SESIP Profile for PSA Certified™ Level 3

Document number:	JSADEN011
Version:	2.0 BETA
Release Number:	01
Authors:	PSA JSA Members: Applus+ Laboratories Arm Limited CAICT DEKRA Testing and Certification ECSEC Laboratory Inc 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:	20/02/2024

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 3 is a fixed time, test laboratory based, evaluation of the PSA-RoT. It is aimed at IoT devices that need to protect against enhanced-basic 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

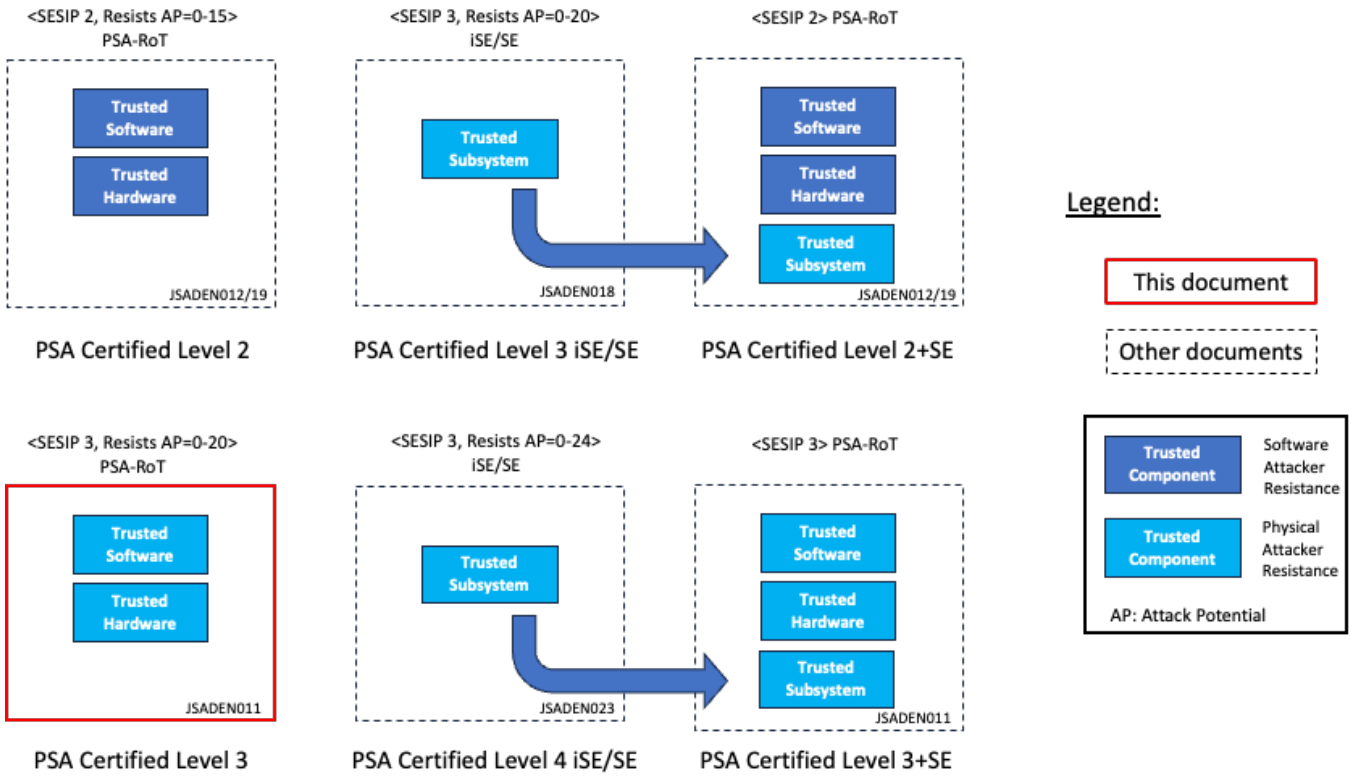

Figure 1: PSA Certified SESIP Profiles for the chip's RoT

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 01

1.2 Release Information

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

Date	Version	Confidentiality	Change
2020-08-28	1.0ALP01	Non-confidential	Initial version to be discussed with JSA members
2020-10-26	1.0ALP02	Non-confidential	Updates discussed with JSA members
2020-12-11	1.0BET01	Non-confidential	Feedback from vendors and JSA members
2022-10-10	1.0 REL 01	Non-confidential	Clearer support for Trusted Sub-systems
2022-11-24	1.0 REL 02	Non-confidential	+ Abstract
2023-10-12	1.0 REL 04	Non-confidential	Alignment with SESIP 1.2 and minor updates
2024-02-02	2.0 BETA 01	Non-confidential	

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
[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
[PSA-L4-iSE-SE]	JSADEN023	JSA	SESIP Profile for PSA Certified™ Level 4 iSE/SE and RoT Component
[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	The entity which when used in composition with a certified PSA Level 3 RoT Component [PSA-L3-COMP] or a certified PSA Level 4 RoT Component [PSA-L4-iSE-SE] form the scope of the certification covered in this profile.
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, 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.
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 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 defined in this document. 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 3+SE Certification

The PSA Certified scheme also considers a PSA Certified Level 3 certification where the product architecture, as illustrated in Figure 2, includes a trusted subsystem, typically an external Secure Element or an on-chip integrated Secure Enclave.

The Developer can obtain the rights to use the specific “PSA Certified Level 3+SE” logo and showcase the solution on **www.psacertified.org**, when the trusted subsystem has been certified for the security functions listed below for protection against physical attacks to at least PSA Certified Level 4 iSE/SE [PSA-L4-iSE-SE], or SESIP4, or AVA_VAN.4 (with Common Criteria).

The L3+SE logo could be used to demonstrate, for example, the benefit of protection against hardware attacks for the most sensitive assets of the product.

1.5.2 PSA Certified RoT Component Certification

The PSA Certified scheme allows for certification of RoT Components that address a subset of the security functions required by an implementation for a Level 3 certifiable PSA Root-of-Trust (RoT) in accordance with this protection profile.

In the PSA Security Model [PSA-SM] such parts of a root-of-trust are referred to as a Trusted Subsystem. 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 (Host Platform) form a complete Level 3 certifiable PSA-Root-of-Trust.

A PSA L3 RoT Component [PSA-L3-COMP] may be used to aid the evaluation of an L3 PSA-RoT certification.

2 Introduction

This SESIP profile proposes a mapping between the security functionality defined in the PSA L3 Protection Profile [PSA-PP-L2] and the SFRs (Security Functional Requirements) listed in the SESIP catalogue [SESIP]. This profile also includes some optional SFRs aiming to cover most of the platform use cases.

The effort for performing the AVA_VAN.3 activities of a standard implementation of a PSA-RoT is **35 person-days**. It is assumed for this workload that:

- the source code for the components in scope of the platform (see Sections 2.4.2 and 2.4.3, hardware design is not required). This shall include drivers for Trusted Subsystems if used;
- no additional SFRs are added in the Profile;
- evaluation activities are not re-used;
- the SFRs “Cryptographic Operation” and “Cryptographic Key Generation” include one cryptographic algorithm;
- the platform does not rely on a certified trusted subsystem or certified PSA Certified RoT Component (see Sections 1.5.1 and 1.5.2).

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 3
PP Version	See title page.
Assurance Claim	SESIP Assurance Level 3 (SESIP 3)
SESIP Standard	*<[GP-SESIP] or [CEN-SESIP]>*
Optional and additional SFRs	*<TBD>*

Table 1: 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	Chip name and version	
	PSA-RoT name and version	
Platform Type	*<TBD>*	
Trusted Subsystem Identification	*<If a trusted subsystem is used, provide reference such as chip name, part number and version.>*	
Trusted Sub-system Certification	*<If a certified trusted subsystem is used please provide the PSA Certificate EAN-13 reference or another identifier.>*	

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 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 are:

- Processor with internal hardware isolation, such as Arm TrustZone technology, and secure memory.
- Processor with multiple cores where one is dedicated to security.
- Processor with external trusted subsystem, such as a Secure Element or secure storage device.
- Use of a separate security processor with secure memory.

Note that secure memory may be integral to the die, on a separate die within the same package or on an external package cryptographically bound to the main chip.

REQ	As stated before, these are examples of different Platform types. The developer shall fill this section based on the evaluated product.
REQ	When a trusted subsystem is relied upon for operation of the PSA Root of Trust, such as an on-chip security subsystem or off-chip Secure Element, the developer shall describe usage of the trusted subsystem, such as, cryptographic provider for the Platform Root-of-Trust and Application Root-of-Trust. The developer may reference any existing security certification of the Trusted Subsystem, such as PSA Certified RoT Component, SESIP, FIPS-140, or Common Criteria. If any existing security certification is not sufficient to cover the trusted subsystem security functions relied upon to establish the PSA Root of Trust, the developer can pre-certify these security functions by: - a PSA Certified Level 3 RoT Component certification [PSA-L3-COMP] or - a PSA Certified Level 4 RoT Component certification [PSA-L4-iSE-SE] Otherwise, these security functions will be evaluated within the scope of the PSA Certified Level 3 security evaluation.

2.4.2 Physical Scope

The hardware is a *<System-on-Chip or a System-in-Package or a discrete solution all with board level integration>.*

The hardware is in the scope of the security evaluation as it provides security features, such as immutable storage or protection of JTAG, which are essential for ensuring the security of the implementation.

<write specific scope details, which may be a silicon chip, a PCB, …>

2.4.3 Logical Scope

The scope for a SESIP Security evaluation, or Target of Evaluation (TOE), according to this profile is the combination of the trusted hardware and firmware components implementing a PSA-RoT with the Security Functional Requirements stated in this document, see Figure 2.

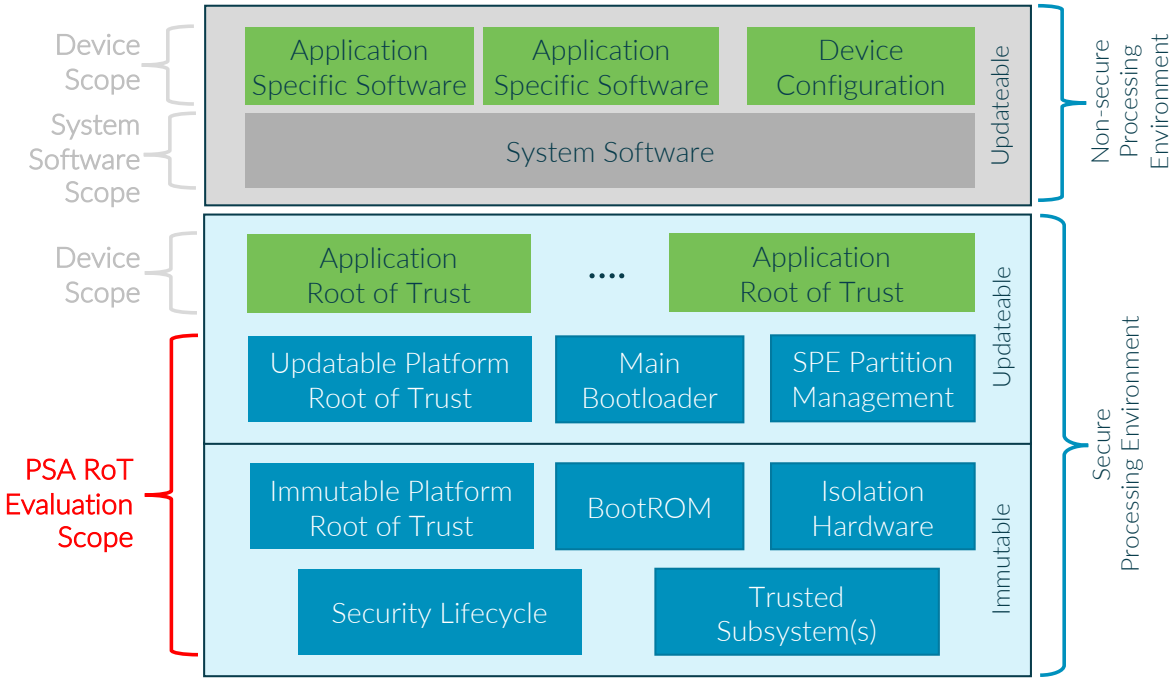

Figure 2: Scope of PSA Certified Level 3

The Chip security evaluation scope includes the following Secure Processing Environment PSA-RoT elements, as described in [PSA-SM]:

- 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 such as attestation, secure storage, and cryptography.
- Any Trusted subsystems that the host processor relies on for protection of its assets, or that implement some of its services.

The Platform 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.

<complete this section with the logical scope of the evaluated product>

2.4.4 Usage and Major Security Features

This profile considers the following features for the purpose of PSA Level 3 security evaluation:

- A Secure Processing Environment (SPE) isolated by hardware mechanisms to protect critical services and related assets from the Non-Secure Processing Environment.
- A Secure Boot process to verify integrity and authenticity of executable code in a chain of trust starting from the Boot ROM. Related certificates are protected in integrity by hardware mechanisms.
- Support for Secure Storage, to protect in integrity and confidentiality sensitive assets for the SPE and related applications. These assets include at least the Hardware Unique Key (HUK), the PSA-RoT Public Key (ROTPK), the Initial Attestation Key (IAK), and the unique instance ID.
- A Security Lifecycle for the SPE, to protect the lifecycle state for the device and enforce the transition rules between states.
- Cryptographic functions services for SPE and SPE applications.
- Support for an attestation method, for example Entity Attestation Token (according to IETF specification).

<complete this section with the additional information from the evaluated product>

2.4.5 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	Additional Objectives for the Environment may be added.
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** 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	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.
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.

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].
REQ	When a trusted subsystem is used for this function, the Chip Vendor shall describe how the trusted subsystem is identified.

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 a trusted subsystem is used for this function, the Chip Vendor shall describe how attestation is performed and which information is exchanged with the trusted subsystem.

4.2.4 Secure Initialization of Platform

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

REQ	Secure initialization functionality shall ensure the integrity and authenticity of the: - Updateable PSA Root of Trust and PSA Root of Trust Services - Trusted Sub-system(s) (if any) - Application Root of Trust (if any).
INFO	The Secure Initialization should be extendable from the SPE to at least the first image of the NSPE code (see section 1.4).
REQ	If the initialization fails, restarts or at most recovery using the update mechanism may be performed. All other functions shall not be available. The application may be used to facilitate this update but shall not provide any other functionality until the authenticity and integrity of the platform is re-established. Any guidance for the application on this shall be explicitly mentioned as a Security Objectives for the operational environment, with explicit reference to where this guidance is provided.
REQ	The user guidance shall describe the secure anti-rollback policies that are enforced by the PSA-RoT. A device shall only execute software versions that do not violate the anti-rollback policies.

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 **confidentiality,** integrity and authenticity of the platform is maintained.

INFO	PSA-RoT consists of an Immutable Platform RoT and an Updateable Platform RoT. This SFR is only applicable to the updatable parts.
REQ	The user guidance shall describe the secure anti-rollback policies that are enforced by the PSA-RoT. A device shall only install software updates of newer versions than the current version on the device.
REQ	If parts of the Platform, for example a Host Platform and a Trusted Subsystem can be updated independently, then this SFR shall be iterated to describe each process.
INFO	Where an existing valid version remains intact after any update is installed, then the update can be verified and authenticity checked, and downgrade attempts rejected, by the TOE during Secure Initialization.
REQ	Where the only existing valid version is lost during any update installation, then the update shall be verified and authenticity checked, and downgrade attempts rejected, by the TOE immediately prior to installation.

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	This profile requires the Platform to be protected against manipulation of the hardware and any data, undetected manipulation of memory contents, by physical probing on the chips surface. In addition to these attack paths, this SFR also includes other attacks such as side-channel attacks to be in the scope.
REQ	If a Trusted Subsystem is used, the link between the Host Platform and the Trusted Subsystem shall be protected to prevent attacks such as probing to reveal secrets or impersonation on the Trusted System of the PSA-RoT by an Application Root of Trust or the NSPE. Such protection can be achieved through cryptographic, or access control means. Protection using cryptographic means is typical where the communications can be easily read, written, or modified by physical probing. The ease of such probing is determined by the attack potential calculation. For instance, physical probing of chip pins would be considered easy, but probing on the die difficult. Protection using access control means, such as hardware access filters or dedicated interconnect, is typical for on-chip solutions. The ease of such probing is determined by the attack potential calculation. For instance, probing on the die would be considered difficult, but if the on-die probe points were connected to chip pins then probing would be easy.

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	This requirement must be interpreted as an isolation between SPE and NSPE.

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	This requirement must be interpreted as an isolation between the PSA Root of Trust and the Application Root of Trust Services.

4.2.10 Cryptographic Operation

The platform provides **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>*
<TBD>	*<TBD>*	*<TBD>*	*<TBD>*	*<TBD>*

Table 5: Cryptographic Operations

REQ	This SFR addresses the algorithms available to the NSPE. As this SFR is mandatory, at least one cryptographic algorithm shall be included in the scope.

REQ	The platform implements some internal functionality that performs cryptographic operations: secure storage, attestation, and boot decryption. The cryptography used by these functions shall be also described in this SFR.
REQ	PSA requires minimum security strength in line with the current version of NIST [SP-800-57] recommendations.
INFO	RSA 2048 will not be accepted in products certified from 2027 onwards.
REQ	When a trusted subsystem is used for some or all of this function, the Chip Vendor shall describe which set of cryptographic operations is performed by the trusted subsystem.

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 NSPE.
REQ	When a trusted subsystem is used for some, or all, of this function, the Chip Vendor shall describe which part of the random number generation is performed by the trusted subsystem.
REQ	If the platform contains multiple random number generators, this SFR shall be iterated to describe each instance.

4.2.12 Cryptographic Key Generation

The platform provides a way to generate cryptographic keys for use in **cryptographic algorithms 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>*
<TBD>	*<TBD>*	*<TBD>*	*<TBD>*

Table 6: Cryptographic Key Generation

REQ	This SFR addresses the key generation algorithms available to the NSPE. As this SFR is mandatory, at least one key generation algorithm shall be included in the scope.
REQ	When a trusted subsystem is used for some, or all, of this function, the Chip Vendor shall describe which set of cryptographic operations is performed by the trusted subsystem.

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 NSPE. As this SFR is mandatory, at least one cryptographic algorithm shall be included in the scope.
REQ	The cryptographic keys used internally by the platform shall be also described in this SFR, including the HUK, ROTPK, IAK secure storage key and boot decryption key (if supported).
REQ	PSA requires minimum security strength in line with the current version of NIST SP800-57 pt 1 recommendations.
INFO	RSA-2048 will be accepted in products certified before the end of 2026.
REQ	When a trusted subsystem is used for some, or all, of this function, the Chip Vendor shall describe which cryptographic keys are stored on the trusted subsystem.

4.3 Optional Security Functional Requirements

4.3.1 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.

4.3.2 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 Secure Partitions** cannot compromise the **confidentiality and** integrity of the other application parts.

INFO	Additional isolation boundaries between each of the Application RoT services.

4.3.3 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 shall be included in the ST as it addresses the authenticated access to the PSA-RoT debug functionality. However, in case that debug features are deactivated prior to the final product is delivered to the end-user, this SFR can be removed.

4.3.4 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	For the secure storage functionality, the developer shall claim in its product security target at least one of the following SFRs: - Secure Encrypted Storage - Secure Confidential Storage
REQ	Secure encrypted storage requires confidentiality and integrity.
REQ	Data stored shall be bound to the unique instance of the platform.
INFO	This SFR can be claimed for the implementation of the Internal Trusted Storage API [PSA-SS] when the confidentiality and integrity properties rely on cryptographic means.
REQ	The scope is all data stored in any memory included in the scope of the evaluation. When a trusted subsystem is used for some, or all, of this function, the Chip Vendor shall describe which set of assets is managed by the trusted subsystem. In cases where data is also stored in a memory which is out of the scope of the evaluation, the "Secure Data Serialization" SFR shall be also claimed.

4.3.5 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	For the secure storage functionality, the developer shall claim in its product security target at least one of the following SFRs: - Secure Encrypted Storage - Secure Confidential Storage
INFO	This SFR can be claimed for the implementation of the Internal Trusted Storage API [PSA-SS] when the confidentiality, integrity and authenticity properties rely on access control mechanisms.
INFO	The scope is all data stored in any memory included in the scope of the evaluation. In cases where data is also stored in a memory which is out of the scope of the evaluation, the "Secure Data Serialization" SFR shall be also claimed.

4.3.6 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 can be claimed for the implementation of the Internal Trusted Storage API [PSA-SS] when the integrity and authenticity properties rely on cryptographic means.
INFO	The scope is all data stored in any memory included in the scope of the evaluation. In cases where data is also stored in a memory which is out of the scope of the evaluation, the "Secure Data Serialization" SFR shall be also claimed.

4.3.7 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.

REQ	This SFR shall be claimed if the platform data is stored in a memory out of the scope of the evaluation, such as a removable or on-PCB Flash, or a cloud-storage service.
INFO	This SFR can be claimed for the implementation of the Protected Storage API [PSA-SS].
INFO	Protection of the cryptographic material used for secure serialized data will rely on one of the mandatory Secure Encrypted Storage or Secure Confidential Storage SFR.

4.3.8 Secure Communication Support

The platform provides 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	If the platform provides multiple different secure channels, this SFR should be iterated for each channel type.

4.3.9 Secure Communication Enforcement

The platform ensures that communication with *<list of endpoints>* can only be done over the secure communication channel(s) supported by the platform using *<list of protocols and measures>*.

INFO	The ST must include an iteration of Secure Communication Support for each secure channel type referenced in this SFR.

5 Mapping and Sufficiency Rationales

5.1 Assurance

The assurance activities defined in [PSA-EM-L2] fulfil the SESIP3 activities. In particular, the required source code review, vulnerability analysis and testing to an equivalent of 35 person-days of the [PSA-EM-L3] is applicable.

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:	

Assurance Class	Assurance Family	Covered by
ALC: Life-cycle support	ATE_CMC.1 Labelling of the TOE	*<Description of which developer evidence is used to meet this requirement>*
	Rationale:	
	ATE_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

6 Appendix: SFRs by PSA Certified Levels

The following table summarizes the required SFRs according to PSA Certified Levels. In this table, Y stands for mandatory SFR, O for optional SFR and N/A for not applicable for this level.

PSA Certified Level	Level 2	Level 3	Level 3 iSE/SE or Level 4 iSE/SE
Scope	PSA-RoT	PSA-RoT	Trusted Subsystem
Evaluation Methodology	SESIP Level 2	SESIP Level 3	SESIP Level 3
Attack Resistance	0-15	0-20	0-20 (Level 3) 0-24 (Level 4)
Mandatory SFRs			
Verification of Platform Identity	Y	Y	Y
Verification of Platform Instance Identity	Y	Y	O
Attestation of Platform Genuineness	Y	Y	O
Secure Initialization of Platform	Y	Y	Y
Attestation of Platform State	Y	Y	O
Secure Update of Platform	Y	Y	Y
Physical Attacker Resistance	N/A	Y	Y
Software Attacker Resistance: Isolation between SPE and NSPE	Y	Y	Y
Software Attacker Resistance: Isolation between PSA-RoT and Application RoT	Y	Y	Y
Cryptographic Operation	Y	Y	Y
Cryptographic Random Number Generator	Y	Y	Y
Cryptographic Key Generation	Y	Y	Y
Cryptographic KeyStore	Y	Y	Y
Secure Storage (At least one of Secure Encrypted Storage, Secure Confidential Storage or Secure Trusted Storage)	Y	Y	O
Additional SFRs			
Secure Communication Support	N/A	N/A	(1)
Optional SFRs			
Audit Log Generation and Storage	O	O	O
Software Attacker Resistance: Isolation of Application Parts (between each of the ARoTs)	O	O	

Secure Debugging	O	O	O
Limited Physical Attacker Resistance	O	N/A	N/A
Secure Data Serialization	O	O	
Secure Communication Support	O	O	
Secure Communication Enforcement	O	O	

Table 8 SFRs by PSA Certified Levels

For iSE/SE, the Secure Communication Support SFR marked with (1) must be included into the security target if protection of the link between the Host Platform and the iSE/SE relies on cryptographic means (as opposed to access control means).