Rambus

Security IP

SESIP Security Target for PSA Certified RoT Component Level 2

VaultIP RT-130

Based on SESIP methodology, version 1.1

Document Revision: F
Document Date: 2023-11-24
Document Number: 001-130410-503/939

Document Status: Accepted

Rambus Inc. Corporate Headquarters
4453 North First Street, Suite 100
San Jose, CA 95134
Phone: +1 408-462-8000
Website : https://www.rambus.com/
Contact : sipsupport@rambus.com

Rambus ROTW Holding B.V.
Boxtelseweg 26A
5261 NE Vught
The Netherlands
Phone: +31-73-6581900

Table of Contents

List of Tables

List of Figures

Document Revision History

Doc Rev	Date (Y-M-D)	Author	Purpose of Revision
A	2023-06-29	MWANG	First Release
B	2023-08-17	MWANG	Updates following feedback from lab Removed claims for Factory Reset and Decommission
C	2023-10-11	MWANG	Updates following feedback from lab
D	2023-11-06	MWANG	Adding claims about secure communication enforce and secure communication support
E	2023-11-20	MWANG	Minor updates about certifications claims and objective environments.
F	2023-11-24	MWANG	Update the reference version number.

1 Introduction

The Security Target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against [SESIP] (in chapter “Security requirements and implementation”) that a potential consumer can rely upon the product upholding if they fulfil the objectives for the environment (in chapter “Security Objectives for the operational environment”).

1.1 SESIP Profile reference

Reference	Value
SESIP version	1.1
PP Name	SESIP Profile for PSA Certified RoT Component Level 2
PP Version	1.0 REL 02
Assurance Claim	SESIP Assurance Level 2 (SESIP 2)
Optional and additional SFRs	Secure External Storage Field Return of Platform Residual Information Purging Reliable Index Secure communication Support Secure communication Enforcement

1.2 ST reference

See title page.

1.3 Platform reference

Reference	Value	
Platform Name	*RT-130 Root of Trust Core*	
Platform Version	*RT-130 FW4.2HW4.1*	
Platform Identification	*Hardware*	*4.1*
	Software	*4.2*
Platform type	*Security Soft IP*	

Table 1 Platform Reference

1.4 Included guidance documents

The following documents are included with the platform.

Reference	Name	Version
[SW_INT]	*VaultIP-130 FW4.2 Software Integration Manual*	*Revision: A* *Date:2023-04-12*
[FW_Manual]	*VaultIP-130 FW4.2 Firmware Reference Manual*	*Revision: B* *Date:2023-11-24*
[HW_INT]	*VaultIP-130 HW4.1 Hardware Integration Manual*	*Revision: A* *Date:2023-04-04*
[HW_Manual]	*VaultIP-130 HW4.1 Hardware Reference Manual*	*Revision: A* *Date:2023-04-13*
[SEC_GUID]	*VaultIP-130 User Security Guidance Manual*	*Revision: C* *Date:2023-11-22*

Table 2 Included guidance documents

1.5 Acronyms

CPU	Central Processing Unit
FW	Firmware
HUK	Hardware Unique Key
IP	Intellectual property
PSA	Platform Security Architecture
RAM	Random-access Memory
SFWBCR	Secure FirmWare Boot Confidentiality Root
GPFW	General Purpose FW
HW	Hardware
OTP	One Time Programmable
PSIRT	Product Security Incident Response Team
ROM	Read-only Memory
SoC	System on Chip
TOE	Target of Evaluation

1.6 Document references

Reference	Name	Version
[SESIP]	*SESIP methodology*	*Version 1.1*
[SEC_DLV]	*Security IP Secure Delivery Process*	*Version 1.0*
[ESV]	*RT-130 Entropy Source Validation Certificate*	-
[FLR]	*Rambus Vulnerability Management Procedure*	*Revision: A*
[OTP]	*VaultIP-130 FW4.2 OTP Static Asset Image Application Note*	*Revision: A*
ATE	*Functional Testing document and evidence*	-

1.7 (Optional) Other Certification

Not applicable

1.8 Platform functional overview and description

1.8.1 Platform type

The RT-130 Root of Trust is a silicon IP core developed to protect an SoC platform and its operation. It allows the SoC to boot securely and protects sensitive key material and assets. At its heart, its Secure Asset Store allows import, negotiation, and creation of secret and private key material. Safe use of key material is enforced through a flexible key use and access policy. Ideal for power and space-sensitive applications like IoT servers, gateways and edge devices, the RT-130 Root of Trust offers the best balance of size and performance available on the market.

1.8.2 Physical Scope

The TOE scope is indicated by the red border in Figure 1. The blue parts of Figure 1, comprising the FPGA processing system, are outside of the evaluation scope.

The physical scope includes is indicated by the red boundary in Figure 1

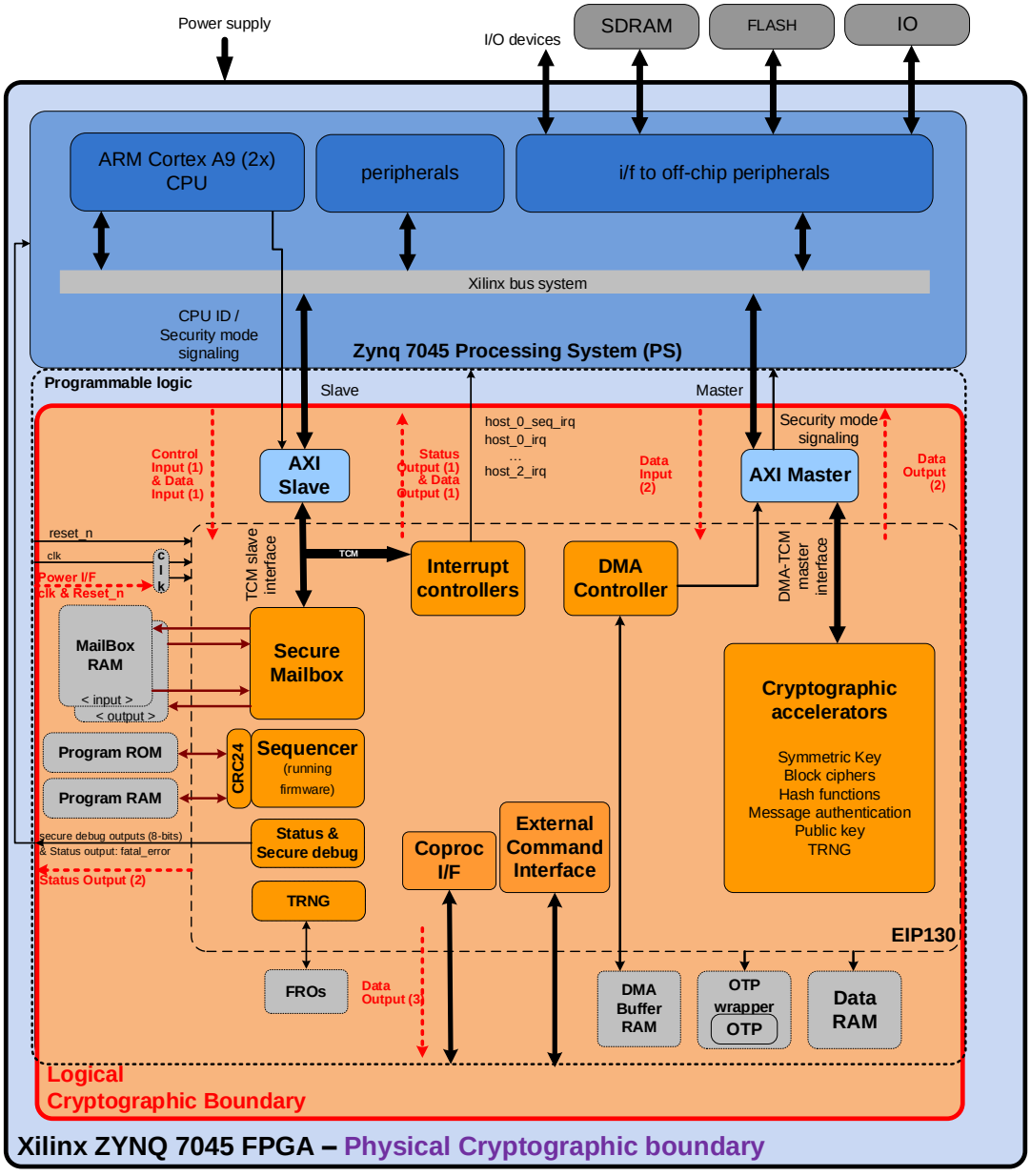

Figure 1 Physical scope of the TOE (bounded by red border)

1.8.3 Logical Scope

The logical scope includes the BootFW (runs in ROM) and GPFW (runs in RAM).

1.8.4 Usage and Major Security Features

The main security features of the TOE are as follows:

- Secure boot
  - Integrity checks at all boot stages
  - BootROM checks the integrity, authenticity and confidentiality of firmware image loaded during booting
- Cryptographic functions
- Secure Firmware update
- Random Number Generator
- Secure storage of security parameters
  - All assets stored in the TOE have been defined with the ownership and use policies
  - Assets cannot be exported in plaintext, unless tagged as public/exportable assets.
  - Sensitive security parameters are never stored in plaintext outside the TOE.
- Anti roll-back
- Platform Isolation
- Token access validation
  - Before executing any commands, the TOE validates the user. Only allowed users are able to use the security services of the TOE.

1.8.5 Required Hardware/Software/Firmware

External NVM for persistent storage of data and the GPFW.

2 Security Objectives for the operational environment

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

ID	Description	Reference
SW_INTEGRATION	The users shall follow the software integration guidance document [SW_INT] for keys.	[SW_INT] all sections
HW_INTEGRATION	In order to build the product securely, the hardware integration manual [HW_INT] shall be followed.	[HW_INT] all sections
SECURE_KEY_PROVISION	Keys like HUK shall be provisioned during provisioning phase in the factory. “In the field” creation of the HUK shall not be allowed.	[SEC_GUID] section 3.2
VERSION_UPDATE	When update is available, the chip vendor shall update the TOE version information.	[SEC_GUID] section 4.2
APPROVED_ALGORITHMS	Users should use NIST approved cryptographic algorithms.	[SEC_GUID] section 4.6, 4.7
RNG_CONFIG	TRNG and DRBG configuration shall follow the security guidance.	[SEC_GUID] section 3.3, 3.4
RNG_USE	TRNG and DRBG use shall follow the security guidance.	[SEC_GUID] section 4.3, 4.4
KEY_MANAGEMENT	Cryptographic keys and certificates outside of the platform are subject to secure key management procedures.	This document
TRUSTED_USERS	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	This document
UNIQUE_ID	The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage	[SEC_GUID] section 3

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: SESIP2 as defined in [SESIP].

The assurance requirements are shown below:

Assurance Class	Assurance Families	
ASE: Security Target evaluation	*ASE_INT.1*	*ST Introduction*
	ASE_OBJ.1	*Security requirements for the operational environment*
	ASE_REQ.3	**Listed security requirements**
	ASE_TSS.1	*TOE summary specification*
ADV: Development	ADV_FSP.4	Complete functional specification
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	*ALC_FLR.2*	*Flaw reporting procedures*
ATE: Tests	ATE_IND.1	Independent testing: conformance
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 3 SESIP2 Assurance Requirements

3.1.1 Flaw Reporting Procedure (ALC_FLR.2)

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

Rambus has built a Product Security Incident Response Team (PSIRT), which is responsible for responding to security incidents. PSIRT manages receipt, investigation and releasing of information about security issues regarding Rambus products.

For external parties that that wish to report a vulnerability, they may contact Rambus via the link below:

https://www.rambus.com/security/response-center/report-vulnerability/

See [FLR] for details.

Products that have a smaller number than the hardware and firmware version number indicated in section 1.3, are considered as older versions. E.g. HW4.0 or FW 4.1.

Products that have a larger number than the hardware and firmware version number indicated in section 1.3, is considered as newer versions. E.g. HW4.2 or FW 4.3.

3.2 Base PP Security Functional Requirements

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

3.2.1 Verification of Platform Identity

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

Conformance rationale:

The platform ID can be read by sending a “system information” token. By sending this token, both the hardware and software version will be output. For more details please refer to [FW_Manual] section 5.21 System Information.

3.2.2 Secure Update of Platform

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

Conformance rationale:

The TOE has a secure update mechanism which is similar to secure booting. For details see 3.3.1. Only GPFW is updatable. When an update is required. The updated GPFW is delivered to the chip vendor via Rambus secure delivery system [SEC_DLV], which requires user authentication via access control. The chip integrator is responsible for installation into VaultIP. This includes updating the FW version information [SEC_GUID]. The updated GPFW will be verified by BootFW before installation, following the same process as described in section "Secure Initialization of Platform" (section 3.3.1).

All the encryption functions are tested at the start of the process.

3.3 SFRs for PSA-RoT Component

3.3.1 Secure Initialization of Platform

The platform ensures its authenticity and integrity during platform initialization. If the platform authenticity or integrity cannot be ensured, the platform will remain in the boot state awaiting a valid FW image. Refer to [FW_Manual] section 5.38.

Conformance rationale:

The FW includes 2 parts, BootFW and GPFW. BootFW is located in ROM. The BootFW is implemented during manufacturing phase and as such, the BootFW is not updatable.

GPFW runs in a specific RAM area of the TOE. When the device is powered off, the GPFW is cleared from the TOE. It is only permanently stored encrypted (AES) in the external NVM.

For further details, see [FW_Manual] 5.38.2 & 5.38.3.

3.3.2 Software Attacker Resistance: Isolation of Platform

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

Conformance rationale:

The TOE is a Root of Trust for a Chip or SoC. It is isolated from other parts of the Chip or SoC and does not share memory with the Chip or SoC.

In addition, only authorized users can load new FW onto the platform, there is no user programmability.

3.3.3 Cryptographic Operation

The platform provides the application with operations, and functionality with algorithms as specified in Specifications, key lengths and modes are described in **Table** 4.

Conformance rationale:

Algorithms	Key lengths (bits)	Modes	Specifications	Usage
AES	128, 192, 256	ECB, CBC, CTR, ICM	NIST FIPS 197 SP800-38A	Encryption, Decryption
	128, 192, 256	CCM	NIST FIPS 197 SP800-38C	Encryption, Decryption
	128, 256	XTS	NIST FIPS 197 SP800-38E	Encryption, Decryption
	128, 192, 256	GCM, GMAC	NIST FIPS 197 SP800-38D	Encryption, Decryption, Authentication
	128, 192, 256	CMAC	NIST FIPS 197 SP800-38B	MAC

Algorithms	Key lengths (bits)	Modes	Specifications	Usage
	128, 192, 256	KWP	NIST FIPS 197 SP800-38F	Key Wrap/Unwrap
	128, 192, 256	CBC-MAC	NIST FIPS 197 SP800-38C	MAC
ECC	P-192, P-224, P-256, P-384, P-521		SP800-56A NIST FIPS 186-5 NIST SP800-186	Key Generation, Key Verification
ECDSA	P-192, P-224, P-256, P-384, P-521		SP800-56A NIST FIPS 186-5 NIST SP800-186	Signature Generation, Signature Verification
ECDH	P-224, P-256, P-384, P-521	one-step KDF using SHA-256	SP800-56A/ C NIST SP800-186	Shared Secret Computation
DH	(1024, 160), (2048, 224), (2048, 256), or (3072, 256)		RFC5114 NIST FIPS 186-4	Key Generation, Key Verification
DH	(1024, 160), (2048, 224), (2048, 256), or (3072, 256)	one-step KDF using SHA-256	SP800-56A/C	Shared Secret Computation
HMAC	112-512	SHA-1	NIST FIPS 198-1 NIST 180-4 NIST FIPS 202	MAC Generation, MAC Verification
	112-512	SHA-224		
	126-512	SHA-256		
	192-1024	SHA-384		
	256-1024	SHA-512		
	112-1152	SHA3-224		
	128-1088	SHA3-256		
	192-932	SHA3-384		
	256-576	SHA3-512		
RSA	n=(1024 to 3072)	RSA-PSS (no CRT)	NIST FIPS 186-5	Signature Verification
	n=(2048 to 3072)	RSA-PSS (no CRT)	NIST FIPS 186-5	Signature Generation
	n=(1024 to 3072)	RSA-PKCS#1v1.5 (no CRT)	NIST FIPS 186-5 PKCS#1	Signature Verification
	n=(2048 to 3072)	RSA-PKCS#1v1.5 (no CRT)	NIST FIPS 186-5 PKCS#1	Signature Generation
KTS-OAEP	n=(1024 to 3072)	RSA-OAEP	SP800-56B	Key Transport Scheme
RSA-KEM	n=(1024 to 3072)	RSA-PKCS#1v1.5 (no CRT)	SP800-56B PKCS#1	Encryption, Decryption
SHA-1		Digest length: 160	NIST FIPS 180-4	Message Digest
SHA-2		Digest length: 224, 256, 384, 512	NIST FIPS 180-4	Message Digest

Algorithms	Key lengths (bits)	Modes	Specifications	Usage
SHA-3		Digest length: 224, 256, 384, 512	NIST FIPS 202	Message Digest
Curve25519	256		RFC 7748 NIST SP800-186	Key Generation, Shared Secret Computation
EdDSA	256		NIST FIPS 186-5 NIST SP800-186	Key Generation, Signature Generation, Signature Verification
ECIES	P-256, P-521	one-step KDF using SHA-256 or SHA-512 + AES256-KWP	SEC 1 ANSI X9.63	Integrated Encryption Scheme (Encryption, Decryption)

Table 4 Crypto Operation

3.3.4 Cryptographic Random Number Generation

The platform provides the application with a way based on DRBG to generate random numbers to as specified in NIST SP800-90A/B/C.

Conformance rationale:

The Deterministic Random Bit Generator is compliant with NIST SP800-90A standard and the Entropy source is compliant with SP800-90B. See [ESV] for certificate details. The RNG system follows SP800-90C (draft).

3.3.5 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in ECC, X25519, EdDSA, AES and HMAC, as specified in [NIST SP800-133r2], and key derivation as specified in [NIST SP800-108r1] and [NIST SP800-56Cr2] for key lengths specified in **Table** 4. .

Conformance rationale:

The TOE supports ECC, X25519, EdDSA key generation through Public Key token ([FW_Manual] section 5.29.1.1). By execution of this command, ECC public key and ECC keypair can be generated.

Users can use token “asset load”-key derivation function to drive keys from a Key Derivation Key according to the MAC based Key Derivation Function. ([FW_Manual] section 5.12)

Users can use token “asset load”- random function to generate AES symmetric keys. ([FW_Manual] section 5.12)

3.3.6 Cryptographic Keystore

The platform provides the application with a way to store cryptographic keys *listed in Table 5* such that not even the application can compromise the *authenticity, integrity, confidentiality* of this data. This data can be used for the cryptographic operations *listed in Table 5.*

Key names	Location	Description	Cryptographic Operation
HUK	OTP	The root key derivation key of the TOE. Immutable, cannot export outside the TOE.	Key Derivation
SFWBCR	OTP	Secure Firmware Boot Confidentiality Root, which is used for unwrapping the AES key for GPFW encryption. Cannot export outside the TOE.	AES (un)wrap
User Defined Keys (e.g. KDK, KEK)	OTP or RAM	Key derived from HUK by users	Key Derivation Key (un)wrap AES encryption

Key names	Location	Description	Cryptographic Operation
User Defined Keys (created via "random")	External Storage	User defined keys can be stored wrapped in external NVM. The (un)wrap operation is performed inside the TOE. User defines whether the key can be exported, and whether it can be exported in plaintext.	AES encryption

Table 5 Cryptographic Keystore

Conformance rationale:

VaultIP stores keys (assets) in OTP and RAM, depending on the usage of the keys. The Host CPU can use the keys according to the asset policy ([FW_Manual] 3.4). Each asset in OTP is CRC-32 protected ([OTP] section 2.3.3).

Confidentiality: Unless required by user, keys are never stored or exported in plaintext. In external NVM, keys are always protected by wrapping in a key blob unless users set keys to be in plaintext, where KEK is stored inside the TOE.

Authenticity: A user/application is required to be authorised/logged in before executing commands that involve sensitive materials (assets). Keys are stored together with information "Ownership", which specifies who may use the asset. The "Ownership" parameter contains both a 32-bit value of application/user id, and a value that identifies the CPU and secure domain. The CPU and secure domain are provided by the hardware.

Only correct user/application on the correct host can use the keys.

Integrity: Each asset in OTP is CRC-32 protected.

Keys can be stored externally in NVM but in this case they are protected by AES encryption (key blob) before being exported from VaultIP. Such keys can be imported in subsequent sessions. (See 3.2.13)

3.4 Additional Security Functional Requirements

3.4.1 Secure Communication Support

The platform provides the application with a secure communication channel.

Conformance rationale:

The security of the communication between the secure processing environment and the VaultIP as trusted subsystem is ensured by the proper physical integration of VaultIP, as required per security objective SW_INTEGRATION and HW_INTEGRATION. All communication between the secure processing environment and VaultIP occurs over the mailbox interfaces and ECI (External Control Interface) which are not directly accessible nor influenceable externally.

3.4.2 Secure Communication Enforcement

The Platform ensures the application can only communicate with the trusted subsystem over a secure communication channel.

Conformance rationale:

The security of the communication between the secure processing environment and the VaultIP as trusted subsystem is ensured by the proper physical integration of VaultIP, as required per security objective SW_INTEGRATION and HW_INTEGRATION. All communication between the secure processing environment and VaultIP occurs over the mailbox interface and ECI (External Control Interface) which are not directly accessible nor influenceable externally. Mailbox interface is used for processing commands and reply, as the main interface for communication. ECI is only used for supporting secure debug functionality by sending authenticated commands. Besides debugging, Mailbox interface is the only way of sending commands to VaultIP. No other, potentially non-secure, communication interface exists.

3.5 Optional Security Functional Requirement

3.5.1 Secure External Storage

The platform ensures that all data stored outside the direct control of the platform, except for public data, is protected such that the confidentiality and integrity is ensured.

Conformance rationale:

Data can be sent outside of the TOE for purpose of persistent storage. All data except for public data is encrypted inside VaultIP before sending outside, utilizing AES-SIV method as specified in [RFC 5297]. See details: [FW_Manual] section 3.7. Token “Symmetric (Un)Wrap” ([FW_Manual] section 5.9) is used for encrypting and decrypting data, using KEK which is located inside the TOE.

3.6 Product Life Cycle

3.6.1 Field Return of Platform

The platform can be returned to the vendor without user data.

Conformance rationale:

User can delete all user data via tokens “select OTP Zeroize and “Zeroize OTP” [FW_Manual] sections 5.34 & 5.35.

3.7 Compliance Functionality

3.7.1 Residual Information Purging

The platform ensures that *temporary data that will not be used anymore,* with the exception of data that will be used later, is erased automatically before the memory is used by the platform or application again and before an attacker can access it.

Conformance rationale:

The TOE automatically deletes temporary or intermediate data from the memory after performing a function. This ensures that all temporary data is deleted and cannot be accessed by an attacker.

3.7.2 Reliable Index

The platform implements a strictly increasing function.

Conformance rationale:

The TOE implements monotonic counters which are stored in OTP. Users can create assets with monotonic counter properties. The counters can be used via token “Monotonic Counter Read” and “Monotonic Counter Increment”. There is a dedicated counter used for anti-rollback of firmware version. This is updated by the “Update RollbackID” token.

HW version is encoded in the HW and is immutable.

4 Mapping and sufficiency rationales

This ST and associated TOE provide exact conformance to SESIP Profile for PSA Certified RoT Component Level 2, aiming at both SESIP certificate and PSA certificate.

4.1 Assurance

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section "Introduction" and "Title"	The ST reference is in the Title, the TOE reference in the "Platform reference", the TOE overview and description in "Platform functional overview and description".
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the operational environment"	The objectives for the operational environment in "Security Objectives for the operational environment" refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section "Security requirements and implementation"	All SFRs in this ST are taken from [SESIP]. "Verification of Platform Identity" is included. "Secure Update of Platform" is included.
	ASE_TSS.1 TOE Summary Specification	Section "Security requirements and implementation"	All SFRs are listed per definition, and for each SFR the implementation and verification is defined in Security requirements and implementation
ADV: Development	ADV_FSP.4	Document [FW_Manual] used to meet this requirement	Complete set of TSF interfaces are well described
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	[FW_Manual] [HW_Manual] [SEC_GUID]	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
	AGD_PRE.1 Preparative procedures	[SW_INT] [HW_INT] [SEC_GUID]	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.

Assurance Class	Assurance Families	Covered by	Rationale
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section “3.1.1”	The flaw reporting and remediation procedure is described.
ATE: Tests	ATE_IND.1 Independent testing: conformance	Functional testing as specified in document [ATE] and additional evaluator testing	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis	Vulnerability assessment is performed by the evaluator	The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.

Table 6 Assurance

4.2 PSA Security Functions Mapping

PSA Security Function	Covered by SESIP SFR	Remark
F.INITIALIZATION	Secure Initialization	Full coverage by the BootFW and GPFW
F.SOFTWARE_ ISOLATION	Software Attacker Resistance: Isolation of Platform	Full coverage by isolating itself with other parts of the SoC.
	~~Software Attacker Resistance: Isolation of Application Parts~~	Not claimed
F.SECURE_ STORAGE	~~Secure Encrypted Storage~~	Not claimed
	~~Secure Storage~~	Not claimed
	~~Secure Encrypted Storage~~	Not claimed
	Secure External Storage	Stored data are encrypted
F.FIRMWARE_ UPDATE	Secure Update of Platform	Full coverage by the BootFW and GPFW
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform	Full coverage by isolating itself with other parts of the SoC.
	Software Attacker Resistance: Isolation of Platform	Full coverage by isolating itself with other parts of the SoC.
	Secure Initialization	Full coverage by the BootFW and GPFW
	Secure Update of Platform	Full coverage by the BootFW and GPFW
F.CRYPTO	Cryptographic Operation	Provides cryptographic algorithms
	Cryptographic KeyStore	Keys are securely stored in OTP and RAM
	Cryptographic Random Number	Provides NIST compliant TRNG

PSA Security Function	Covered by SESIP SFR	Remark
	Cryptographic Key Generation	Keys are securely generated
F.ATTESTATION	Verification of Platform Identity	Provides guidance on how to check system information.
	~~Verification of Platform Instance Identity~~	Not claimed
	~~Attestation of Platform Genuineness~~	Not claimed
	~~Attestation of Platform State~~	Not claimed
F.AUDIT	~~Audit Log Generation and Storage~~	Not claimed
F.DEBUG	~~Secure Debugging~~	Not claimed
Additional security functionality (section 4.4	Secure Communication Support	Only one internal channel could be used for communication.
	Secure Communication Enforcement	Only one internal channel could be used for communication.
	Secure External Storage	Data is encrypted by the TOE and stored outside.
	Field Return of Platform	Support deleting of all user data
	Residual Information Purging	The TOE automatically deletes temporary or intermediate data from the memory after performing a function.
	Reliable Index	The TOE implements monotonic counters which are stored in OTP

Table 7 PSA Security Functions Mapping