SESIP Profile for PSA Certified™ Level 4 iSE/SE and RoT Component

psacertified™

psacertified™
level four RoT component

psacertified™
level four iSE/SE

Document number:	JSADEN023
Version:	2.0 BETA
Release Number:	03
Authors:	PSA JSA Members: Applus+ Laboratories Arm Limited CAICT DEKRA Testing and Certification ECSEC Laboratory Inc Institute for Information Industry ProvenRun 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:	09/07/2024

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. An overview of SESIP Profiles important to the PSA Certified scheme is given in Figure 1 that shows how this document relates to others for the chip's Root of Trust.

PSA Certified Level 4 iSE/SE is a fixed time, test laboratory based, evaluation of a PSA-RoT's Trusted Subsystem. It is aimed at IoT devices that need to protect against physical and software attacks with attacker potential in the range 0-24 (equivalent to JIL Moderate). A PSA Certified Level 4 iSE/SE Trusted Subsystem must meet a mandatory set of Security Functional Requirements (SFRs). Where this condition is not met, this document can alternatively be used for a PSA Certified Level 4 RoT Component certification.

Developers submit their PSA-RoT to an approved test laboratory, listed on **www.psacertified.org**, for Level 4 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 4 iSE/SE, SESIP, Certification, IoT, Platform Security Architecture, Questionnaire, PSA, Security, PSA Certified RoT Component

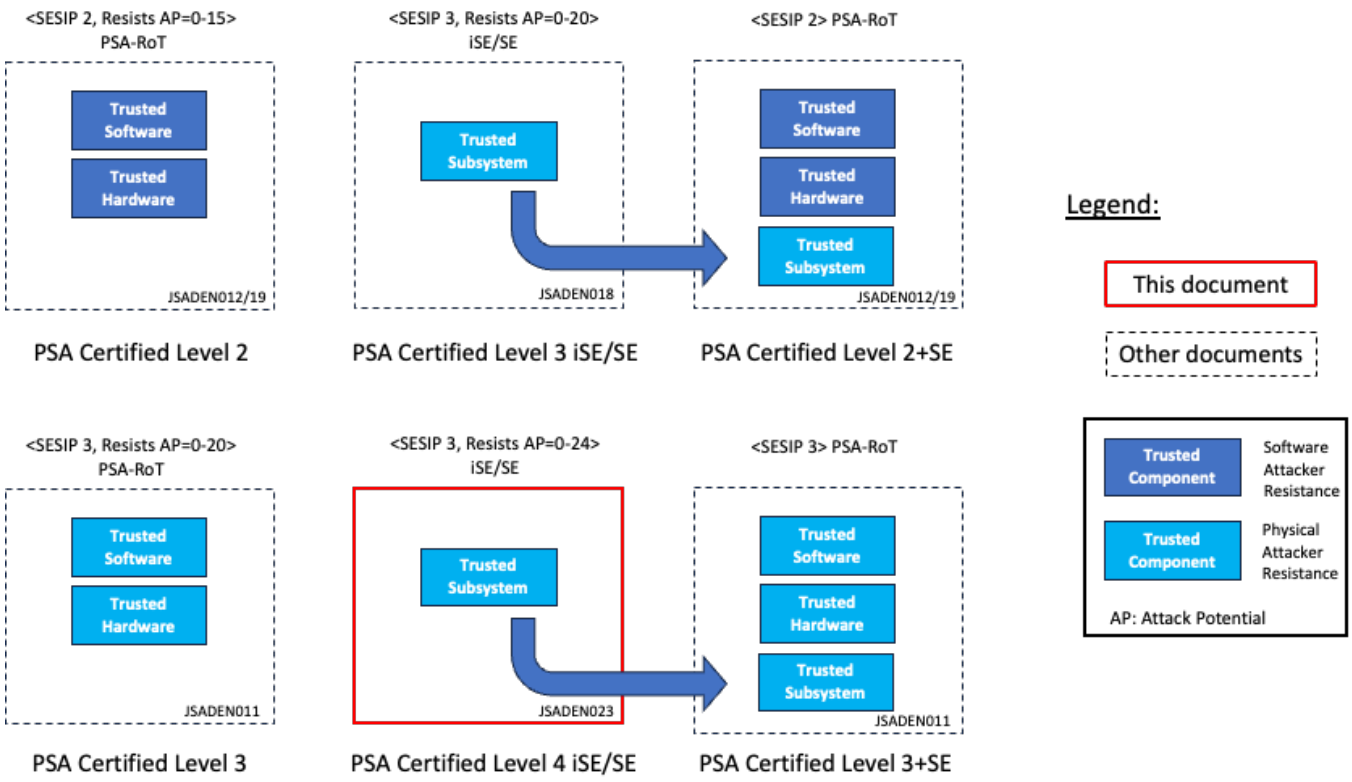

Figure 1: PSA Certified SESIP Profiles for the chip's RoT

Non-Confidential Proprietary Notice

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

Contents

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Released, version 2.0 BETA 03

1.2 Release Information

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

Date	Version	Confidentiality	Change
2024-03-05	2.0 BETA 01	Non-confidential	Derived from [PSA-L3-Comp], v2.0 to align with SESIP v1.2 docs
2024-03-22	2.0 BETA 02	Non-confidential	Improvements to section 1.5
2024-07-09	2.0 BETA 03	Non-confidential	Clarification to section 1.5.3

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 Methods
[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
[PSA-L3-Comp]	JSADEN018	JSA	SESIP Profile for PSA Certified™ RoT Component Level 3
[GP-SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.2
[CEN-SESIP]	EN 17927	CEN/CENELEC	Security Evaluation Standard for IoT Platforms (SESIP) 2023
[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]	JSADEN014	ARM	Platform Security Model
[PSA-SS]	IHI 0087	ARM	PSA Certified Secure Storage API, Version 1.0 or later
[SP-800-57]	SP 800-57 Part 1	NIST	Recommendation for Key Management: Part 1 – General, Rev. 5

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 assessment of products submitted for PSA Certified. 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 3 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
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.

Term	Meaning
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-dependent 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

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.

This SESIP Profile considers two scopes for evaluation, both a subset of a PSA Root-of-Trust and typically form a Trusted Subsystem.

1) Integrated Secure Enclave (iSE) or external Secure Element (SE) or
2) Root of Trust Components.

The security assurance for PSA Certified Level 4 iSE/SE and RoT Component is SESIP3 augmented with AVA_VAN.4, to protect against physical and software attacks with an attack potential rating of 0 – 24 inclusive (corresponding to JIL moderate, as in AVA_VAN.4).

Security Assurance Requirements (SAR) dependencies of AVA_VAN.4, such as ADV_ARC.1 or ATE_DPT.1, are not considered for PSA Certified Level 4 iSE/SE or PSA Certified Level 4 RoT Component evaluation. The evaluator will follow the SESIP3 evaluation methodology and consider the need of additional resistance for the SFRs.

From the certification standpoint, products that pass evaluation will receive a PSA Certified Level 4 RoT Component or a PSA Certified Level 4 iSE/SE certificate.

The SESIP standard associated with this document is defined either by GlobalPlatform [GP-SESIP] or by CEN/CENELEC [CEN-SESIP].

1.5.1 PSA Certified Level 4 iSE/SE Certification

The scope of the PSA Certified Level 4 iSE/SE is an integrated Secure Enclave or external Secure Element. In the context of the PSA Certified scheme and when a standalone PSA-RoT cannot provide this level of protection for all its security functions, these iSE/SE are used as a Trusted Subsystem for the implementation of a PSA-RoT and provide the targeted protection for the most critical assets of the PSA-RoT.

Table 1 summarizes applicable SFRs for PSA Certified L4 iSE/SE certification. A PSA Certified Level 4 iSE/SE is mandatory to achieve a Level 3+SE certification.

A PSA Certified Level 4 RoT Component may be used to aid in the evaluation of a Level 3 certification.

The Developer can obtain the rights to use the specific “PSA Certified Level 4 iSE/SE” logo and showcase the solution on **www.psacertified.org** when the above SFRs have been certified by the CB under this SESIP Profile.

1.5.2 PSA Certified Level 4 Root of Trust Component Certification

The PSA Certified Level 4 RoT Component 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 Security Model [PSA-SM], such parts of a Level 2 or Level 3 certifiable chip are referred to as a Trusted Subsystem, which can be subject to 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 most of them all optional. Table 1 summarizes applicable SFRs for PSA Certified RoT Component certification.

The Developer can obtain the rights to use the specific "PSA Certified Level 4 RoT Component" logo and showcase the solution on **www.psacertified.org** when the SFRs have been certified by the CB under this SESIP Profile.

1.5.3 SFRs for iSE/SE and RoT Components

The following table summarizes which of the SFRs from Section 4 are mandatory or optional for inclusion to a Security Target for an iSE/SE or a RoT component.

SFRs	Inclusion in Security Target for iSE/SE	Inclusion in Security Target for RoT Component
Verification of Platform Identity	Mandatory	Mandatory
Verification of Platform Instance Identity	Optional	Optional (2)
Attestation of Platform Genuineness	Optional	Optional (2)
Secure Initialization of Platform	Mandatory	Optional (2)
Attestation of Platform State	Optional	Optional (2)
Secure Update of Platform	Mandatory	Mandatory (3)
Physical Attacker Resistance	Mandatory	Mandatory
Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Optional	Optional
Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Optional	Optional
Cryptographic Operation	Mandatory	Optional (2)
Cryptographic Random Number Generation	Mandatory	Optional (2)
Cryptographic Key Generation	Mandatory	Optional (2)
Cryptographic KeyStore	Mandatory	Optional (2)
Secure Communication Support	Optional (1)	Optional
Audit Log Generation and Storage	Optional	Optional
Software Attacker Resistance: Isolation of Application Parts	Optional	Optional

Secure Debugging	Optional	Optional
Secure Encrypted Storage	Optional	Optional
Secure Confidential Storage	Optional	Optional
Secure Trusted Storage	Optional	Optional
Secure Data Serialization	Optional	Optional

Table 1: Mandatory SFRs for iSE/SE and RoT Component

The Secure Communication Support SFR marked with (1) must be included in the security target if the iSE/SE includes mechanisms to protect the communication between the Host Platform and the iSE/SE. Though the use of cryptography is typical, the effectiveness of the included mechanism will be part of the iSE/SE evaluation. The correct use of the iSE/SE mechanism by a PSA RoT will be in the scope of the PSA RoT certification.

Where the iSE/SE does not implement any mechanism, the Secure Communication Support SFR (1) must not be included in the security target. However, the means used by a PSA RoT to protect the communication to an iSE/SE will be in the scope of the PSA RoT certification.

For RoT Component, at least one of the optional SFR marked with (2) must be included in the security target besides the mandatory SFRs. If the RoT component cannot support the mandatory SESIP SFR Secure Update of Platform (3), the security target shall provide a rationale for exclusion.

2 Introduction

This SESIP profile covers the platform types which implement a subset of the SFRs (Security Functional Requirements) described in [SESIP-PP-L2] or [SESIP-PP-L3], with the goal of being re-used in a platform which targets conformance with [SESIP-PP-L2] or [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.4 activities.

In this SESIP Profile the term Platform should be read as the iSE/SE or 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 shall 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 Level 4 iSE/SE or RoT Component
PP Version	See title page.
Assurance Claim	SESIP Assurance Level 3 (SESIP3)
SESIP Standard	*<[GP-SESIP] or [CEN-SESIP]>*
Optional and additional SFRs	*<TBD>*

Table 2: SESIP Profile Reference

2.2 Platform Reference

The platform is uniquely identified by its chip (hardware) reference and its PSA defined Root of Trust (software) reference as described below. The developer declares that only the evaluated and successfully certified products identify in this way.

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

Table 3: 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 4: Guidance Documents

REQ	The guidance shall 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.

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 Enclave or Secure Element.
- A Trusted Platform Module.
- A Security Coprocessor.

REQ	The developer shall 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 5: Security Objectives for the Operational Environment

INFO	Some examples of objectives are listed, adjust as applicable.
REQ	The guidance shall 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 shall 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 shall be defined.

4 Security Requirements and Implementation

4.1 Security Assurance Requirements

The SESIP claimed assurance requirements package is **SESIP3** augmented with AVA_VAN.4 security assurance component, 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 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:

REQ	For every SFR, a description of the implementation in the platform needs to be included.
INFO	Statement of the SFRs uses **bold text** to identify places where fields with angle brackets (<>) in the SESIP catalog have been filled with specificities of the platform considered in this Profile.
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.
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.

4.2.1 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 Verification of Platform Instance Identity

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

4.2.3 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.

4.2.4 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the 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 4.2.6) can be performed**.

REQ	If the initialization fails, restarts or at most recovery using the update mechanism may be performed. All other functionalities 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.

4.2.5 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.

4.2.6 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.

4.2.7 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.

INFO	In this Profile, the considered attack potential is resistance 0-24 (AVA_VAN.4 and JIL Moderate). It applies to all SFRs.

4.2.8 Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)

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	The PSA-RoT PP [SESIP-PP-L3] requires SPE/NSPE isolation. However, that does not mandate that an iSE/SE or RoT Component also support the isolation required by this SFR.
INFO	Where this SFR is not supported, then there are use case restrictions, see below.
INFO	Where this SFR is supported, the lab must include additional assessment to time.
INFO	This SFR applies to isolation of the platform (i.e. the Secure Enclave/Element) from the Host Platform or any other device with access (e.g. another MCU).

INFO	If the platform also provides internal isolation, this SFR also applies to those isolation mechanisms. This permits the case where the platform is used to host SPE and any NSPE operations. Where no such internal isolation is provided then the platform cannot be used to host any NSPE processing.
INFO	Because the platform implements PSA-RoT functionality within the SPE, then it is essential that an attacker able to run code outside of the SPE, whether on the platform itself, or on the Host Platform, cannot compromise the security functionality implemented in the SPE on the platform.
REQ	Provision of isolation mechanisms of the platform, or within the platform, does not guarantee that they will be used when integrated with the Host Platform. The developer must describe what mechanisms are available, if any, and how they may be used to support isolation of SPE functionality from the NSPE in accordance with the isolation types defined in [SESIP-PP-L3].
REQ	If isolation of the platform relies on integration rules of the iSE/SE to the device, such as the presence of a TrustZone aware controller for the iSE/SE, then the user guidance shall provide this information.
INFO	This SFR can be iterated in case that the platform implements different isolation mechanisms.

4.2.9 Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)

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	The PSA-RoT PP [SESIP-PP-L3] requires SPE/NSPE isolation. However, that does not mandate that an iSE/SE or RoT Component also support the isolation required by this SFR.
INFO	Where this SFR is not supported, then there are use case restrictions, see below.
INFO	Where this SFR is supported, the lab must include additional assessment to time.
INFO	This SFR applies to isolation between the PSA Root of Trust and any Application Root of Trust Services on the platform itself (e.g. the Secure Enclave/Element).
INFO	If the platform provides internal isolation, the SFR applies to those internal isolation mechanisms. This permits the case where the platform is used to host PSA-RoT and any Application RoT services. Where no such internal isolation is provided then the platform cannot be used to host both PSA-RoT and Application RoT services.
INFO	Because the platform implements PSA-RoT functionality, then it is essential that an attacker able to run code in an Application RoT partition, whether on the platform itself, or on the Host Platform, cannot compromise the security functionality implemented in the PSA-RoT on the platform.
REQ	Provision of isolation mechanisms in, or of, the Platform does not guarantee that they will be used when combined with the Host Platform. The developer must describe what mechanisms are available, if any, and how they may be used to support isolation of PSA-RoT functionality from the Application RoT Services in accordance with the isolation types defined in [SESIP-PP-L3].
REQ	If isolation of the platform relies on integration rules of the iSE/SE to the device, such as the presence of a TrustZone aware controller for the iSE/SE, then the user guidance shall provide this information.
INFO	This SFR can be iterated in case that the platform implements different isolation mechanisms.

4.2.10 Cryptographic Operation

The platform provides **Operations in Table 6** functionality with **algorithms in Table 6** as specified in **specifications in Table 6** for key lengths **described in Table 6** and modes **described in Table 6**.

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

Table 6: 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.

4.2.11 Cryptographic Random Number Generation

The platform provides 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.

4.2.12 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in **cryptographic algorithms in Table 7** as specified in **specifications in Table 7** for key lengths **described in Table 7**.

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

Table 7: 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.

4.2.13 Cryptographic KeyStore

The platform provides 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.

4.3 Additional Security Functional Requirements

<Complete this section with the additional SFRs defined in SESIP.>

REQ	For iSE/SE, the link between the Host Platform and the iSE/SE must be protected to prevent attacks such as bus probing to reveal secrets or impersonation. Such protection can be achieved through cryptographic or access control means. If this protection relies on cryptographic means, then the SFR defined in Section 4.3.1 (Secure Communication Support) is mandatory for inclusion in the iSE/SE Security Target.
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 4.2.6 to 4.2.13), must be detailed in every applicable SFR.

4.3.1 Secure Communication Support

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

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

INFO	This SFR covers protection of the communication channel between the Host Platform and the iSE/SE when this protection relies on cryptographic means. For this secure communication channel, support from the iSE/SE is required.
INFO	If the platform provides multiple different secure channels, thus SFR should be iterated for each channel type.

4.4 Optional Security Functional Requirements

INFO	The SFRs listed in this section are optional for a PSA-RoT L2 certification following [SESIP-PP-L2] or a PSA-RoT L3 certification following [SESIP-PP-L3]. In case of an iSE/SE or PSA RoT Component certification a claim for any of these only supports a PSA-RoT certification if that certification also makes the claim. However fulfilling an SFR in a 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 for this Profile has a different scope to the term Platform in a PSA-RoT Level 2 or Level 3 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 4.2.6 to 4.2.13) must be detailed in every applicable SFR.

4.4.1 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.

4.4.2 Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust services)

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

INFO	This SFR applies to isolation between each of the Application Root of Trust services on the platform itself (e.g. the Secure Enclave/Element).
INFO	This permits the case where the platform hosts isolated Applications RoT services. Where no such internal isolation is provided then the platform cannot be used to host isolated Applications RoT services. However, additional Application RoT services may be implemented entirely on the Host Platform.
INFO	Where the platform implements isolated Application RoT services, an attacker able to run code outside of any Application Root of Trust service, whether on the platform itself, or on the Host Platform, cannot compromise the security functionality implemented in other hosted Application RoT services, or services implemented in the PSA-RoT on the platform.
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 must describe what mechanisms are available, if any, and how they may be used to support isolation of each of the Application Root of Trust servicesin accordance with the isolation types defined in [SESIP-PP-L3].
INFO	This SFR can be iterated in case that the platform implements different isolation mechanisms.

4.4.3 Secure Debugging

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

The platform ensures that all user data stored, 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.

4.4.4 Secure Encrypted Storage

The platform ensures that all user data stored, 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.

4.4.5 Secure Confidential Storage

The platform ensures that all data stored, except for *<list of data stored>*, is protected to ensure its confidentiality, integrity, authenticity, and binding to the platform instance.

REQ	Secure confidential storage requires confidentiality, integrity and authenticity.
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 with access control mechanisms 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.

4.4.6 Secure Trusted Storage

The platform ensures that all user data, except for *<list of data stored in plaintext>*, is protected to ensure its integrity, authenticity, and binding to the platform instance.

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 Trusted 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.

4.4.7 Secure Data Serialization

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** *<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 serialized data, it is likely that Secure Encrypted Storage or Secure Confidential 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 this Profile fulfil the SESIP3 activities and extend the Vulnerability Assessment assurance to AVA_VAN.4.

REQ	This section shall 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.4 Methodical vulnerability analysis	Vulnerability and testing carried out by the laboratory
	Rationale:	

Table 8: Assurance Mapping and Sufficiency Rationales