RZ/G3S Security Target for SESIP Profile, PSA Certified™ Level 3 RoT Component

Rev 3.1, 2026-8-6

Renesas Electronics Corporation

1 Introduction

The “RZ/G3S Security Target for SESIP Profile, PSA Certified™ Level 3 RoT Component” describes the RZ/G3S platform and the specific properties and capabilities of the platform that have been evaluated for conformance to the SESIP Profile for PSA Certified RoT Component Level 3.
The Security Functional Requirements (SFRs) identified in this Security Target demonstrate the ability of the platforms to act as a Trusted Subsystem to achieve composite certifications such as PSA Certified Level 2 plus Secure Element and PSA Certified Level 3.

1.1 SESIP profile reference

Reference	Value
PP Name	SESIP Profile for PSA Certified Level 3 Version 1.0, GPS_SPE_111
PP Version	1.0
Assurance Claim	SESIP Assurance Level 3 (SESIP3) PSA Certified Level 3 (PSA Certified RoT Component Certification)
SESIP Standard	GP SESIP (GP_FST_070, Public Release v1.2)
Optional and additional SFRs	Mandatory SFRs: Verification of Platform Identity Secure Update of Platform Physical Attacker Resistance Optional SFRs: Verification of Platform Instance Identity Secure Initialization of Platform Cryptographic Operation Cryptographic Random Number Generation Cryptographic Key Generation Cryptographic KeyStore

Table 1 SESIP profile reference

1.2 Platform reference

Reference	Value
Platform Name	RZ/G3S Group
Platform Version	1.0
Platform Identification	Commercial Name: RZ/G3S Group Part Numbers: 1 x Cortex-A55, 2 x Cortex-M33 w/14mm BGA package: R9A08G045S37GBG 1 x Cortex-A55, 1 x Cortex-M33 w/14mm BGA package: R9A08G045S17GBG 1 x Cortex-A55, 2 x Cortex-M33 w/13mm BGA package: R9A08G045S35GBG 1 x Cortex-A55, 1 x Cortex-M33 w/13mm BGA package: R9A08G045S15GBG
	RZ MPU Security Package for RZ/G3S Version 3.2.0.0-update1
Platform Type	General-purpose microprocessor

Table 2 Platform reference

1.3 Included guidance documents

The following documents are included with the platform:

Reference	Name	Version
[UM]	RZ/G3S Group User's Manual: Hardware (R01UH1014EJ0120)	Rev 1.20
[RELNOTE]	RZ/G3S Security Package Release Note (R11UT0114EJ0101)	Rev 1.01
[SUPGUIDE]	RZ/G3S SMARC EVK Security Startup Guide (R11AN1005EJ0101)	Rev 1.01
[LUPGUIDE]	SMARC EVK of RZ/G3S Linux Start-up Guide (R01US0645EJ0106)	Rev 1.06
[SECUM]	RZ/G3S Security Package Security User's Manual (R11AN1006EJ0100)	Rev 1.00
[REPORT]	NIST SP800-90B Entropy Assessment Report for RZ/G3S RSIP Driver (EPMSM-AB-25-0001)	Ver.1.00
[Errata]	RZ MPU Security Package for RZ/G3S Version 3.2.0.0-update1 Errata (EPMSM-AB-26-0006)	Rev.1.00

Table 3 Included guidance documents

[UM] and the RZ MPU Security Package can be downloaded from the Renesas web site (www.renesas.com). [RELNOTE], [SUPGUIDE], [LUPGUIDE] and [SECUM] are included in the RZ MPU Security Package for RZ/G3S Version 3.2.0.0-update1. [REPORT] and [Errata] is provided upon specified user request by Renesas as a reference material.

1.4 Platform functional overview and description

1.4.1 Platform Type

RZ/G3S Group are general purpose MPUs that contain the RSIP-E50B security engine, an on-chip isolated subsystem comprising:

- A cryptographic engine, providing hardware-accelerated cryptography
- A True Random Number Generator
- Dedicated internal RAM, to isolate all operations from the rest of the chip
- A secure key handling mechanism, enabling the secure storage of keys outside the security engine
- An Access Management Circuit, which shuts down the security engine in the event of an illegal access attempt

These security architectures are common specifications for the RZ/G3 series, and RZ/G3S is the product group that forms the foundation of the RZ/G3 series.

1.4.2 Physical Scope

The physical scope of the platform consists of the RZ/G3S Group products as described by [UM].

Figure 1 RZ/G3S Group Block Diagram shows the block diagram of the RZ/G3S Group.

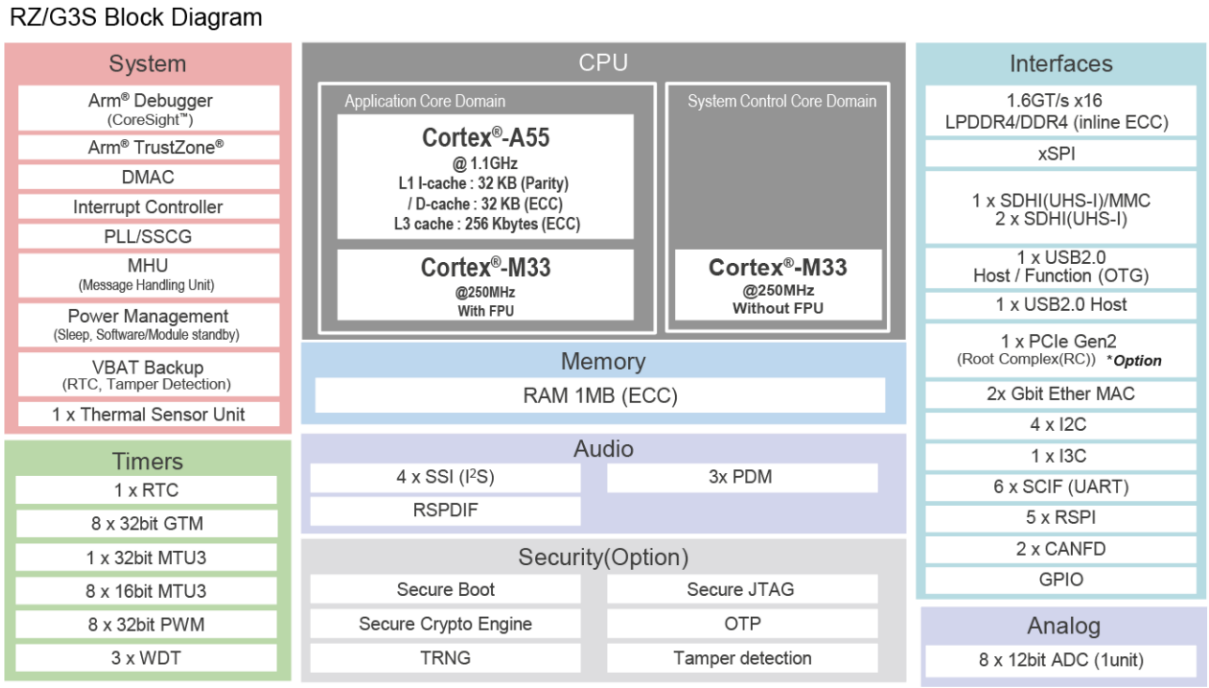


Figure 1 RZ/G3S Group Block Diagram

Figure 2 Platform Evaluation Physical Scope shows the physical scope of the evaluation. The RSIP-E50B security engine contained within the RZ/G3S Group provides the security features listed in section 1.4.1 Platform Type.

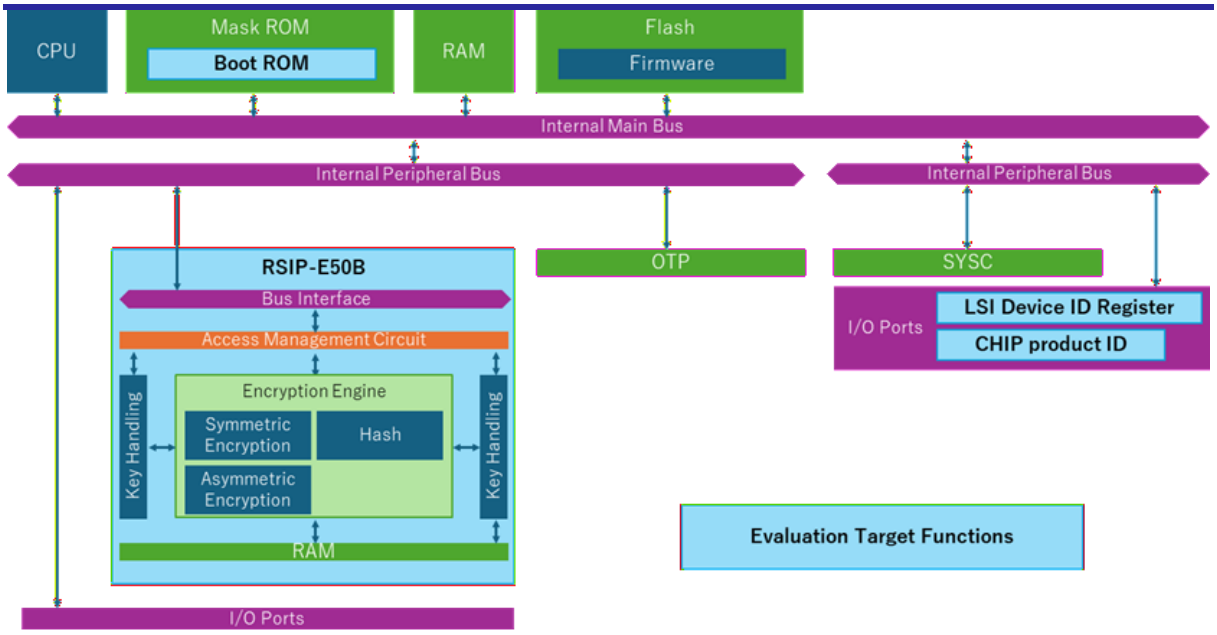


Figure 2 Platform Evaluation Physical Scope

The software to use the platform is provided by the RZ MPU Security Package for RZ/G3S. The TOE scope is depicted in Figure 3 TOE Scope**.** The blue parts are within the evaluation scope, and the grey parts are outside the evaluation scope. Parts within scope are:

- The RSIP-E50B security engine plus on-chip support hardware as shown above
- Security Driver implemented in OP-TEE OS for the RSIP security engine

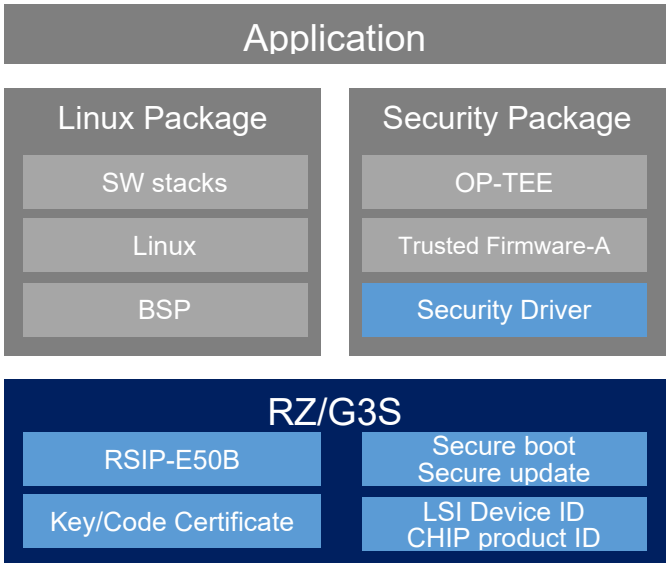


Figure 3 TOE Scope

Guidance documentation for the security driver is included in [SECUM] which is available for public download from the Renesas web site (www.renesas.com).

1.4.3 Logical Scope

The platform includes the following Secure Processing Environment (SPE) PSA-RoT elements:

Immutable Platform Root of Trust:

- LSI Device ID and Chip product ID
- Boot ROM Code in the Mask ROM
- Root of Trust Public Key (RoTPK) Hash in the OTP

Updateable Platform Root of Trust:

- Key Certificate and Code Certificate

1.4.4 Usage and Major Security Features

General description:

The RZ/G3S microprocessor includes an Arm® Cortex®-A55 (1.1GHz) CPU, 16-bit LPDDR4 or DDR4 interface and low-power mode. It also has many interfaces such as PCIe, CAN FD, and 12-bit ADC, making it ideal for applications such as IoT edge applications.

RSIP-E50B as an integrated secure element functionality:

The RZ/G3S Group contains the RSIP-E50B Security Engine. RSIP (Renesas Secure IP) E-type security engines provide secure element functionality integrated into an MCU/MPU/SoC. The security engine is an isolated subsystem inside the chip, managed and protected by dedicated control logic – the Access Management Circuit. The Access Management Circuit will shut down the security engine in the event of improper access via the CPU or the debugger, providing protection against fault injection and Differential Fault Analysis (DFA) attacks. The security engine contains hardware cryptographic accelerators for a wide variety of cryptographic operations, including:

- Symmetric encryption/decryption
- Asymmetric encryption/decryption
- Signature generation and verification
- Key generation (symmetric and asymmetric algorithms)
- CMAC and HMAC functions
- Hash functions
- True Random Number Generation

The cryptographic accelerators include side-channel protections for attacks such as SPA/DPA and timing analysis.

The security engine has its own dedicated internal RAM, enabling all crypto operations to be physically isolated within the security engine, inaccessible by any other bus master or slave. In addition, the security engine supports advanced key handling, with secure application key

storage and usage. Application keys can be stored in wrapped (encryption plus MAC) format with AES-128-CCM mode, wrapped by the chip's Hardware Unique Key (HUK). Since wrapped keys can be unwrapped only by the security engine within the specific chip that wrapped them, the wrapping mechanism provides unlimited, unclonable secure storage of application keys, binding the keys to the specific MPU.

Unique ID:

The platform contains 32 bits LSI Device ID as a platform identifier. This value uniquely identifies the platform. 128 bits CHIP product ID is stored in OTP field and a unique ID for each chip. Also, the Key Certificate and Code Certificate, which are stored in flash ROM and verified and loaded during secure boot, contain 4 bytes of version information. These value uniquely identifies the platform instances.

Secure boot and Secure update:

Boot ROM code in the Mask ROM as a RoT valudates the RoT public key by comparing hash value which is stored in OTP. The RoT public key is used to link the chain of trust and the boot ROM code verifies the signatures on the Key Certificate and Code Certificate with ECDSA NIST P-256 with SHA2-256. The Code Certificate contains the hash value of the firmware image, and the integrity of the firmware is verified by comparing the hash value of the firmware image. The Key Certificate and Code Certificate are updatable parameters, and after updating, the parameters are similarly verified via the Secure Boot procedure.

1.4.5 Required Hardware/Software/Firmware

No additional hardware, software, or firmware are required to utilize the platform.

2 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.	The platform user must setup OTP fields and install keys and certificates according to [SECUM] section 3.5, and [SUPGUIDE] section 2.1.5. Therefore, the key provisioning process is out of scope of this evaluation. The platform user must setup Wrapped Keys according to [SECUM] section 3.4, and [SUPGUIDE] section 9.3.
TRUSTED_USERS	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	The RSIP-E50B driver should be implemented in the SPE. The platform user must configure the peripheral security attribution correctly to place the security engine in the SPE, as per [SECUM] section 5.3.1.
UNIQUE_ID	The integrity and uniqueness of the unique identification of the platform must be provided by the platform user during the personalization stage.	As per [UM] section 6.3.62 and described in 3.2.1 Verification of Platform Identity, the platform's unique ID is provisioned as part of the Renesas manufacturing process. Also, the platform's instance unique ID is provided as part of the Renesas manufacturing process as per [SECUM] section 3.5.3 and described in 3.2.2 Verification of Platform Instance Identity.

Table 4 Security Objectives for the Operational Environment

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is **SESIP3**.

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 report flaw and generate any needed update and distribute it, the developer has defined the following procedure:

Renesas has a dedicated team that is responsible for the overall management of monitoring, investigating, and communicating security issues. Renesas PSIRT (Product Security Incident Response Team) operates as an independent unit with assigned window persons for every Renesas business unit, to ensure that internally and externally identified security vulnerabilities are captured, communicated, and addressed across all Renesas groups and any affected customers.

The publicly available interface can be accessed via www.renesas.com/psirt, whereby individuals and/or companies outside Renesas can securely submit vulnerability reports through a dedicated email address (renesas_psirt@lm.renesas.com) using PGP encryption.

Once a vulnerability has been entered into the system, from either the public interface or internally, internal Renesas operating procedures for corrective action of security incidents and vulnerabilities govern the processing of the vulnerability. This process includes the following steps:

- Reporting the security issue – Security issues can be reported for PSIRT processing via the external web/email interface, from Renesas internal product design teams via the PSIRT window persons, or by PSIRT members directly. If the external report is received from a Renesas customer, Renesas QAD (Quality Assurance Division) will also be involved in the ensuing communications.
- Investigating the security issue – PSIRT confirms the existence, reproducibility, and threat assumptions in the report. Once confirmed, PSIRT works closely with the relevant product design team(s) to ensure that addressing the security issue is given appropriate priority, with consideration given to the scope of the affected product(s), the seriousness of the vulnerability, and the feasibility of an attack.
- Taking actions for the security issue – The product design team works with PSIRT to determine a corrective action plan. If the issue is software-related, updated software and user manual, security manual, and/or other equivalent documentation is created for distribution to customers. If the issue is silicon-related, the corrective action most likely will require a new product revision. Until the revision update is performed, usage restrictions and recommendations will be added to the user manual, security manual, and/or other equivalent documentation.
- Notifying the customer – The product design team creates a corrective action plan, which includes a plan of action, notification of interested parties both internal and

external to Renesas, and completion schedule. Depending on the production status and origin of the vulnerability report, either the product design team or PSIRT will handle communication with the report originator. For any issues in released products that affect Renesas customers, Renesas QAD will serve as the main point of contact to ensure that Renesas customers are informed of the vulnerability and can appropriately address the issue in their end products.

3.2 Base PP Security Functional Requirements

As a base, the platform fulfills 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 contains LSI Device ID, e.g., RZ/G3S rev1.0 and so on, that is a 32-bits register field as described in [UM] section 6.3.62. 31 to 28 bit indicates the product version, and 27 to 0 bit indicates the product specific fixed value.

3.2.2 Verification of Platform Instance Identity

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

Conformance rationale:

The platform contains CHIP product ID that is a read only 128 bits register field as described in [UM] section 6.3.63 LSI Product Register. CHIP product ID is a unique ID for each chip set in Renesas. Initial value is specific on each chip. That field is written as part of the production process, and the production testing procedures verify the value has been written correctly.

3.2.3 Secure Initialization of Platform

The platform ensures its authenticity and integrity during the platform initialization.

Conformance rationale:

Boot ROM Code in the mask ROM as the first stage bootloader (BL1) is executed immediately after reset. Boot ROM Code executes Initial Program Loader (IPL) as the second stage bootloader (BL2) after confirming the integrity.

Renesas provides sample codes for IPL to confirm integrity any bootloader as the third stage bootloaders (BL3x) with verification function. However, those sample codes are not within scope of this evaluation because the implementation of BL2 and above is up to the user. Our sample IPL Secure Boot confirms the integrity of the program image by verifying signature of BL3x with the public key, as described in [SECUM] section 3.1. Also, encryption with common key is supported for program protection as option.

The process for enabling the security features of RZ/G3S and transitioning the product to a secure state is called “Provisioning”. User should perform the Provisioning process in appropriately to secure the product at the product development stage and the manufacturing stage, as described in [SECUM] section 3.5. That includes secure installation procedures for the public key used for program signature verification and the common key for program decryption. These setups are part of the operational environment as described in 2 Security Objectives for the operational environment and are not within scope of this evaluation.

If the initialization fails at any steps, the boot process enters failsafe mode immediately and waits for program image download from SCIF. The program image downloaded from SCIF is also subject to Verification Function in the Mask ROM.

3.2.4 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 firmware image is verified by the Image Signing Public Key in Code Certificate and a hash of this key is stored in Key Certificate. Key Certificate is verified by RoT PK and a hash of RoT PK is stored in OTP as an immutable RoT as shown in [SECUM] section 3.1. Users can update Key Certificate and Code Certificate includes firmware image which are stored in the external flash memory. These updated Certificates and firmware are verified by the boot ROM inside the Mask ROM during the boot sequence using the Chain of Trust originating from the RoT PK according to the procedure described in 3.2.3 Secure Initialization of Platform.

To prevent rollback, the current firmware version is recorded in OTP. The version number embedded in the updated firmware’s certificate is compared against the version stored in OTP as shown in [SECUM] section 3.1.

3.2.5 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.

Conformance rationale:

The platform provides resistance to physical attacks by incorporating protections for both side-channel attacks and fault injection attacks.

SPA/DPA protections for AES operations are provided using masking techniques. PKI operations (i.e. RSA and ECC operations) are protected against timing attacks. The effectiveness of these protections is verified by both simulation and by physical testing of the silicon.

The entire security engine operation is protected against fault injection attacks by the Access Management Circuit, shown in Figure 2 Platform Evaluation Physical Scope. The Access Management Circuit will shut down the RSIP-E50B in the event of improper access via the

CPU or the debugger. A reset is required if you intend to use the RSIP-E50B again. Multiple verifications to confirm correct sequential operation are conducted during each cryptographic operation, providing protection against fault injection and Differential Fault Analysis (DFA) attacks.

3.2.6 Cryptographic Operation

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

Algorithm	Operations	Specification	Key lengths	Modes
AES	Encryption, decryption, MAC	NIST FIPS PUB 197 NIST SP800-38A (ECB, CBC, CTR) NIST SP800-38B (CMAC) NIST SP800-38D (GCM) IEEE 1619-2007 (XTS)	128, 256 bits	ECB, CBC, CTR, XTS, GCM, CMAC
RSA	Public-key encryption, private-key decryption	IETF RFC 8017 FIPS PUB 186-4	1024, 2048, 3072, 4096 bits	N/A
ECC	Signature generation, signature verification	FIPS PUB 186-4 FIPS PUB 186-5	Curves: NIST P-192, P-224, P-256; Brainpool P-256r1	N/A
Hash	SHA	FIPS PUB 180-4	N/A	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
	MAC	FIPS PUB 198	N/A	HMAC-SHA1, HMAC-SHA224, HMAC-SHA256

Table 5: Cryptographic Operations

Conformance rationale:

The above crypto operations are supported by the RSIP-E50B, as documented in [UM] section 43. However, the driver software only supports limited crypto operations of the RSIP-E50B. The driver software provided in RZ MPU security package supports the cryptographic operations shown in Table 5 as documented in [SECUM] section 3.4.

The Boot ROM Code confirms the initial program loader (IPL) integrity by verifying a signature with ECDSA NIST P-256 with SHA-256 as described in 3.2.3 Secure Initialization of Platform. As an option, IPL can be encrypted with AES-128-CBC mode.

The platform provides the Secure IP driver as described in [SECUM] section 5.3.1 for OP-TEE OS as a referenced sample to enable access to cryptographic functions provided by the

Secure IP. The driver's interface specification requires the caller to input an initialization vector for AES encryption; inputting specific values could compromise randomness. To prevent that, a random number generated by the SPE must be inputted to the interface. As indicated in [Errata], guidance regarding that will be provided in an updated version of [SECUM].

3.2.7 Cryptographic Random Number Generation

The platform provides a way based on *thermal noise* to generate random numbers to as specified in SP800-90A.

Conformance rationale:

The random number generation is designed based on NIST SP800-90A CTR_DRBG; the initial seed utilizes an entropy source derived from thermal noise, and bit strings are generated using the algorithm specified for CTR_DRBG. Compliance of this implementation has been confirmed through CAVP verification as certified as A7803.

3.2.8 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.

Conformance rationale:

The following table identifies the cryptographic key types and key lengths that can be generated by the RSIP-E50B.

Algorithm	Specification	Key lengths
AES	NIST FIPS PUB 197	128, 256 bits
RSA	FIPS PUB 186-4 Appendix B.3.3	1024, 2048, 3072 bits
ECC – SEC and Brainpool prime curves	FIPS PUB 186-4 FIPS PUB 186-5	192, 224, 256 bits

Table 6: Cryptographic Key Generation

3.2.9 Cryptographic KeyStore

The platform provides a way to store *the cryptographic keys* such that not even the application can compromise the *authenticity, integrity and confidentiality* of this data. This data can be used for the cryptographic operations listed in 3.2.6 Cryptographic Operation.

Conformance rationale:

Cryptographic operation key handling with RSIP-E50B:

Unlimited secure key storage is provided by the secure key handling mechanism of the RSIP-E50B. Secure keys used for the cryptographic operations listed in 3.2.6 Cryptographic Operation are stored in wrapped format, ensuring authenticity, integrity, and confidentiality by using AES with a unique 128-bit key derived from the hardware unique key (HUK). By

leveraging the HUK, this mechanism binds the wrapped key to the specific chip that wrapped it. The HUK is not used directly in order to protect the HUK from exposure.

Once a key is wrapped, its plaintext cannot be exposed outside the RSIP-E50B - the HUK is accessible only by the RSIP-E50B, and the unwrapped key is handled only in the dedicated internal RAM within the RSIP-E50B.

There is no need to install plaintext on the RSIP-E50B to wrap secure keys with HUK. Secure keys can be sent to the RSIP-E50B encrypted using the Key Update Key (KUK) that is a 256-bit symmetric key. The RSIP-E50B will decrypt the secure keys using the provisioned KUK and then wrap them with HUK.

Secure boot and secure update key handling:

There are three types of keys used in the Mask ROM Verification Function described in 3.2.3 Secure Initialization of Platform and 3.2.4 Secure Update of Platform:

- Root of Trust Public Key (RoT PK)
- Image Signing Public Key
- Image Decryption Key

RoT PK is stored in a Key Certificate stored at a specified address in the loader program in the external flash memory for booting. Key Certificate specification is shown in [SECUM] section 3.1, and loader program allocation is shown in [UM] section 4.1.
RoT PK is the key for signature verification of ECDSA NIST-P256 with SHA2-256 for Key Certificate signature. Before verification, RoT PK hash with SHA2-256 is calculated and compered with RoT PK Hash stored in OTP, so RoT PK is immutable parameter as Root of Trust.

Image Signing Public Key is also stored in a Code Certificate stored at a specified address in the loader program in the external flash memory for booting. Code Certificate specification is also shown in [SECUM] section 3.1. Image Sining Public Key is used for verification for the signature of loader program image. Before verification, Image Singing Public Key hash with SHA2-256 is calculated and compered with the public key hash stored in Key Certificate. Key Certificate can be updated, so Image Signing Public Key is updatable. The authenticity and integrity of Key Certificate is verified using RoT PK through secure boot process.

Image Decryption Key is wrapped by the RSIP-E50B as described in above and stored in OTP. The loader program can be encrypted with this key using AES-128-CBC mode as option.

-

4 Mapping and sufficiency rationales

4.1 Assurance

Assurance Class	Assurance Family	Covered by
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	1 Introduction and title page of this security target.
	Rationale: The ST reference is in 1.1 **SESIP profile reference**, the TOE reference in 1.2 Platform reference, the TOE overview and description in 1.4 Platform functional overview and description.	
	ASE_OBJ.1 Security requirements for the operational environment	2 Security Objectives for the operational environment
	Rationale: The objectives for the operational environment in **2 Security Objectives for the operational environment** refers to the guidance documents.	
	ASE_REQ.3 Listed Security requirements	3 Security requirements and implementation
	Rationale: All SFRs addressed by the TOE and described in **3 Security requirements and implementation** are listed in 1.1 **SESIP profile reference**.	
	ASE_TSS.1 TOE Summary Specification	3 Security requirements and implementation
	Rationale: All SFRs are listed per definition, and for each SFR the implementation and verification are defined in 3.2 **Base PP Security Functional Requirements**.	
ADV: Development	ADV_FSP.4 Complete functional specification	• [SECUM] • [UM]
	Rationale: [SECUM] contains the functional specification of the RSIP-E50B and driver software.	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	• [SECUM] • [SUPGUIDE] and the source code
	Rationale: [SECUM] contains the mapping of the implementation of the TOE Security Functions to the SFRs described in the relevant sections of this security target. The source code of RZ MPU security Package for RZ/G3S downloaded by following [SUPGUIDE] is available in clear text, which can be mapped directly to the hardware registers used to implement the SFRs.	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	• [SECUM] • [UM]
	Rationale: [SECUM] and [UM] describe the operation of the platform and how to use the platform to create an end application.	
	AGD_PRE.1 Preparative procedures	• [SECUM] • [UM] • [SUPGUIDE]
	Rationale: [SECUM], [UM] and [SUPGUIDE] describe how to prepare the platform as part of an end-product.	

Assurance Class	Assurance Family	Covered by
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	• [SECUM] • [UM]
	Rationale: The presence of the RSIP-E50B is determined by the definition of [UM]. The complete part number, including product group, is typically available on the silkscreen of the chip and available via the mechanisms described in 3.2.1 Verification of Platform Identity. Application-level software support to utilize the RSIP-E50B is described in the [SECUM].	
	ALC_CMS.1 TOE CM Coverage	• [UM]
	Rationale: [UM] specifies the presence (or lack) of the RSIP-E50B. Modification of a component of the RZ/G3S will be reflected in the version of the part number described in 3.2.1 Verification of Platform Identity. The complete manifest of RZ/G3S contents is maintained by Renesas in accordance with internal design process requirements.	
	ALC_FLR.2 Flaw reporting procedures	3.1.1 Flaw Reporting Procedure (ALC_FLR.2)
	Rationale: The flaw reporting and remediation procedure is described in 3.1.1 Flaw Reporting Procedure (ALC_FLR.2).	
ATE: Tests	ATE_IND.1 Independent testing: conformance	N/A
	Rationale: The evaluator will perform independent testing.	
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis	N/A
	Rationale: The evaluator will perform penetration testing.	

Table 7 Assurance Mapping and Sufficiency Rationales

5 Version history

Rev	Description	Date
1.0	First release	2025-12-12
1.1	Modified “1.1 SESIP profile reference”	2026-1-27
1.2	Added or corrected explanations based on review feedback from the evaluation laboratory	2026-2-27
2.0	Updated “1.4.4 Usage and Major Security Features” according to mentions in SFRs. Updated “2 Security Objectives for the operational environment” to assume the provisioning process is performed as key installation procedure. Moved the description about firmware version from “3.2.1 Platform Identity” to “3.2.2 Platform Instance Identity”.	2026-3-6
2.1	Modified or corrected explanations based on review feedback from the evaluation laboratory and the certification body.	2026-4-28
2.2	Modified or corrected explanations based on review feedback from the evaluation laboratory and the certification body.	2026-6-29
3.0	Modified Figure 2 according to SFR explanations. Added the Errata into guidance documents and its explanation to 3.2.6. Cryptographic Operation.	2026-7-13
3.1	Updated the description in Section 3.2.4, Secure Update of Platform. Updated Table 5 in Section 3.2.6, Cryptographic Operation. Updated Table 6 in Section 3.2.8, Cryptographic Key Generation.	2026-8-6