SESIP Profile for PSA Certified™ Level 2

Based on [SESIP] methodology, version "Public Release v1.1"

psacertified™

psacertified™
level two

Document number:	JSADEN012
Version:	1.0
Release Number:	BET04
Author	PSA JSA Members: Applus+, S.L Arm Limited CAICT ECSEC Laboratory Inc Prove & Run S.A.S. Riscure B.V. SGS Brightsight B.V. Trust CB B.V. UL TS B.V.
Authorized by:	PSA JSA Members
Date of Issue:	04/04/2022

Contents

1 About this document

1.1 Current Status and Anticipated Changes

Current Status: Beta

1.2 Release Information

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

Date	Version	Confidentiality	Change
2020-12-09	1.0ALP01	Non-confidential	Initial version to be discussed with JSA members
2021-01-27	1.0BET01	Non-confidential	Updates discussed with JSA members
2020-02-10	1.0BET02	Non-confidential	Feedback provided by JSA members
2020-03-08	1.0BET04	Non-confidential	External partner review

1.3 References

This document refers to the following documents.

1.3.1 Normative references

Ref	Doc No	Author(s)	Title
[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-L2]	JSADEN004	JSA	PSA Certified Attack Method for PSA L2
[PSA-AM-L3]	JSADEN008	JSA	PSA Certified Attack Method for PSA L3
[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-L3]	JSADEN011	JSA	SESIP Profile for PSA Certified™ Level 3
[SESIP]	GP_FST_070	GlobalPlatform	Security Evaluation Standard for IoT Platforms (SESIP) v1.1
[CEM]	CCMB-2017-04-004		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 Architecture Security Model v1.0

1.4 Terms and Abbreviations

This document uses the following terms and abbreviations (see PSA-SM and PSA Cert L1 V2.1 or newer questionnaire).

Term	Meaning
Application	Used in SESIP to refer to the components which are out of the scope of the evaluation. It is a synonym for Connected Application.
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.
Connected Application	Software developed by an IoT vendor, implementing IoT end-user use case based on the underlying Connected Platform. May be referred to as “Application” when there is no ambiguity.
Connected Platform	Combination of hardware and software that provides a runtime environment for a Connected Application. A Connected Platform implements security features and makes security services available to the Connected Application. May be referred to as “platform” when there is no ambiguity.
Connected product	Combination of a Connected Platform and a Connected Application that a product vendor puts on the market.May be referred as “product” when there is no ambiguity.
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.
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. In SESIP terms, the NSPE is the “application”.
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 SESIP to refer to the components which are in the scope of the evaluation. It is a synonym for Connected platform.
Product	Used by SESIP as a synonym for Connected product
PSA	Platform Security Architecture
PSA Certification Body	The entity that receives applications for PSA security certification, issues certificates, maintains the security certification scheme, and ensures consistency across all the evaluation laboratories.
PSA Functional APIs	PSA defined Application Programming Interfaces on which security services can be built. APIs defined so far include Crypto, Secure Storage and Attestation.
PSA Functional API Certification	Functional certification confirms that the device implements the PSA Functional APIs correctly by passing the PSA Functional certification test suites.
PSA Root of Trust (PSA-RoT)	The PSA defined combination of the Immutable Platform RooT of Trust and the Updateable Platform Root of Trust, and considered to be the most trusted security component on the device. See [PSA-SM].
Immutable Platform Root of Trust	The minimal set of hardware, firmware and data of the PSA-RoT, which is inherently trusted because it cannot be modified following manufacture. There is no software at a deeper level that can verify that it as authentic and unmodified.
Updateable Platform Root of Trust	The firmware, software and data of the PSA-RoT that can be securely updated following manufacture.
Platform Root of Trust Service(s)	PSA defined security services for use by PSA-RoT, Application RoT Service(s) and by the NSPE. Executes in the Secure Processing Environment and may use Trusted Subsystems. This includes the services offered by the PSA Functional APIs.

SESIP Profile	Document providing a common set of functionality 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). In SESIP terms, the SPE is the “platform”.
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
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 2

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 TOE. The evaluation laboratory examines measures and processes to ensure that a functional TOE 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 2 product, either through the PSA Certified Level 2 Protection Profile [PSA-PP-L2] and associated evaluation methodology [PSA-EM-L2], or through a SESIP evaluation using this SESIP Profile defined in this document, which defines the scope and security requirements for the evaluation of a TOE implementing the PSA architecture.

1.5.1 PSA Certified Level 2 Ready Evaluation

The PSA Certified scheme allows for pre-certification evaluation of FPGA or development-based systems, which provide reference designs for ASIC or custom chip, but which may not be able to meet all security functions of this profile. In this case, only the claimed security functions are tested by the Evaluation Laboratory who issues the Evaluation Technical Report. No PSA Certified Level 2 certificate is generated for a Level 2 Ready evaluation, but the Developer can obtain the rights to use a specific "PSA Certified Level 2 Ready" logo and showcase its solution on **www.psacertified.org**.

Such a logo could be used to demonstrate, for example, the benefit of software security assurance offered from an evaluated FPGA based system for development of secure AROTs, RTOS or device while maximizing chances of passing PSA Certified Level 2 certification for future ASIC or custom chips based on the FPGA reference design.

1.5.2 PSA Certified Level 2+SE

The PSA Certified scheme also considers a PSA Certified Level 2 certification where the product architecture, as illustrated in Figure 1, includes a trusted subsystem, typically a Secure Element, that is certified for the considered security functions for protection against hardware attacks and at least at AVA_VAN.3 (with Common Criteria, PSA Certified Level 3 RoT component [PSA-Comp] or SESIP3).

The Developer can obtain the rights to use a specific "PSA Certified Level 2+SE" logo and showcase its solution on **www.psacertified.org**. Such a logo could be used to demonstrate, for example, the benefit of protection against hardware attacks for the most sensitive assets of the product.

2 Introduction

This SESIP profile proposes a mapping between the security functionality defined in the PSA L2 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.2 activities of a standard implementation of a PSA-RoT is **25 man-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 Protection Profile;
- evaluation activities cannot be reused;
- the SFRs “Cryptographic Operation” and “Cryptographic Key Generation” include one cryptographic algorithm.

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 Level 2
PP Version	V1.0BET03
Assurance Claim	SESIP Assurance Level 2 (SESIP 2)
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**	
TOE Name	<TBD>	
TOE Version	<TBD>	
TOE Identification	Chip name and version	
	PSA-RoT name and version	
TOE 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 in particular 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 TOE Type

<The developer must choose an appropriate TOE 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.
- Use of a separate security processor with secure memory.

INFO	As stated before, these are examples of different TOE types. The developer must 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 must provide references for the trusted subsystem, such as chip name, part number and version. The developer must 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 Common Criteria, FIPS-140, SESIP, or PSA Certified RoT Component. 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 either: • a PSA Certified Level 2 security certification for RoT components [PSA-Comp] • a PSA Certified Level 3 security certification for RoT components if the product applies for PSA Certified Level 2+SE certification. Otherwise, these security functions will be evaluated within the scope of the PSA Certified Level 2 security evaluation.

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.

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.

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 TOE 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.

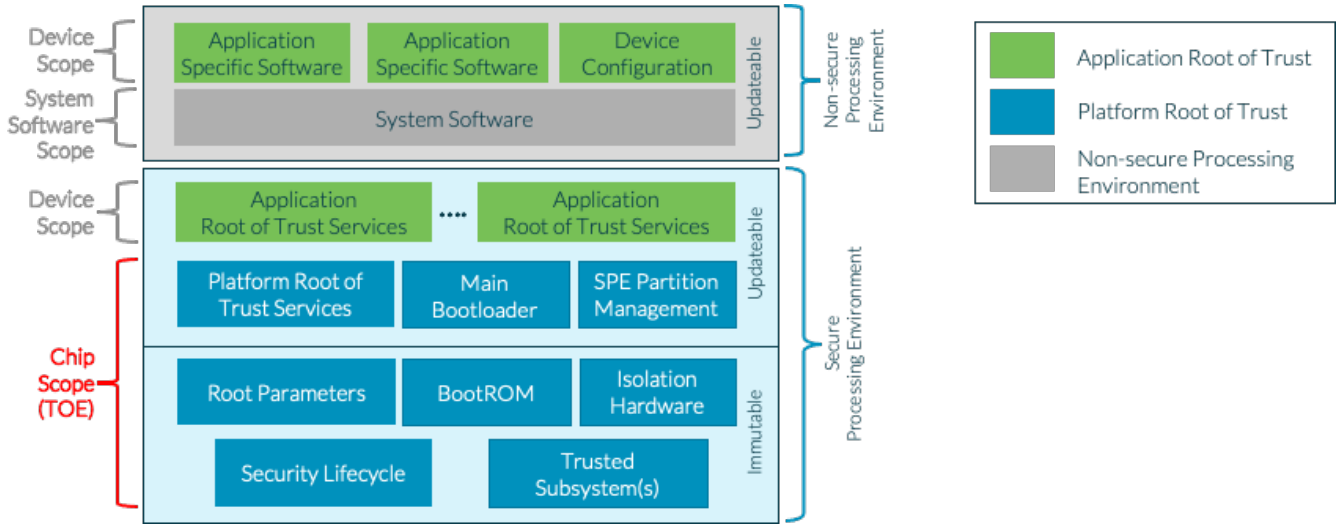

Figure 1: Scope of PSA Certified Level 2

<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 2 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 TOE 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 TOE are subject to secure key management procedures.	*<[Ref1]> Section X*
TRUSTED_USERS	Actors in charge of TOE 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 TOE must be provided by the TOE 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 must list in particular 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 TOE should be supported by the development, production and test environment. Otherwise, if the integrity and uniqueness of the unique identification is responsibility of the TOE 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 **SESIP2** 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. Additional SFRs are then added to suit the vendor's objectives. For every SFR, a description of the implementation proposed in the TOE and of the way this implementation is assessed also needs to be included.

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 and their versions.

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 cannot be cloned or changed without detection.

REQ	When a trusted subsystem is used for this function, the Chip Vendor must 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 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 can be performed**.

INFO	Secure initialization must include: - Updateable Root of Trust - Application Root of Trust (if any) - NSPE code (application and OS)
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 reestablished. 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.

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 must only install software updates of newer versions than the current version on the device.

4.2.7 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.

4.2.8 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.

4.2.9 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>*
<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 must 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 functionality must be also described in this SFR.
REQ	PSA requires equivalence of at least 128-bit security level.
REQ	When a trusted subsystem is used for some or all of this function, the Chip Vendor must describe which set of cryptographic operations is performed by the trusted subsystem.

4.2.10 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 NSPE.
REQ	When a trusted subsystem is used for some or all of this function, the Chip Vendor must describe which part of the random number generation is performed by the trusted subsystem.

4.2.11 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>*
<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 must be included in the scope.
REQ	PSA requires equivalence of at least 128-bit security.
REQ	When a trusted subsystem is used for some or all of this function, the Chip Vendor must describe which set of cryptographic operations is performed by the trusted subsystem.

4.2.12 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 *<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 must be included in the scope.
REQ	The cryptographic keys used internally by the platform must be also described in this SFR, including the HUK, ROTPK, IAK secure storage key and boot decryption key (if supported)..
REQ	PSA requires equivalence of at least 128-bit security.
REQ	When a trusted subsystem is used for some or all of this function, the Chip Vendor must describe which cryptographic keys are stored on the trusted subsystem.

4.3 Additional Security Functional Requirements

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

4.3.1 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	Trusted Subsystems used for the implementation of the PSA-RoT, which include both hardware and software components, are also in the scope of evaluation. This SFR is mandatory when a Trusted Subsystem is used. The developer must describe the mechanism that is used to protect in confidentiality and integrity the communication between the SPE and the trusted subsystem and add the appropriate SFRs to cover the Trusted Subsystem functionality.
INFO	Level 2+SE requires a protected link between the SE and the SPE part of the SoC's to prevent basic attacks such as probing the PCB to reveal secrets. An on-chip Trusted Subsystem is likely to have secure communication support if it is a private peripheral.

4.4 Optional Security Functional Requirements

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 **Secure Partitions in the Application Root of Trust** cannot compromise the integrity and confidentiality of the other application parts.

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

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 data stored by the application, with the exception of *<list of exceptions>*, is made unavailable.

<Describe the implementation in the TOE that covers this SFR>

REQ	If the platform implements secure debugging, this SFR must 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.

4.4.4 Secure Encrypted Storage (internal 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 storage functionality may be covered by the following SFRs: - Secure Encrypted Storage (internal storage) - Secure Storage (internal storage) - Secure External Storage It is mandatory to define at least one SFR covering the secure storage functionality.
REQ	Secure encrypted storage requires confidentiality and integrity.
REQ	Data stored must be bound to the unique instance of the platform.
INFO	This SFR covers the encrypted internal storage functionality available to the NSPE.
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 must describe which set of assets is managed by the trusted subsystem. In case that the data is stored in a memory which is out of the scope of the evaluation, the SFR “Secure External Storage” must be also claimed.

4.4.5 Secure Storage (internal 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>*.

REQ	Secure storage functionality may be covered by the following SFRs: - Secure Encrypted Storage (internal storage) - Secure Storage (internal storage) - Secure External Storage It is mandatory to define at least one SFR covering the secure storage functionality.
INFO	This SFR covers the internal storage functionality available to the NSPE implementing authenticity and integrity (confidentiality not required).
INFO	The scope is all data stored in any memory included in the scope of the evaluation. In case that the data is stored in a memory which is out of the scope of the evaluation, the SFR "Secure External Storage" must be also claimed.

4.4.6 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** *<and binding to the platform instance, versioning>* is ensured.

REQ	Secure storage functionality may be covered by the following SFRs: - Secure Encrypted Storage (internal storage) - Secure Storage (internal storage) - Secure External Storage It is mandatory to define at least one SFR covering the secure storage functionality.
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 ToE 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-L2] fulfill the SESIP2 activities. In particular, the required source code review, vulnerability analysis and testing to an equivalent of 25 man days of the [PSA-EM-L2] is applicable.

REQ This section must be completed by the ST writer.

Assurance Class	**Assurance Family**	**Covered by**	**Rationale**
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	*<Section "Introduction" and title page of the Security Target>*	*<TBD>*
	ASE_OBJ.1 Security requirements for the operational environment	*<Section "Security Objectives for the Operational Environment" of the Security Target>*	*<TBD>*
	ASE_REQ.3 Listed Security requirements	*<Section "Security Requirements and Implementation" of the Security Target>*	*<TBD>*
	ASE_TSS.1 TOE Summary Specification	*<Section "Security Requirements and Implementation" of the Security Target>*	*<TBD>*
ADV: Development	ADV_FSP.4 Complete functional specification	*<Description of which developer evidence is used to meet this requirement>*	*<TBD>*
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	*<Description of which developer evidence is used to meet this requirement>*	*<TBD>*
	AGD_PRE.1 Preparative procedures	*<Description of which developer evidence is used to meet this requirement>*	*<TBD>*
ALC: Life-cycle support	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>*	*<TBD>*
ATE: Tests	ATE_IND.1 Independent testing: conformance	*<Description of which developer evidence is used to meet this requirement>*	*<TBD>*
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis	Vulnerability and testing carried out by the laboratory	*<TBD>*

Table 7: Assurance Mapping and Sufficiency Rationales

5.2 Functionality

REQ The aim of this table is to detail the mapping between [PSA-PP-L2] and the SESIP requirements defined in the current document based on the platform implementation.

Please, consider the following points to fill the table:

- Optional SFRs (Section 4.3) are included in this table. Any that are not claimed must be clearly indicated together with an explanation of why it is not claimed.
- Additional SFRs (Section 4.3) are not included in this table. If the Platform claims additional SFRs, add them to the table along with an explanation.
- To provide the mapping to F.SECURE_STORAGE, select the appropriate secure storage SFR(s).
- This profile can be used for a wide range of functionalities. This is the case, for example, secure storage. Please, make sure that the mapping is consistent with the platform implementation.

Table 8 Functionality Mapping and Sufficiency Rationales

PSA Security Function	**(detail)**	**Covered by SESIP SFR**	**Rationale**
F.INITIALIZATION	Boot sequence in scope: • Chip • PSA Root of Trust • Application Root of Trust Services	Secure Initialization of Platform	Full coverage
F.SOFTWARE_ ISOLATION	Level 1: Isolation between SPE and NSPE	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage
	Level 2: Isolation between PSA-RoT and Application RoT	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Full coverage
	(Optional) Level 3: Isolation between Application RoT	Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust services)	Full coverage
F.SECURE_ STORAGE	Integrity and Confidentiality (optional)	Secure Encrypted Storage (internal storage)	Requires encryption mechanism providing both integrity and confidentiality.
	Authenticity and integrity (optional)	Secure Storage (internal storage)	Requires authenticity and integrity

	Binding to the RoT	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Stored data is isolated from the NSPE and Application Root of Trust Services by using a unique HUK for each platform.
	Basic rollback – atomicity	Not covered by any SESIP SFR. Note added in "Secure Encrypted Storage".	Covered by user guidance.
	External storage (optional)	Secure External Storage	Requires encryption mechanism providing authenticity, integrity and confidentiality.
F.FIRMWARE_ UPDATE	Integrity and authenticity of the update.	Secure Update of Platform	Full coverage
F.SECURE_STATE	Protects itself against abnormal situations caused by programmer errors or violation of good practices from code executed outside of the TOE, either from SPE or NSPE.	Software Attacker Resistance: Isolation of Platform	Full coverage
	Controls the access to its services by Applications and checks the validity of parameters of any operation requested from Applications	Software Attacker Resistance: Isolation of Platform	Full coverage
	Enters a secure state upon platform initialization error or software failure detection, without exposure of any sensitive data.	Partially covered by the SFR "Secure initialization of platform" and "Secure update of platform".	Full coverage
F.CRYPTO	Minimum cryptographic operations supported: Attestation Secure Storage	Cryptographic Operation	Additional algorithms can be added based on the supported algorithms provided by the PSA cryptographic API.

	Minimum cryptographic keys for secure storage: • Attestation • Secure Storage	Cryptographic KeyStore	Additional algorithms can be added based on the supported algorithms provided by the PSA cryptographic API.
	PSA SM requires that all devices implement at least the following trusted cryptographic services: • True random number generator • Global nonce counter	Cryptographic Random Number	The evaluation of the random number generator shall follow a recognized methodology, e.g. [AIS31] or [SP800-90].
		Cryptographic Key Generation	Additional algorithms can be added based on the supported algorithms provided by the PSA cryptographic API.
F.ATTESTATION		Verification of Platform Identity	Unique identification of the platform
	Unique platform number	Verification of Platform Instance Identity	Unique identification of the platform instance
	Proof of origin	Attestation of Platform Genuineness	"Verification of Platform Instance" and "Verification of Platform Instance Identity" are included in the attestation token.
	Lifecycle state	Attestation of Platform State	Full coverage
F.AUDIT	(Optional) Protect the stored audit records from unauthorized deletion	Audit Log Generation and Storage	Full coverage
	(Optional) Prevent unauthorized modifications	Audit Log Generation and Storage	Full coverage
F.DEBUG	Optional	Secure Debugging	Full coverage if the debug functionality is available to the end user.