immediately prior to execution and, optionally, at the time of download. This includes the executable code and any related data, such configuration data and version numbering. 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.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
S1.2 (Optional)	The System Software shall prevent unauthorized rollback of updates to system software, any applicable application software and authentication data. A mechanism may be provided to support authorized rollback for recovery reasons. *NB: Anti-rollback is strongly recommended but not mandatory in PSA Level 1 V3.0.*			
	(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.)			
S1.3 (Optional)	The System Software should perform Secure Boot for the NSPE System Software and application specific software. Note that the first stage of the System Software should be authenticated by the PSA RoT, see C1.2 and D1.1. This requirement refers to extending the chain of trust beyond the first stage of the NSPE. The Secure Boot process shall ensure the security of the device in the event of a failure.			

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). The System Software should rely only on the PSA-RoT for all other PSA RoT stored or derived critical security parameters, 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 and BP5.6).			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
	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.)			
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, key lengths, random number generation, and generation of critical security parameters from low entropy sources, 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 a minimum security strength in line with the current version of NIST SP-800-57 [15] recommendations. RSA-2048 will not be accepted in products certified from 2027 onwards			
	(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 establish a trust relationship when making a connection with any devices or servers. This is typically achieved through authentication. This will likely be used for Device requirement D2.2.			
	(Describe how this requirement is met.)			
S3.2	The System Software shall provide the ability to ensure the confidentiality and integrity of data exchanged with remote devices and servers.			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

	This will likely be used for Device requirement D2.3.			
	(Describe how this requirement is met.)			
S3.3	The System Software shall provide 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. This will likely be used for Device requirement D2.4. *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. List the protocols used and if they are certified.)			

5.4 Hardening

ID	Requirement	Supported?		
		Yes	Partial	N/A
S4.1 (Optional)	The System Software shall support an attestation method that can be used to prove the genuineness of the device. If possible, the current security lifecycle state of the device should be included. This should make use of a PSA RoT Initial Attestation Key (see C1.4), or equivalent, to bind any attestation report to the specific chip instance. This will likely be used for Device requirement D3.2.			
	(Describe how this requirement is met. Note that use should be made of the PSA-RoT secure attestation service for the most secure solution.)			
S4.2	Software functionality that is not needed for the intended usage of the device shall not be installed. If non-installation is not practical then techniques to prevent use should, wherever possible, be used. Where this can only be determined by the Device manufacturer, the System Software shall provide the necessary mechanisms. This will likely be used for Device requirement D3.3.			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
S4.3 (Optional)	The System Software should provide logging of security relevant events and errors. The log should include sufficient detail to determine what happened and should be integrity protected. Examples of relevant security events and errors may include those related to secure boot (S1.3, C1.2), updates (S1.1, C2.1), anti-rollback (S1.2, C2.2), access violations (S4.6, C1.1), unauthorized access (S3.1, S4.4, S6.1, S7.1, C1.4, C2.3), invalid data (D3.8, S4.5). *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 physical or logical interfaces shall be validated defensively against malformed input. Data output via physical or logical interfaces shall not lead to the identification of vulnerable devices or result in a device vulnerability. Data transferred via critical system software Application Programming Interfaces (API) shall be validated defensively against malformed input and return data should not lead to a vulnerability. *NB: System Software compliance may be limited because any data input or output that is application specific may only be practical at the Device level (see D3.8).*			
	(Describe how this requirement is met.).			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
S4.6	If supported, 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. Where supported, each authenticated user, application, process, etc., shall have limited privileges based on pre-determined and/or securely configurable access controls.			
	(Describe how this requirement is met.)			

5.5 Passwords and Critical Security Parameters

ID	Requirement	Supported?		
		Yes	Partial	N/A
S5.1	If the System Software has a mechanism to reset passwords and critical security parameters, they shall not be resettable to any universal factory default value. Such data 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.)			
S5.3	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.			
	(Describe the cryptographic algorithms and key sizes used for user authentication)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

5.6 Configuration

ID	Requirement	Supported?		
		Yes	Partial	N/A
S6.1	If the System Software allows security-relevant configuration changes via a network or other interface, the related configuration change shall only be accepted after authentication (see S1.1, 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).			
	(Describe how this requirement is met.)			

5.7 Privacy

ID	Requirement	Supported?		
		Yes	Partial	N/A
S7.1	If the System Software allows persistent storage of personal configuration data, it shall allow only the owner or an authorized entity to read and erase this data.			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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. Instructions are given in section 2.5 on selection of one of “Yes”, “Partial” or “N/A” as the answer.

Where cryptography is used to meet any of the requirements, then best practice cryptography shall be used, see section 1.4.

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 Service(s) (see C1.2) and at least the first executable code image, but ideally all, of the NSPE system software and application specific software (see S1.3). The Secure Boot process shall ensure the security of the device in the event of a failure.			
	(Describe how this requirement is met. Describe how a Secure Boot failure is handled and how the security of the device is maintained.)			
D1.2	The device shall ensure the authenticity and integrity, and apply any anti-rollback checks, of software updates. Delivery of software updates via network interfaces shall be in accordance with D2.2. The device shall be configured to ensure that the PSA-RoT and any Application RoT Service(s) updates are performed (see C2.1), and that any anti-rollback checks are performed (see C2.2). The device shall be configured to ensure that any system software update is performed, (see S1.1), and that any anti-rollback checks are performed (see S1.2). The device shall apply application software updates and ensure that any anti-rollback checks are performed. Push or pulled automatic update and/or update notification should be enabled by default if the deployment eco system requires it. Disabling, enabling, or postponing installation of security updates and/or update notifications shall be possible by authorized entities. *NB: Anti-rollback is strongly recommended but not mandatory in PSA Level 1 V3.0.*			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

6.2 Communication

ID	Requirement	Supported?		
		Yes	Partial	N/A
D2.1	The device shall close all physical and logical interfaces not necessary for the intended use of the device. Examples include, serial and network interfaces, TCP/UDP ports or sockets relating to services not required.			
	(Describe how this requirement is met.)			
D2.2	For two-way communication, the device shall ensure that a trust relationship is established when making a connection with any devices or servers. This is typically achieved through authentication. This will likely rely on System Software requirement S3.1.			
	(Describe how this requirement is met.)			
D2.3	The device shall ensure the confidentiality and integrity of all data exchanged with connected devices and servers. Critical security parameters, including passwords, and any service or personally identifiable sensitive data shall always be protected in confidentiality. This will likely rely on System Software requirement S3.2.			
	(Describe how this requirement is met.)			
D2.4	The device shall use secure protocols for D2.2 and D2.3. The selected protocols shall not leak data that would lead to the identification of vulnerable devices or result in a device vulnerability. *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.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

6.3 Hardening

ID	Requirement	Supported?		
		Yes	Partial	N/A
D3.1	Deployed (production) devices shall be protected against unauthorized use of debug or test features, with rules depending on device lifecycle state. Where debug is not permitted, debug symbols shall not be present in the code images on the device. The device shall make inaccessible or erase critical security parameters, including passwords and any sensitive user assets and credentials, when debug and test features are enabled.			
	(Describe which technical measures disable or deactivate debug)			
D3.2 (Optional)	The current security lifecycle state of the device should be reportable, ideally in an attestable form, for example, using an Entity Attestation Token[2]. This will likely rely on System Software requirement S4.1.			
	(Describe how this requirement is met.)			
D3.3	Software functionality that is not needed for the intended usage of the device shall not be installed. If non-installation is not practical then techniques to prevent use should, wherever possible, be used. Hardware functionality, interfaces and test points that are not needed for the intended usage of the device shall be disabled. If disabling is not possible then techniques to prevent use should, wherever possible, be used. This will likely rely on System Software requirement S4.2.			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
D3.4 (Optional)	The device should support audit logging of security relevant events and errors. The log should include enough details to determine what happened. Examples of relevant security events and errors may include those related to secure boot (D1.1, S1.3, C1.2), updates (D1.2, S1.1, C2.1), anti-rollback (D1.2, S1.2, C2.2), access violations (D3.7, D3.9, S4.6, C1.1), unauthorized access (D3.10, S3.1, S4.4, S6.1, S7.1, C1.4, C2.3), invalid data (D3.8, S4.5). *NB: Not all devices may support logging, for example, due to constrained resources. 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 audit logging, it shall restrict read access to log files to authorized users only. Write access shall be restricted to the logging service.			
	(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.)			
D3.7	The device shall be configured to ensure that all application specific software and system software executes with the lowest level of privilege necessary for the intended function. For example, each authenticated user, application, process, etc., shall have minimal privileges based on pre-determined and/or securely configurable access controls. This will likely rely on System Software requirement S4.6.			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
D3.8	Data input via physical or logical interfaces shall be validated defensively against malformed input. Data output via physical or logical interfaces shall not lead to the identification of vulnerable devices or result in a device vulnerability. Data transferred via critical Application Programming Interfaces (API) shall be validated defensively against malformed input and return data should not lead to a vulnerability. *NB: System Software level validation (see S4.5) may be limited because any application specific validation may only be practical at the Device level.*			
	(Describe how this requirement is met.)			
D3.9	The device shall be configured to make use of hardware isolation mechanisms (including those configured by privileged software) to control access to memory and registers. This applies to both instruction fetches and data accesses by processors and hardware engines. It is a mandatory requirement that the device is configured to ensure isolation of the SPE from the NSPE. This may require support by the System Software (see S2.2, S4.6, S7.1) and Chip (see C1.1, C1.4, C2.3)			
	(Describe how this requirement is met.)			
D3.10	The device shall ensure that any security-relevant configuration changes, including critical security parameters and passwords, via a network or other interface, shall only be accepted after authentication.			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

6.4 Passwords and Critical Security Parameters

ID	Requirement	Supported?		
		Yes	Partial	N/A
D4.1	All critical security parameters, including passwords, shall be unique per device or defined by the user. Such data shall not be resettable to any universal factory default value. Such data must not be easily determined by automated means or obtained from publicly available information. *NB: It follows that such data shall not be embedded in source code.*			
	(Describe how this requirement is met.)			
D4.2	If the device makes use of critical security parameters, including passwords, they should conform with security best practices, including, length, complexity, generation (for example, keys from passwords), and stored securely (see D4.5). NB: see NIST SP 800-63B guidelines for memorized secrets.			
	(Describe how this requirement is met.)			
D4.3	If the device makes use of critical security parameters, including passwords, the device shall implement mechanisms aimed at making brute force attacks impractical. For example, the device can apply rate limiting, or disable password entry and 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, including passwords, for authorization, the device shall implement mechanisms to prevent perpetual authorization. For example, the device can implement an inactivity time-out.			
	(Describe how this requirement is met.)			
D4.5	The device shall use secure storage for persistent critical security parameters, including passwords, and device identity (see D4.6). Storage of such data should use the PSA RoT. PSA-RoT storage mechanisms to bind the stored data to the specific device instance and, where supported, security lifecycle state. NB: The PSA-RoT secure storage offers protection against software attacks and basic physical attacks such as probing of any accessible interfaces. See C1.3 and C1.4.			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Requirement	Supported?		
		Yes	Partial	N/A
	(Describe how this requirement is met.)			
D4.6	The device shall be uniquely identifiable. For any machine-readable identity, secure storage provided by the PSA-RoT is required to prevent unauthorized modification or tampering, see D4.5 and C1.4. The unique device identity must be included in any attestation claim set, making the identity verifiable and attributable to that device instance.			
	(Describe how this requirement is met.)			
D4.7	The Device shall use best practice cryptography as required by applicable standards or recommended by national security agencies, covering choice of algorithms, key lengths, random number generation, and generation of critical security parameters from low entropy sources, 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 a minimum security strength in line with the current version of NIST SP-800-57 [15] recommendations. RSA-2048 will not be accepted in products certified from 2027 onwards.			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

6.5 Privacy

ID	Requirement	Supported?		
		Yes	Partial	N/A
D5.1	The device must ensure that any stored personal data, including that in any log files, shall only be accessible by the owner or an authorized entity. The device must support the erasure of any local data, including any personal information, passwords, keys, and log files, created through use by the end user, unless explicitly required to persist. Any such erasure, including through a factory reset (see section 1.4), must be authorized, and must leave the device in a secure state.			
	(Describe how this requirement is met.)			
D5.2 (optional)	The device shall use secure storage for persistent end user personal data, in accordance with D4.5.			
	(Describe how this requirement is met. Note that use should be made of the PSA-RoT secure storage service for the most secure solution.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

7 Regulations

7.1 EU Cyber Resilience Act

This section covers the requirements from EU Cyber Resiliency Act (EU-CRA) through a preliminary best endeavor mapping of PSA Certified based on the proposal document [8], its annexes [9] and adoption of the changes in [10].

PSA Certified Device level questions (section 6) requirements are mapped in section 7.1.1 to ANNEX I section 1 of [9] because they refer to the properties of the product, in other words, the device. This means that the given mappings are thought to comply with, or support meeting, the relevant requirement. The requirements will also be applicable to system software (e.g., operating systems) and the hardware (e.g., microprocessors and microcontrollers) in accordance with the classification in ANNEX III of [9]. However, the relevance in those cases may be less obvious and justification for non-compliance will be necessary.

ANNEX I section 2 of [9] is concerned with the vulnerability handling responsibilities of the device vendor and is covered in section 7.1.2.

ANNEX II of [9] is concerned with the user information and instruction responsibilities of the device vendor and is covered in section 7.1.3.

ANNEX III of [9] places product types into two classes where Class II products represent a greater risk than Class I products [8]. Such products require a "specific conformity assessment"; see ANNEX VI of [9] which covers conformity assessment procedures.

Some text in this section is reproduced without change from [9], the contents of which are licensed by the European Union under the Creative Commons Attribution 4.0 International (CC BY 4.0) license[7,8]. The original text can be found here **https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act**.

It is anticipated that EU-CRA will adopt the detailed technical requirements being developed by CEN/CENELEC in the context of the Radio Equipment Directive [14], see section 7.3. The timeframe is thought to be 2025.

7.1.1 Product Requirements (ANNEX I section 1)

ANNEX I section 1 ID	Products with digital elements shall;	Supported?		
		Yes	Partial	N/A
1	be designed, developed and produced in such a way that they enable an appropriate level of cybersecurity based on the risks.			
	(Describe how this requirement is met.)			

[7] **https://creativecommons.org/licenses/by/4.0/**

[8] **https://digital-strategy.ec.europa.eu/en/pages/legal-notice#ecl-inpage-km0gezfs**

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ANNEX I section 1 ID	Products with digital elements shall;	Supported?		
		Yes	Partial	N/A
3.aa[9]	be placed on the market without any known exploitable vulnerabilities.			
	(Describe how this requirement is met.)			
3.a	be placed on the market with a secure by default configuration, including the possibility to reset the product to its original state, and including a default setting that security updates be installed automatically according to requirements in point (aaa) of this section and Annex II (9), with a clear and easy-to-user opt-out mechanism;			
	(Describe how this requirement is met.) The following are set by default: D1.1, D2.1, D2.2, D2.3, D2.4, D3.1, D3.3, D3.7, D3.8, D4.1, D4.2, D4.3, D4.4. Reset is covered by: D5.1			
3.aaa	where applicable under Annex I,1 (3)a of this section, set as a default setting – which can be switched off – that security updates are installed automatically on products with digital elements if not installed within a certain timeframe;			
	(Describe how this requirement is met.)			
3.b	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems			
	(Describe how this requirement is met.) The following ensure unauthorised access is denied; D1.1, D2.1, D2.2, D2.4, D3.1, D3.3, D3.7, D3.9, D4.3, D4.6, D5.2			
3.c	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanism			
	(Describe how this requirement is met.) The following ensure confidentiality of data: D2.2, D2.3, D2.4, D3.7, D4.5, D5.1, D5.2			
3.d	protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions			
	(Describe how this requirement is met.) 1) D1.1, D1.2, D2.1, D2.2, D2.4, D3.1, D3.3, D3.10, D4.5 2) Report on corruptions: D3.4, D3.5, D3.7, D4.5, D5.1, D5.2			

[9] Was ANNEX I section 2

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ANNEX I section 1 ID	Products with digital elements shall;	Supported?		
		Yes	Partial	N/A
3.e	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product ('minimisation of data')			
	(Describe how this requirement is met.) D3.3, D3.7, D3.8			
3.f	protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks			
	(Describe how this requirement is met.) D2.1, D2.2, D2.4, D3.1, D3.3, D3.7, D3.8, D3.10			
3.g	minimise the negative impact by themselves or connected devices on the availability of services provided by other devices or networks			
	(Describe how this requirement is met.) D2.2, D2.4, D3.3			
3.h	be designed, developed and produced to limit attack surfaces, including external interfaces;			
	(Describe how this requirement is met.) D1.1, D2.1, D2.2, D2.4, D3.1, D3.3, D3.7, D3.8, D4.2			
3.i	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques			
	(Describe how this requirement is met.) D1.2, D3.7, D3.8, D3.9, D4.1, D4.3, D4.2, D4.4, D4.5			
3.j	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions			
	(Describe how this requirement is met.) D3.4, D3.5			
3.k	enable that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates by default, but with a clear and easy-to-user opt-out mechanism, and where applicable through the notification of available updates to users, and the option to temporarily postpone them			
	(Describe how this requirement is met.) D1.2			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ANNEX I section 1 ID	Products with digital elements shall;	Supported?		
		Yes	Partial	N/A
3.i	provide the possibility for users to securely and easily remove all data and settings and, where such data can be transferred to other products or systems, ensure this is done in a secure manner.			
	(Describe how this requirement is met.)			

7.1.2 Vulnerability Handling Requirements (ANNEX I section 2)

Annex I Section 2 ID	Manufacturers of the products with digital elements shall:	Supported?		
		Yes	Partial	N/A
1	identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product			
	(Describe how this requirement is met.)			
2	in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;			
	(Describe how this requirement is met.)			
3	apply effective and regular tests and reviews of the security of the product with digital elements			
	(Describe how this requirement is met.)			
4	once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and user friendly information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch			
	(Describe how this requirement is met.)			
5	put in place and enforce a policy on coordinated vulnerability disclosure			
	(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Annex I Section 2 ID	Manufacturers of the products with digital elements shall:	Supported?		
		Yes	Partial	N/A
6	take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements			
	(Describe how this requirement is met.)			
7	in relation to the cybersecurity risks posed to the products with digital elements, provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely and, where applicable, automatic manner			
	(Describe how this requirement is met.)			
8	ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.			
	(Describe how this requirement is met.)			

7.1.3 Information and Instructions to the User (ANNEX II)

Annex II ID	As a minimum, the product with digital elements shall be accompanied by;	Supported?		
		Yes	Partial	N/A
2[10]	the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received			
	(Describe how this requirement is met.)			
3	Name and type and any additional information enabling the unique [identification] of the product			
	(Describe how this requirement is met.)			
4	the intended purpose, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties			
	(Describe how this requirement is met.)			
5	any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks			

[10] Items 1, 6 and 7 were removed in [10]

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Annex II ID	As a minimum, the product with digital elements shall be accompanied by;	Supported?		
		Yes	Partial	N/A
	(Describe how this requirement is met.)			
8[10]	the type of technical security support offered by the manufacturer, expected product lifetime and end-date and until when the technical security support will be provided, at the very least until when users can expect to receive security updates			
	(Describe how this requirement is met.)			
9	detailed instructions or, where applicable, an internet address referring to such detailed instructions and information on: (a) the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use; (b) how changes to the product can affect the security of data; (c) how security-relevant updates can be installed; (d) the secure decommissioning of the product, including information on how user data can be securely removed. (e) how the default setting of automatically installed updates, as required by point (aaa) of section 1.3 of Annex I, can be turned off.			
	(Describe how this requirement is met.)			
10	If the manufacturer decides to make available the software bill of materials to the user, the information and instructions to the user accompanying the product with digital elements shall also include that software bill of materials as set out in Section 2, point (1) of Annex I			
	(Describe how this requirement is met.)			

7.2 UK Product Security and Telecommunications Infrastructure

The PSTI Act from the UK government comes into force on 29th April 2024.

The security requirements applicable to relevant connectable products[11] are defined in Schedule 1 of [11] and relate to passwords, information on how to report security issues, and information on minimum security update periods. Under Schedule 2 of [11], compliance with ETSI EN 303 645 [2] provisions 5.1-1, 5.1-2, 5.2-1, and 5.3-13 is deemed to show compliance with the Schedule 1 requirements. The requirements and the ETSI Provisions are covered in the section 7.2.1. The ETSI provisions are quoted with permission and are © ETSI 2020 All rights reserved.

Section 7.2.2 covers the minimum information required for any statement of compliance in accordance with Schedule 4 of [11].

[11] Note that Schedule 3 of [11] covers connectable products that are not in scope of the PSTI.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

7.2.1 Security Requirements

Schedule 1 ID	ETSI Provision deemed to show compliance with Schedule 1 security requirement	Supported?		
		Yes	Partial	N/A
1.(2) Passwords	Provision 5.1-1: Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user. Provision 5.1-2: Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.			
	(Describe how this requirement is met.) D4.1, D4.2			
2.(2) Information on how to report security issues	Provision 5.2-1: The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum: • contact information for the reporting of issues; and • information on timelines for: 1) initial acknowledgement of receipt; and 2) status updates until the resolution of the reported issues.			
	(Describe how this requirement is met.) BP2.1, BP2.2, BP2.3, BP2.4, BP2.5			
3.(2) Information on minimum security update periods	Provision 5.3-13: The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.			
	(Describe how this requirement is met.) BP2.2			

7.2.2 Minimum Information Required for Statement of Compliance

Schedule 4 of [11] specifies the minimum information that must be included in any statement of conformance. PSA certification is a statement of conformance to the PSA requirements, thus the following table lists the PSTI requirements and coverage by the PSA Certified process.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Schedule 4 ID	Minimum Information Required for Statement of Conformance	Supported?		
		Yes	Partial	N/A
1.(1)(a)	product (type, batch)			
	Section 3.3 Product Reference			
1.(1)(b)	name and address of each manufacturer of the product and, where applicable, each authorised representative;			
	Section 3.1 Contact			
1.(1)(c)	a declaration that the statement of compliance is prepared by or on behalf of the manufacturer of the product			
	Section 3.6 Declaration for new questionnaire or section 3.7 Declaration for reuse of an existing questionnaire and section 3.8 Declaration of conformance for a Device level certificate			
1.(1)(d)	a declaration that, in the opinion of the manufacturer, they have complied with either— (i) the applicable security requirements in Schedule 1; or (ii) the deemed compliance conditions in Schedule 2;			
	Device level PSA Certificate awarded			
1.(1)(e)	the defined support period for the product that was correct when the manufacturer first supplied the product;			
	(Describe how this requirement is met.) BP3.3			
1.(1)(f)	signature, name and function of the signatory			
	Section 3.8 Declaration of conformance for a Device level certificate			
1.(1)(g)	the place and date of issue of the statement of compliance.			
	Section 3.8 Declaration of conformance for a Device level certificate			

7.3 Radio Equipment Directive (RED) Cyber-security Requirements

The supplement [13] to Radio Equipment Directive (RED) covers articles 3(3) points (d), (e) and (f) concerning cyber-security.

The task of generating the detailed cyber-security requirements is covered in the ANNEXES [14]. Clause 1.1 (a) of Part A of Annex II concerns the "*detailed technical specifications"*. Clause 1.1 (b) concerns the "*test methods or equivalent approaches and conditions to verify compliance of the radio equipment with the corresponding specifications*".

ANNEX I of lists the following three harmonized standards, subsequently generated by CEN/CENELEC JTC13 working group 8.

1. prEN18301-1 covers the common security requirements for connected radio equipment.
2. prEN18301-2 covers the common security requirements for radio equipment processing focusing on childcare, toys, and wearables.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

3. prEN18301-3 covers the common security requirement focusing of processing virtual money or items of a monetary value.

Though the documents listed above are currently not available, the guidance given in parts of Part B of ANNEX II indicates the expected contents of the detailed requirements documents. The standards need to reflect the generally acknowledged state of art, and technical solutions to be proportionate to the risk that they aim to address.

The guidance relevant here to an assessment of a chip, system software or device, is summarized in section 7.3.1. Note that there is overlap in some of the requirements in clauses 2.1, 2.2 and 2.3 and that these clauses refer to [13] 3(3) points (d), (e) and (f) respectively [13]. Note also that the table excludes text from [14] in the identified clauses that concern generation of the specifications.

It is anticipated that the listed detailed requirements specifications will be adopted by the EU-CRA and compliance with the RED will be applicable only to the non-cyber-security parts. The timeframe is thought to be 2025.

7.3.1 Security Requirements

Scope	ANNEX II Part B Clause	Objective	Supported?		
			Yes	Part-ial	N/A
Authentication and access control	2.1 (c) 2.2 (b) 2.3 (b)	implement appropriate authentication and access control mechanisms;			
		(Describe how this requirement is met.)			
Attack Surfaces	2.1 (f) 2.2 (h) 2.3 (f)	protect the exposed attack surfaces and minimise the impact of successful attacks.			
		(Describe how this requirement is met.)			
Network Monitoring	2.1 (a)	include elements to monitor and control network traffic, including the transmission of outgoing data;			
		(Describe how this requirement is met.)			
DoS	2.1 (b)	are designed to mitigate the effects of ongoing denial of service attacks;			
		(Describe how this requirement is met.)			
Vulnerabilities at deployment	2.1 (d)	are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the network or its functioning or misuse of network resources;			
		(Describe how this requirement is met.)			
	2.2 (c)	are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Scope	ANNEX II Part B Clause	Objective	Supported?		
			Yes	Part-ial	N/A
		not contain publicly known exploitable vulnerabilities as regards data protection and privacy;			
		(Describe how this requirement is met.)			
	2.3 (c)	are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards financial or monetary data;			
		(Describe how this requirement is met.)			
Updates	2.1 (e)	are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to the radio equipment harming the network or its functioning or the misuse of network resources;			
		(Describe how this requirement is met.)			
	2.2 (d)	are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability of personal data;			
		(Describe how this requirement is met.)			
	2.3 (d)	are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability of financial or monetary data;			
		(Describe how this requirement is met.)			
Protection of data	2.2 (a)	protect stored, transmitted or otherwise processed personal data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability;			
		(Describe how this requirement is met.)			
	2.3 (a)	protect stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability;			
		(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Scope	ANNEX II Part B Clause	Objective	Supported?		
			Yes	Part-ial	N/A
Notification of changes	2.2 (e)	include functionalities to inform the user of changes that may affect data protection and privacy;			
		(Describe how this requirement is met.)			
Logging	2.2 (f)	log the internal activity that can have an impact on data protection or privacy;			
		(Describe how this requirement is met.)			
	2.3 (e)	log the internal activity that can have an impact on financial or monetary data			
		(Describe how this requirement is met.)			
Deletion of personal data	2.2 (g)	allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal data;			
		(Describe how this requirement is met.)			

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Appendix A 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, development and other best practices that contribute to comprehensive device security. These are collated from references ETSI 303645 [2], NIST8259A [3], SB-327 [4], UK DSIT [5], and Matter [6], and ioXt [7].

The 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 categorize the 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 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, enabling externally identified vulnerabilities to be reported.			
	(Optional notes)			
BP3.3 (Optional)	The Developer should explicitly state the minimum length of time for which the device will receive security updates or provide an expiration date after which security updates will not be issued.			
	(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 their vulnerability disclosure policy and response plan, which should be easily accessible from its website.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Best practice
BP2.2	The Developer should provide its public point of contact as part of its vulnerability disclosure policy, enabling externally identified vulnerabilities to be reported. See Appendix A.1.
BP2.3	The Developer should act in a timely manner after discovery of a vulnerability, provide security updates and make them available to affected devices.
BP2.4	The Developer should actively monitor for vulnerabilities likely to affect the security of its device and have a defined maintenance plan.
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 or provide an expiration date after which security updates will not be issued. 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 ensure 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.
BP4.4	The Developer should follow a secure management process for the generation and issuance of Critical Security Parameters.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

A.6 Installation, Commissioning and Reset

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.
BP5.3	If the device requires any user installation or commissioning operation then that mode should automatically end if not completed within a specific time, or after a specific number of failed attempts.
BP5.4	Information required for a user to install or commission a device should be hidden or removable from the device, or if performed electronically, for example over a wireless link, then that link must be protected in accordance with D2.4, to prevent an attacker performing an installation.
BP5.5	Initiation of user installation or commissioning should require physical proximity and action by the user, such as pressing a button, that cannot be achieved remotely.
BP5.6	Where a factory reset is supported, all local data, including any keys and personal data, created through use by the end user must be erased, unless explicitly required to persist.

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 their personal data.
BP6.4	The Developer should minimize and anonymize whenever possible the data collected from end-user logs.

A.8 Development

ID	Best practice
BP7.1	The Developer should make use of development tools, for example, static code analysis, as part of a Security Design Lifecycle.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ID	Best practice
BP7.2	The Developer should make use of available in-processor code hardening technologies that aim, for example, and not limited to; • provide protection against stack smashing or overflow attacks, • enhance control flow integrity making it difficult for an attacker to mount call/jump and return orientated programming attacks, • make it difficult for an attacker to gain or escalate privilege, • guard against memory safety violations, and so on.
BP7.3	The Developer should ensure that the manufacturing process correctly and completely establishes and confirms that all the required security related controls and configuration have been set and the correct Critical Security Parameters have been used.

A.9 Hardening

ID	Best practice
BP8.1	Battery powered devices should minimize the impact on battery life through excessive queries by rate limiting, possibly limiting the rate to zero, for periods of time.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 [2], 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 D4.6: 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: Authenticating parameter configuration	S6.1: Configuration D3.10: 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 unauthorized disclosure	S3.3: Secure protocols that do not leak
5.6-4: Software disable of debug interface	S4.2: Unneeded functionalities

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

ETSI EN 303 645 V2.1.0 (2020-04) Provisions	PSA Level 1 Requirements
5.11-1: User data erasure	S7.1: Erase user data
5.13-1: Input validation	S4.5: Data validation D3.8: Data validation

B.2 NISTIR 8259A

The following table considers the NIST cybersecurity baseline [3].

NISTIR 8259A Capabilities	PSA Level 1 Requirements
Device identification	C1.4 ID storage S2.1 Device ID D4.6 Identification
Device configuration	C2.3 Access control PSA-RoT S6.1 Configuration D3.10 Configuration
Data protection	C1.1 Isolation C1.3 Protecting critical security parameters C1.4 Secure storage C2.3 Authorised access to sensitive data C2.4 Cryptography S2.2 Secure storage S2.3 Cryptography S3.2 Secure communication S6.1 Configuration S7.1 Erase user data D2.3 Secure Communication D4.5 Secure Storage D5.1 Data erasure D5.2 Personal data

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

NISTIR 8259A Capabilities	PSA Level 1 Requirements
Logical access to interfaces	C2.3 Access control PSA-RoT S3.1 Connection authentication S3.2 Communication encryption S3.3 Secure protocols S4.2 Unneeded functionalities S4.5 Input validation S4.6 Privilege and access control S6.1 Configuration D2.1 No unused port D2.2 Communication authentication D2.3 Communication encryption D2.4 Secure protocols D3.1 Debug ports D3.3 Unneeded functionalities D3.7 Privilege and access control D3.9 Isolation mechanisms
Software and firmware update	C2.1 Firmware update C2.2 Rollback S1.1 System software update S1.2 Rollback S6.1 Configuration D1.2 Rollback
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 [4] 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.

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

(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

B.4 Matter

This appendix gives preliminary mappings to Matter [6] Security Requirements and Security Best Practice.

Matter Security Requirements		**PSA Level 1 Requirements**
Commissioning	13.3 a	BP5.3
	13.3 b	D4.2
	13.3 c	BP5.3
	13.3 d	C1.4, C1.5, S4.1, D4.1
	13.3 e	BP5.4
	13.3 f	BP5.4
	13.3 g	S6.1, D3.10
Factory Reset	13.4 a	BP5.6
	13.4 b	C1.3, S2.2, D5.1, BP5.6
Firmware	13.5 a	D1.2
	13.5 b	D1.2
	13.5 c	S4.5

Matter Security Best Practices		**PSA Level 1 Requirements**
Crypto	13.6.1 a	C1.1, C1.2, C1.3, C1.4, C2.3, C2.4
	13.6.1 b	C1.1, C1.2, C1.3, C1.4, C2.3, C2.4
	13.6.1 c	C1.1, C1.2, C1.3, C1.4, C2.3, C2.4
	13.6.1 d	C2.4
	13.6.1 e	D2.4
Commissioning	13.6.2 a	BP4.4
	13.6.2 b	BP5.4
	13.6.2 c	BP5.5
	13.6.2 d	BP5.4
	13.6.2 e	BP4.4

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Matter Security Best Practices		PSA Level 1 Requirements
	13.6.2 f	None
	13.6.2 g	Not applicable
Firmware	13.6.3 a	BP2.2
	13.6.3 b	D1.1
	13.6.3 c	BP4.4
Manufacturing	13.6.4 a	D1.1, D1.2, D2.1, D3.1, D3.3, BP7.3
Resiliency	13.6.5.a	C1.2, D1.1, D3.4
Battery devices	13.6.6 a	BP8.1
Tamper resistance	13.6.7 a	Influence which PSA Cert Level
Bridging	13.6.8	Not applicable
Distributed Compliance Register	13.6.9	Not applicable

B.5 ioXt

This appendix has not been updated in this version.

This appendix gives preliminary mappings to the ioXt Baseline Profile certifiable requirements [7].

ioXt Baseline Profile certifiable requirement		PSA Level 1 Requirements
No Universal Passwords	UP1	S5.1, S5.2
Secured Interfaces	SI1.1	S3.3
	SI1.2	S4.2, D2.1, D3.1, D3.3
	SI1.3	S3.1, D2.2, D2.4
	SI1.4	S3.2, S3.3, D2.2, D2.3, D2.4
Proven Crypto	PC1	C2.4, S2.3, S5.3
Verified Software	VS1	BP2.3
	VS2	C1.2 S1.1, D1.1, D1.2
	VS3	C2.4
Automatic Software Updates	AA1	C2.1, S1.1
	AA2	BP2.4
	AA3	BP2.3
Vulnerability Reporting	VDP1	BP2.1
	VDP2	BP2.2
Security Expiration Data	SE1.1	BP3.3
	SE1.2	BP3.2

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

Appendix C Changes Guide from V2.2 REL 01

This appendix lists the impact of changes between this revision and the V2.2 REL 01. Items marked “Unchanged” may include those with minor typographic corrections. Those marked “Clarification” aim to clarify the requirement through re-phrasing or the addition of supplementary information, but with no intended change to the requirement. Those marked “New” have been added in this version. Those marked “Extended” means that requirement has new elements that may be applicable.

L1 V3.0 ALPHA	Changes from v2.2 REL 1	
C1.1	Unchanged	
C1.2		Clarification
C1.3	Unchanged	
C1.4	Unchanged	Clarification
C1.5	New	
C2.1	Unchanged	
C2.2	Unchanged	
C2.3	Unchanged	
C2.4	Unchanged	

L1 V3.0 ALPHA	Changes from v2.2 REL 1	
S1.1	Unchanged	
S1.2	Unchanged	
S2.1		Extended
S2.2	Unchanged	
S2.3	Unchanged	
S3.1		Clarification
S3.2	Unchanged	
S3.3	Unchanged	
S4.1		Clarification
S4.2		Clarification
S4.3		Clarification
S4.4	Unchanged	
S4.5		Extended
S4.6	Unchanged	

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

S5.1	Unchanged	
S5.2	Unchanged	
S5.3	Unchanged	
S6.1	Unchanged	
S7.1	Unchanged	

L1 V3.0 ALPHA	Changes from v2.2 REL 1	
D1.1		Clarification
D1.2		Extended
D2.1	Unchanged	
D2.2		Clarification
D2.3		Extended
D2.4		Clarification
D3.1		Clarification
D3.2	Unchanged	
D3.3		Clarification
D3.4		Clarification
D3.5		Clarification
D3.6	Unchanged	
D3.7		New
D3.8		New
D3.9		New
D3.10		New
D4.1	Unchanged	
D4.2		Clarification
D4.3		Clarification
D4.4		Clarification
D4.5		Clarification
D4.6		New
D4.7		New
D5.1		Clarification
D5.2	Unchanged	

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

L1 V3.0 ALPHA	Changes from v2.2 REL 1	
BP1.1	Unchanged	
BP1.2	Unchanged	
BP2.1	Unchanged	
BP2.2	Unchanged	
BP2.3	Unchanged	
BP2.4	Unchanged	
BP2.5	Unchanged	
BP3.1	Unchanged	
BP3.2	Unchanged	
BP3.3	Unchanged	
BP4.1	Unchanged	
BP4.2	Unchanged	
BP4.3	Unchanged	
BP4.4	Unchanged	
BP5.1	Unchanged	
BP5.2	Unchanged	
BP5.3	Unchanged	
BP5.4	Unchanged	
BP5.5	Unchanged	
BP5.6	Unchanged	
BP6.1	Unchanged	
BP6.2	Unchanged	
BP6.3	Unchanged	
BP6.4	Unchanged	
BP7.1	Unchanged	
BP7.2	Unchanged	
BP7.3	Unchanged	
BP8.1	Unchanged	

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 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 v3.0	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 (Optional) 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 v3.0	Expected answer
C1.4 ID Storage	“Yes”

D.1.3 NISTIR 8259A Mapping

PSA Certified L1 v3.0	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”

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 v3.0	Expected answer
S1.1 Firmware update	“Yes”
S1.2 (Optional) Prevent rollback	Any Answer
S1.3 (Optional) Secure Boot of NSPE first stage	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 (Optional) Attestation method of lifecycle state	Any Answer
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 If supported, Lowest privilege necessary	“Yes” or “N/A”
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 v3.0	Expected answer
S1.1 Firmware update	“Yes”
S1.2 Prevent unauthorized rollback	“Yes”
S2.2 Secure Storage	“Yes”

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

PSA Certified L1 v3.0	Expected answer
S2.3 Best Practice Crypto	“Yes”
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” or “N/A”
S5.2 If Passwords, then best practice	“Yes” or “N/A”
S5.2 Passwords best practice	“Yes” or “N/A”
S5.3 User Auth	“Yes” or “N/A”
S6.1 Configuration	“Yes” or “N/A”
S7.1 Erase user data	“Yes” or “N/A”

D.2.3 NISTIR 8259A Mapping

PSA Certified L1 v3.0	Expected answer
S1.1 System software 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”
S4.6 Privilege access control	“Yes” or “N/A”
S5.2 Passwords best practice	“Yes” or “N/A”
S6.1 Security config changeable – auth first	“Yes” or “N/A”
S7.1 Personal data erasable /device reset	“Yes” or “N/A”

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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 v3.0	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 (Optional) Security lifecycle attestable	Any Answer
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”
D3.7 Lowest privilege	“Yes” or “N/A”
D3.8 Data Input	“Yes” or “N/A”
D3.9 Hardware based isolation	“Yes”
D3.10 Configuration	“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”
4.6 Configuration	“Yes”
D5.1 Restrict access to personal data/logs to auth users	“Yes” or “N/A”
D5.2 (Optional) Personal data stored on PSA-RoT secure storage	Any Answer

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

D.3.2 ETSI EN 303 645 v2.1.0 Mapping

PSA Certified L1 v3.0	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”
D4.2 Device uses password best practice	“Yes” or “N/A”
D4.3 Ability to disable passwords or apply time out after unsuccessful auth against a password	“Yes” or “N/A”

D.3.3 NISTIR 8259A Mapping

PSA Certified L1 v3.0	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 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” or “N/A”
D3.7 Privilege access control	“Yes” or “N/A”
D3.9 Isolation mechanisms	“Yes” or “N/A”
D3.10 Configuration	“Yes”
D5.1 Restrict access to personal data/logs to auth users	“Yes” or “N/A”
D4.6 Identification	“Yes
D5.2 (Optional) Personal data stored on PSA-RoT secure storage	“Yes” or “N/A”

D.3.4 SB-327 Mapping

PSA Certified L1 v3.0	Expected answer
D4.2 Device uses password best practice	“Yes”

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential

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?	
Draft EU-CRA (section 7.1) compliance?	
UK PTSI Act (section 7.2) compliant?	
Draft RED (section 7.3) compliance?	
ETSI EN 303 645 Chip section pass achieved?	
ETSI EN 303 645 System Software section pass achieved?	
ETSI EN 303 645 Device pass achieved?	
NISTIR 8259A Chip section pass achieved?	
NISTIR 8259A System Software section pass achieved?	
NISTIR 8259A Device section pass achieved?	
SB-327 mapping pass achieved?	

Copyright © 2017 – 2023 Arm Limited or its affiliates. All rights reserved.
Non-Confidential