SESIP Profile for PSA Certified™ RoT Component Level 3

Document number:	JSADEN018
Version:	1.0 REL
Release Number:	02
Author:	PSA JSA Members: Applus+ Laboratories Arm Limited CAICT 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:	PSA JSA Members
Date of Issue:	24/11/2022

© Copyright Arm Limited 2017-2022. All rights reserved.

Abstract

PSA Certified is the independent security evaluation scheme for Platform Security Architecture (PSA) based IoT systems. It establishes trust through a multi-level assurance program for chips containing a security component called a Root of Trust (PSA-RoT) that provides trusted functionality to the platform. The multi-level scheme has been designed to help device makers and businesses get the level of security they need for their use case.

PSA Certified Level 3 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against substantial physical and software attacks. The Level 3 documents include: a SESIP Profile that describes the Target of Evaluation, its assets, the security objectives and security functions that will be evaluated and an Attack Methods (AM) document describing the attacks in scope.

Developers submit their PSA-RoT to an approved test laboratory, listed on **www.psacertified.org**, for Level 3 evaluation and receive an Evaluation Technical Report. If the PSA-RoT is assessed as passing and approved by the independent Certification Body, a digital certificate will be issued on the PSA Certified website.

Keywords

PSA Certified Level 3, SESIP, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security

Copyright ©2017-2022 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 © 2022 Arm Limited (or its affiliates). All rights reserved.

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

Contents

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Released, version 1.0 REL 02.

1.2 Release Information

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

Date	Version	Confidentiality	Change
2022-10-10	1.0 REL 01	Non-confidential	Derived from [PSA-L2-Comp]
2022-11-24	1.0 REL 02	Non-confidential	+ Abstract

1.3 References

This document refers to the following documents.

1.3.1 Normative references

Ref	Doc No	Author(s)	Title
[PSA-L1]	JSADEN001	JSA	PSA Certified Level 1 Questionnaire
[PSA-EM-L2]	JSADEN003	JSA	PSA Certified: Evaluation Methodology for PSA L2
[PSA-EM-L3]	JSADEN010	JSA	PSA Certified: Evaluation Methodology for PSA L3
[PSA-AM]	JSADEN004	JSA	PSA Certified Attack Method
[PSA-PP-L2]	JSADEN002	JSA	PSA Certified Level 2 Lightweight Protection Profile
[PSA-PP-L3]	JSADEN009	JSA	PSA Certified Level 3 Lightweight Protection Profile
[SESIP-PP-L2]	JSADEN012	JSA	SESIP Profile for PSA Certified™ Level 2
[SESIP-PP-L3]	JSADEN011	JSA	SESIP Profile for PSA Certified™ Level 3
[PSA-L2-Comp]	JSADEN017	JSA	SESIP Profile for PSA Certified™ RoT Component Level 2
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.1
[CEM]	CCMB-2017-04-004	Common Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, revision 5, April 2017.

1.3.2 Informative references

Ref	Doc No	Author(s)	Title
[GP-ROT]	GP_REQ_025	GlobalPlatform	Root of Trust Definitions and Requirements, Version 1.1, Public Release, June 2018
[PSA-SM]	ARM DEN 0079	Arm	Platform Security Model v1.1

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations (see PSA-SM and PSA-L1).

Term	Meaning
Application	Used in this SESIP Profile to refer to the components which are out of the scope of the evaluation.
Application Root of Trust Service(s)	Application specific security service(s) that are not defined by PSA. Such services execute in the Secure Processing Environment and are required to be in Secure Partitions.
Application Specific Software	Software that provides the functionality required of the specific device. This software runs in the Non-Secure Processing Environment, making use of the System Software, Application RoT Services and PSA-RoT Services.
Critical Security Parameter	Secret information, with integrity and confidentiality requirements, used to maintain device security, such as authentication data (passwords, PIN, certificates), secret cryptographic keys, etc..
Evaluation Laboratory	Laboratory or facility that performs the technical review of questionnaires submitted for Level 1 PSA certification. The list of evaluation laboratories participating to PSA Certified can be found on www.psacertified.org
Hardware Unique Key (HUK)	Secret and unique to the device symmetric key that must not be accessible outside the PSA Root of Trust. It is a Critical Security Parameter.
Host Platform	Used in this SESIP Profile to refer to the entity which when used in composition with the platform form a PSA Level 2 certifiable PSA-RoT (including any PSA-RoT Services).
Initial Attestation Key (IAK)	A PSA-RoT secret private key from an asymmetric key-pair used to sign attestation reports, thus ensuring that the report is bound to a unique PSA-RoT (and so device) instance.
Non-secure Processing Environment (NSPE)	The processing environment that hosts the non-secure System Software and Application Specific Software. PSA requires the NSPE to be isolated from the SPE. Isolation between partitions within the NSPE is not required by PSA though is encouraged where supported.
Partition	The logical boundary of a software entity with intended interaction only via defined interfaces, but not necessarily isolated from software in other partitions. Note that both the NSPE and SPE may host partitions.
Platform	Used in this SESIP Profile to refer to the components which are in the scope of the evaluation.
PSA	Platform Security Architecture

Term	Meaning
PSA Certification Body	The entity that receives applications for PSA security certification, issues the certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories.
PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
PSA Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.
PSA Root of Trust (PSA-RoT)	The PSA defined combination of the Immutable Platform Root of Trust and the Updateable Platform Root of Trust and is considered to be the most trusted security component on the device. See [PSA-SM].
Immutable Platform Root of Trust	The minimal set of hardware, firmware, and data of the PSA-RoT, which is inherently trusted because it cannot be modified following manufacture. There is no software at a deeper level that can verify that it as authentic and unmodified.
Updateable Platform Root of Trust	The firmware, software and data of the PSA-RoT that can be securely updated following manufacture.
Platform Root of Trust Service(s)	PSA defined security services for use by PSA-RoT, Application RoT Service(s) and by the NSPE. Executes in the Secure Processing Environment and may use Trusted Subsystems. This includes the services offered by the PSA Functional APIs.
SESIP Profile	Document providing a common set of functionalities for similar products
Secure Partition	A Partition in the Secure Processing Environment.
Secure Processing Environment Partition Management	Management of the execution of software in Secure Partitions. Typical implementations will provide scheduling and inter partition communication mechanisms. Implementations may also enforce isolation between the managed Secure Partitions.
Secure Processing Environment (SPE)	The processing environment that hosts the PSA-RoT, and any Application RoT Service(s).
Secure Boot	The process of verifying and validating the integrity and authenticity of updateable firmware and software components as a pre-requisite to their execution. This must apply to all the firmware and software in the SPE. It should also apply to the first NSPE image loaded, which may extend the NSPE secure boot chain further.
Security Target (ST)	Document providing an implementation-dependant statement of security of a specific identified platform.
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.
TOE	Target of Evaluation. In this SESIP Profile it is a synonym for Platform.
Trusted subsystem	A security subsystem that the PSA-RoT relies on for protection of its assets, or that implement some of its services.

1.5 PSA Certified Level 3

PSA defines a common hardware and software security platform, providing a generic security foundation and allowing secure products and features to be developed on top of this platform.

The PSA Certified scheme involves the evaluation by a laboratory of a device against a set of security requirements and, in case of a successful evaluation, the certification by the PSA Certified certification body of this platform. The evaluation laboratory examines measures and processes to ensure that a functional platform is not vulnerable to the identified threats to the levels defined in this document.

The PSA programme recognises that there will be different security requirements and different cost/security trade-offs for different applications and eco-systems. This is reflected in specifications by introducing a range of assurance levels.

Two evaluation paths are currently possible for a PSA Certified Level 3 product, either through the PSA Certified Level 3 Protection Profile [PSA-PP-L3] and associated evaluation methodology [PSA-EM-L3], or through a SESIP evaluation using the SESIP Profile for PSA Certified Level 3 [SESIP-PP-L3].

1.5.1 PSA Certified Level 3 Root of Trust Component Certification

The PSA Certified scheme allows for certification of components that address a subset of the security functions required by an implementation for a Level 2 or Level 3 certifiable PSA Root-of-Trust (RoT). A typical example is an IP block that will be used in a chip. The IP could address a few security functions, with the rest of the chip covering all other requirements. Another example is an external chip that addresses a subset of the security functions, which when connected to another chip form a complete Level 2 or Level 3 certifiable PSA-RoT.

In PSA-SM such parts of a Level 2 or Level 3 certifiable chip are referred to as a Trusted Subsystem, which can be subject a Root-of-Trust Component (or RoT Component) certification. The intermediate step of certifying a RoT Component allows composite certification. This is especially beneficial as the RoT Component can be used in many chip products needing a Level 2 or Level 3 certified PSA-Root-of-Trust.

This component profile is based on the existing [SESIP-PP-L3]. The difference is that, where in [SESIP-PP-L3] all the SFRs that are required to meet PSA Certified requirements are mandatory, in this profile they are all optional. However, the SESIP process mandates that all Security Targets must include the “Verification of Platform Identity” SFR, and all must either include the “Secure Update of Platform” SFR or argue under ALC_FLR.2 why updates are not applicable [SESIP].

1.5.2 PSA Certified L2+SE Certification

A PSA L3 RoT Component may be used in composition for a PSA L2+SE RoT certification. In addition to the standard mandatory Security Functional Requirements, the following are also mandatory for L2+SE;

- 4.2.1 Verification of Platform Identity
- 4.2.2 Secure Update of Platform
- 4.3.3 Secure Initialization
- 4.3.6 Cryptographic Operation
- 4.3.7 Cryptographic Random Number Generation
- 4.3.9 Cryptographic KeyStore
- 4.4.1 Secure Communication Enforcement
- 4.4.2 Secure Communication Enforcement

Note that a PSA L3 RoT Component may be used to aid in the evaluation of an L3 PSA-RoT certification.

2 Introduction

This SESIP profile covers the platform types which implement a subset of the SFRs (Security Functional Requirements) described in [SESIP-PP-L3], with the goal of being re-used in a platform which targets conformance with [SESIP-PP-L3].

Due to the heterogeneity of the types of platforms that can claim conformance to this SESIP profile, no effort guideline is included for the AVA_VAN.2 activities as there is in [SESIP-PP-L3].

In this SESIP Profile the term Platform should be read as the PSA-RoT Component that implements the specific subset of SFRs described in any Security Target prepared against this profile. The Platform is intended to be used in composition with a Host Platform, which, in this SESIP Profile is referred to as the Application. Together, the Platform and the Application should form a PSA-RoT suitable for certification against [SESIP-PP-L2] or [SESIP-PP-L3].

For consistency, in the remainder of this document the term Platform refers to the PSA-RoT Component and the term Application refers to Host Platform.

Reading guide:

In the document there is guidance information aiming to facilitate reader understanding. This information can be easily identified as it is included in tables with a grey background:

REQ: guidance that must be considered and followed for the Security Target writing.

INFO: clarification to be considered.

2.1 SESIP Profile Reference

Reference	Value
PP Name	SESIP Profile for PSA Certified RoT Component Level 3
PP Version	See title page.
Assurance Claim	SESIP Assurance Level 3 (SESIP 3)
Optional and additional SFRs	*<TBD>*

Table 1: SESIP Profile Reference

2.2 Platform Reference

The platform is uniquely identified by its hardware and/or software references, depending on the platform type.

Reference	Value	
Platform Name	*<TBD>*	
Platform Version	*<TBD>*	
Platform Identification	*<TBD hardware>*	
	<TBD software>	
Platform type	*<TBD>*	

Table 2: Platform Reference

2.3 Included Guidance Documents

The following documents are included with the platform:

Reference	Name	Version
<[Ref1]>	*<Full title of the document>*	*<Vx.y>*

Table 3: Guidance Documents

REQ	The guidance must list all the documents that will be provided to the evaluator for the documentation review, covering AGD_OPE.1 and AGD_PRE.1. This documentation is expected to be available to the customers without restrictions.
REQ	Detailed integration guidance must be part of the platform, for the platform types targeted by this SESIP profile.

2.4 Platform Functional Overview and Description

2.4.1 Platform Type

<The developer must choose an appropriate platform type.>

Some examples include:

- A cryptographic engine.
- A software cryptographic library.
- A storage peripheral.
- A Secure Element.
- A Trusted Platform Module.
- A Security Coprocessor.

INFO	The developer must fill this section based on the evaluated platform.

2.4.2 Physical Scope

The platform consists of a combination of software, hardware, and guidance documents:

<The developer must describe the delivery method for each of the platform parts listed above.>

REQ	The parts comprising the platform must be defined here. Note that the content of this section will depend on the physical scope of the platform. For example, the platform can be defined as software only or Verilog RTL description.

2.4.3 Usage and Major Security Features

The platform supports the following major security features:

<complete this section with the major security features of the platform on a high level >

2.4.4 Required Hardware/Software/Firmware

<clarify if the platform is supplied with existing apps, Application Root of Trust Services, or other components>

3 Security Objectives for the operational environment

For the platform to fulfil its security requirements, the operational environment (technical or procedural) must fulfil the following objectives.

ID	Description	Reference
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	*<[Ref1]> Section X*
TRUSTED_USERS	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	*<[Ref1]> Section X*
UNIQUE_ID	The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage.	*<[Ref1]> Section X*
<TBD>	*<TBD>*	*<TBD>*

Table 4: Security Objectives for the Operational Environment

INFO	Some examples of objectives are listed, adjust as applicable.
REQ	The guidance must list all the documents that will be provided to the evaluator for the documentation review, covering AGD_OPE.1 and AGD_PRE.1. This documentation must be available to the customers.
REQ	The integrity and uniqueness of the unique identification of the platform should be supported by the development, production, and test environment. Otherwise, if the integrity and uniqueness of the unique identification is responsibility of the platform user, then the objective for the environment UNIQUE_ID must be defined.

4 Security Requirements and Implementation

4.1 Security Assurance Requirements

The claimed assurance requirements package is SESIP3 as described in Section 5.1.

4.1.1 Flaw Reporting Procedure (ALC_FLR.2)

In accordance with the requirement for a flaw reporting procedure (ALC_FLR.2), including a process to report a flaw and generate any needed update and distribute it, the developer has defined the following procedure:

<Describe the procedure, including where flaws can be reported (website and/or email address), how the reported flaws are handled in a timely manner, and how an application developer/end-user is informed of the update.>

4.2 Base PP Security Functional Requirements

As a base, the platform fulfils the following security functional requirements:

INFO	The “Verification of Platform Identity” and the “Secure Update of Platform” requirements are explicitly listed here, because they are mandatory in all SESIP Security Targets. Additional SFRs are then added to suit vendor objectives.
REQ	The “Physical Attacker Resistance” (4.2.3) requirement is mandatory in [PSA-PP-L3], and therefore, considered mandatory in this document.
REQ	For every SFR, a description of the implementation in the Platform needs to be included.
INFO	The SFRs listed in this section relate to the platform. In general, fulfilling an SFR in a PSA-RoT Component certification does not automatically mean that the same SFR is fulfilled when in composition for a Level 2 or Level 3 PSA-RoT certification. This is because the term Platform in a component certification very likely has a different scope to the term Platform in a Level 2 or Level 3 PSA-RoT certification.

4.2.1 Verification of Platform Identity

The platform provides a unique identification of the platform, including all its parts and their versions.

INFO	This requirement is mandatory according to [SESIP].

4.2.2 Secure Update of Platform

The platform can be updated to a newer version in the field such that the integrity, authenticity, and confidentiality of the platform is maintained.

REQ	This SFR is only applicable to the updatable parts of the platform. If the platform cannot be updated, under ALC_FLR.2 it shall be argued why updates are not applicable.
REQ	The user guidance shall describe the secure anti-rollback policies that are enforced by the platform. A device must only install software updates of newer versions than the current version on the device.

4.2.3 Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises any of the other functional requirements.

4.3 SFRs for PSA-RoT Component

INFO	The SFRs listed in this section are mandatory for a PSA-RoT L3 certification following [SESIP-PP-L3]. However, in a PSA-RoT Component certification only a subset of PSA-RoT SFRs can be claimed.
REQ	Developer must implement at least one SFR from the list in this section to qualify for claiming conformance with this Profile.
REQ	Any use of cryptography, random numbers, key generation, and key storage that is for use solely within the component, i.e., not available to the application (so not declared in sections 4.3.6 to 4.3.9), must be detailed in every applicable SFR.
INFO	The SFRs listed in this section relate to the PSA-RoT Component. In general, fulfilling an SFR in a Component certification does not automatically mean that the same SFR is fulfilled when in composition for a Level 2 or Level 3 PSA-RoT certification. This is because the term Platform in a PSA-RoT Component certification has a different scope to the term Platform in a PSA-RoT Level 2 and Level 3 certification.

4.3.1 Verification of Platform Instance Identity

The platform provides a unique identification of that specific instantiation of the platform, including all its parts and their versions.

4.3.2 Attestation of Platform Genuineness

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that ensures that the platform cannot be cloned or changed without detection.

REQ	When the platform supports this function, the platform vendor must describe how attestation is performed and what information is used and exchanged with the Application.

4.3.3 Secure Initialization of Platform

The platform ensures its authenticity and integrity during platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will go to **a state where no other operation except optionally Secure Update of Platform (section 4.2.2) can be performed**.

REQ	If the initialization fails, restarts or at most recovery using the update mechanism may be performed. All other functionality must not be available. The application may be used to facilitate this update but must not provide any other functionality until the authenticity and integrity of the platform is re-established. Any guidance for the application on this must be explicitly mentioned as a Security Objectives for the operational environment, with explicit reference to where this guidance is provided.

4.3.4 Attestation of Platform State

The platform provides an attestation of the state of the platform, such that it can be determined that the platform is in a known state.

4.3.5 Software Attacker Resistance: Isolation of Platform

The platform provides isolation between the application and itself, such that an attacker able to run code as an application on the platform cannot compromise the other functional requirements.

INFO	This SFR aims to cover the case where the platform can play a part in implementing the isolation between the SPE and NSPE, and between the PSA-RoT and any Application RoT Services. For example, if the platform is implemented in a Secure Element device, then an attacker able to run code outside of the PSA-RoT, whether on the host MCU or the Secure Element itself, cannot compromise the platform security functionality implemented in the Secure Element.
REQ	Provision of isolation mechanisms in the device that implements the platform does not guarantee that they will be used when combined with the Host Platform. The developer should describe what mechanisms are available, if any, and how they may be used to support isolation of PSA-RoT functionality from the NSPE and Application RoT Services in accordance with the isolation types defined in [SESIP-PP-L3]. See also section 4.5.2.
INFO	This SFR can be iterated in case that the platform implements different isolation mechanisms.

4.3.6 Cryptographic Operation

The platform provides the application with Operations in Table 5 functionality with algorithms in Table 5 as specified in specifications in Table 5 for key lengths described in Table 5 and modes described in Table 5.

Algorithm	**Operations**	**Specification**	**Key lengths**	**Modes**
<TBD>	*<TBD>*	*<TBD>*	*<TBD>*	*<TBD>*
<TBD>	*<TBD>*	*<TBD>*	*<TBD>*	*<TBD>*

Table 5: Cryptographic Operations

INFO	This SFR addresses the algorithms available to the application. In other words, for use under composition by the PSA-RoT, any Application RoT Services, or by the NSPE.
REQ	When the platform supports this function, the platform vendor must describe how it is performed and what information is used and exchanged with the application.
REQ	PSA requires equivalence of at least 128-bit security level.

4.3.7 Cryptographic Random Number Generation

The platform provides the application with a way based on *<list of entropy sources>* to generate random numbers to as specified in *<specification>*.

INFO	This SFR addresses the RNG functionality available to the application. In other words, for use under composition by the PSA-RoT, any Application RoT Services, or by the NSPE.

4.3.8 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in cryptographic operations in Table 6 as specified in specifications in Table 6 for key lengths described in Table 6.

ID	Algorithm	Specification	Key lengths
<TBD>	*<TBD>*	*<TBD>*	*<TBD>*
<TBD>	*<TBD>*	*<TBD>*	*<TBD>*

Table 6: Cryptographic Key Generation

REQ	This SFR addresses the key generation algorithms available to the application. In other words, for use under composition by the PSA-RoT, any Application RoT Services, or by the NSPE.
REQ	PSA requires equivalence of at least 128-bit security.

4.3.9 Cryptographic KeyStore

The platform provides the application with a way to store *<list of assets, such as cryptographic keys and passwords>* such that not even the application can compromise the *<selection: authenticity, integrity, confidentiality>* of this data. This data can be used for the cryptographic operations *<list of operations>*.

REQ	This SFR addresses all the cryptographic key storage functionality available to the application, in other words, for use under composition by the PSA-RoT, any Application RoT Services, or by the NSPE.
REQ	PSA requires equivalence of at least 128-bit security.

4.4 Additional Security Functional Requirements

<complete this section with the additional SFRs defined in [SESIP].>

INFO	This section allows inclusion of SESIP SFRs which are part of the SESIP catalogue from [SESIP] but not defined in [PSA-PP-L2] or [SESIP-PP-L3].
REQ	In case the platform is a Trusted Subsystem is used to create the PSA-RoT, the SFRs defined in Section 4.4.1 (Secure Communication Support) and Section 4.4.2 (Secure Communication Enforcement) are mandatory.
REQ	Additional SFRs not defined in [PSA-PP-L2] or [SESIP-PP-L3] can be added under two specific conditions: - They must not affect any of the SFRs defined in [PSA-PP-L2] or [PSA-PP-L3]. This must be assessed by the Security Evaluation Laboratory. - They will not be recognised by the PSA RoT Component program since this additional functionality is not mapped to any SFR(s) defined in [PSA-PP-L2] or [PSA-PP-L3]. However, in the scope of a SESIP evaluation they will be recognised.
REQ	Any use of cryptography, random numbers, key generation, and key storage that is for use solely within the component, i.e., not available to the application (so not declared in sections 4.3.6 to 4.3.9), must be detailed in every applicable SFR.

4.4.1 Secure Communication Support

The platform provides the application with one or more secure communication channel(s).

The secure communication channel authenticates *<list of endpoints>* and protects against *<list of attacks including disclosure, modification, replay, erasure>* of messages between the endpoints, using *<list of protocols and measures>*.

INFO	A Trusted Subsystem used in the implementation of a PSA-RoT is an example of a PSA certifiable RoT Component. Therefore, a Trusted Subsystem is the platform, which is connected to the application (the Host Platform) in composition.
INFO	A Trusted Subsystem may comprise both hardware and software elements.
INFO	This SFR is mandatory in [SESIP-PP-L3] when a Trusted Subsystem is used to create the PSA-RoT. Therefore, it is likely that this SFR is in effect mandatory in this Protection Profile.
REQ	The developer must describe the mechanism that is used to protect in confidentiality and integrity the communication between the platform and the application and must include the appropriate SFRs to cover the Trusted Subsystem functionality.
REQ	Level 2 + SE requires the link between the platform and the application to be protected to prevent attacks such as probing to reveal secrets. Typically, this means use of cryptography where the link is easily accessible, for example, on a PCB trace or a physical pin of a device. An on-chip Trusted Subsystem must be shown to be accessible only by the SPE.
INFO	If the platform provides multiple different secure channels, thus SFR should be iterated for each channel type.

4.4.2 Secure Communication Enforcement

The platform ensures that the application can only communicate with **trusted subsystems** over the secure communication channel(s) supported by the platform using *<list of protocols and measures>*.

REQ	Level 2 + SE requires a protected link between a Trusted Subsystem and the remainder of the SPE to prevent basic attacks such as probing the PCB to reveal secrets. An on-chip Trusted Subsystem must be shown to be accessible only by the SPE.
INFO	This SFR is mandatory in [SESIP-PP-L3] when a Trusted Subsystem is used to create the PSA-RoT. Therefore, it is likely that this SFR is in effect mandatory in this Protection Profile.
INFO	The ST must include an iteration of Secure Communication Support for each secure channel type referenced in this SFR.

4.5 Optional Security Functional Requirements

INFO	The SFRs listed in this section are optional for a PSA-RoT L3 certification following [SESIP-PP-L3]. In case of a PSA-RoT Component certification a claim for any of these only supports an PSA-RoT certification if that certification also makes the claim.
INFO	The SFRs listed in this section relate to the PSA-RoT Component. In general, fulfilling an SFR in a Component certification does not automatically mean that the same SFR is fulfilled when in composition for a Level 2 or Level 3 PSA-RoT certification. This is because the term Platform in a PSA-RoT Component certification has a different scope to the term Platform in a PSA-RoT Level 2 and Level 3 certification.
REQ	Any use of cryptography, random numbers, key generation, and key storage that is for use solely within the component, i.e., not available to the application (so not declared in sections 4.3.6 to 4.3.9) must be detailed in every applicable SFR.

4.5.1 Audit Log Generation and Storage

The platform generates and maintains an audit log of *<list of significant security events>* and allows access and analysis of these logs following a specific *<access control policy>*.

INFO	The developer can choose whether to implement this functionality and claim the SFR or not to implement it and not claim the SFR.

4.5.2 Software Attacker Resistance: Isolation of Application Parts

The platform provides isolation between parts of the application, such that an attacker able to run code as one of the *<list of application parts>* cannot compromise the integrity and confidentiality of the other application parts.

INFO	This SFR covers additional isolation boundaries between each of the Application RoT services.
REQ	Provision of isolation mechanisms in the device that implements the platform does not guarantee that they will be used when combined with the Host Platform. The developer should describe what mechanisms are available, if any, and how they may be used to support ARoT-ARoT isolation in accordance with the isolation types defined in [SESIP-PP-L3]. See also section 4.3.5.

4.5.3 Secure Debugging

The platform only provides *<list of endpoints>* authenticated as specified in *<specification>* with debug functionality.

The platform ensures that all data stored by the application, with the exception of *<list of exceptions>*, is made unavailable.

REQ	If the platform implements secure debugging, this SFR must be included in the ST as it addresses the authenticated access to the platform debug functionality. However, in case that debug features are deactivated prior to the final product is delivered to the end-user, this SFR does not need to be claimed.

4.5.4 Secure Encrypted Storage

The platform ensures that all data stored by the application, except for *<list of data stored in plaintext>*, is encrypted as specified in *<specification>* with a platform instance unique key of key length *<key length>*.

REQ	Secure encrypted storage requires confidentiality and integrity.
INFO	This SFR covers the encrypted internal storage functionality available to the application, in other words, for use under composition by the PSA-RoT, any Application RoT Services, or by the NSPE.
INFO	The scope is all data stored in encrypted form in all physical memory included in the platform.
REQ	When the platform supports this function, the platform vendor must describe how it is performed and what information is used and exchanged with the Application.

4.5.5 Secure Storage

The platform ensures that all data stored by the application, except for *<list of data stored in plaintext>*, is protected to ensure its authenticity and integrity as specified in *<specification>* with a platform instance unique key of key length *<key length>*.

INFO	This SFR covers the internal storage functionality available to the application, in other words, for use under composition by the PSA-RoT, any Application RoT Services, or by the NSPE.
INFO	Secure storage requires authenticity and integrity (confidentiality not required).
INFO	The scope is all data stored in any memory included in the scope of the evaluation.
REQ	When the platform supports this function, the platform vendor must describe how it is performed and what information is used and exchanged with the Application.

4.5.6 Secure External Storage

The platform ensures that all data stored outside the direct control of the platform, except for *<list of data stored outside the direct control of the platform>*, is protected such that the **authenticity, integrity, confidentiality** *<selection: and binding to the platform instance, versioning>* is ensured.

INFO	This SFR must be claimed if the platform data is stored in an external memory out of the scope of the evaluation.
INFO	If the platform relies on data stored in Secure External Storage, it is likely that Secure Encrypted Storage or Secure Storage will be necessary to implement the protection of the stored data.

5 Mapping and Sufficiency Rationales

5.1 Assurance

The assurance activities defined in [PSA-EM-L3] fulfil the SESIP3 activities. In particular, the required source code review, vulnerability analysis and testing of the [PSA-EM-L3] is applicable.

REQ This section must be completed by the ST writer.

Assurance Class	**Assurance Family**	**Covered by**
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	*<Section "Introduction" and title page of the Security Target>*
	Rationale:	
	ASE_OBJ.1 Security requirements for the operational environment	*<Section "Security Objectives for the Operational Environment" of the Security Target>*
	Rationale:	
	ASE_REQ.3 Listed Security requirements	*<Section "Security Requirements and Implementation" of the Security Target>*
	Rationale:	
	ASE_TSS.1 TOE Summary Specification	*<Section "Security Requirements and Implementation" of the Security Target>*
	Rationale:	
ADV: Development	ADV_FSP.4 Complete functional specification	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
	AGD_PRE.1 Preparative procedures	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	

ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
	ALC_CMS.1 TOE CM Coverage	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
	ALC_FLR.2 Flaw reporting procedures	*<ALC_FLR section in the Security Target and description of which developer evidence is used to meet this requirement>*
	Rationale:	
ATE: Tests	ATE_IND.1 Independent testing: conformance	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis	Vulnerability and testing carried out by the laboratory
	Rationale:	

Table 7 : Assurance Mapping and Sufficiency Rationales

5.2 PSA Security Functions Mapping

INFO	This section shows the platform mapping to the PSA Security Functions in [PSA-PP-L3]. For example, a platform implementing a cryptographic library running on a specific hardware the table would be filled as: PSA Functionality: F.CRYPTO Covered by SESIP SFR: Cryptographic Operation

PSA Security Function	Covered by SESIP SFR
F.INITIALIZATION	Secure Initialization
F.SOFTWARE_ ISOLATION	Software Attacker Resistance: Isolation of Platform
	Software Attacker Resistance: Isolation of Application Parts
F.SECURE_ STORAGE	Secure Encrypted Storage
	Secure Storage
	Secure Encrypted Storage
	Secure External Storage
F.FIRMWARE_ UPDATE	Secure Update of Platform
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform
	Software Attacker Resistance: Isolation of Platform
	Secure Initialization
	Secure Update of Platform
F.CRYPTO	Cryptographic Operation
	Cryptographic KeyStore
	Cryptographic Random Number
	Cryptographic Key Generation
F.ATTESTATION	Verification of Platform Identity
	Verification of Platform Instance Identity
	Attestation of Platform Genuineness
	Attestation of Platform State
F.AUDIT	Audit Log Generation and Storage
F.DEBUG	Secure Debugging
F.PHYSICAL	Physical Attacker Resistance
Additional security functionality	Secure Communication Support
	Secure Communication Enforcement

Table 8 Functionality Mapping and Sufficiency Rationales