Security Target for RZ MPU

Rev 1.6, 2023-06-13

Renesas Electronics Corporation

1 Introduction

The Security Target describes the Platform (in this chapter) and the exact security properties of the Platform that are evaluated against GlobalPlatform Technology Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.1 (in chapter “Security requirements and implementation”) that a potential consumer can rely upon the product upholding if they fulfill the objectives for the environment (in chapter “Security Objectives for the operational environment”).

1.1 SESIP profile reference

Reference	Value
PP Name	SESIP Profile for PSA Certified Level 2
PP Version	V1.0 REL 01
Assurance Claim	SESIP Assurance Level 2 (SESIP 2)
Optional and additional SFRs	N/A

Table 1 SESIP profile reference

1.2 Platform reference

Reference	Value	
Platform Name	RZ/G2L, RZ/G2LC, RZ/G2UL and RZ/V2L	
Platform Version	1	
Platform Identification	Chip name and version	RZ/G2L: R9A07G044L17GBG, R9A07G044L27GBG, R9A07G044L18GBG, R9A07G044L28GBG RZ/G2LC: R9A07G044L16GBG, R9A07G044L26GBG RZ/G2UL: R9A07G043U15GBG, R9A07G043U16GBG RZ/V2L: R9A07G054L17GBG, R9A07G054L27GBG, R9A07G054L18GBG, R9A07G054L28GBG
	PSA-RoT name and version	Security Package for RZ MPU v1.1
Platform Type	General-purpose Microprocessors with Arm® Cortex®-A55 CPUs	
Trusted Subsystem Identification	Security IP, an inner component common to all of these platform	
Trusted Sub-system Certification	N/A	

Table 2 Platform reference

1.3 Included guidance documents

The following documents are included with the platform:

Reference	Name	Version
R01AN6346EJ	Security Package for RZ MPU Security User's Manual	Rev 3.1
R01UH0914EJ	RZ/G2L Group, RZ/G2LC Group User's Manual: Hardware	Rev 1.10
R01UH0936EJ	RZ/V2L Group User's Manual: Hardware	Rev 1.10
R01UH0968EJ	RZ/G2UL Group User's Manual: Hardware	Rev 1.00
R01US0553EJ	RZ/G Verified Linux Package Version 3.0.0-update1 Release Note	Rev 1.03
R01US0565EJ	RZ/V Verified Linux Package Version 3.0.0 Release Note	Rev 1.01
R11AN0556EJ	RZ/G2L and RZ/G2LC SMARC EVK Security Start-up Guide	Rev 1.21
RZ_SCE_Driver_Usage	RZ_SCE_Driver_Usage.rst* *This document is published on "renesas-rz" repository in Github - RZ_SCE_Driver_Usage	3.17/rz

Table 3 Included guidance documents

1.4 (Optional) Other Certification

The product has previously been evaluated following PSA Level one:

Scheme	PSA Certified Level One
Certification body	TrustCB
Certification number	0716053550439-10101
Certificate date	2022-06-08

Table 4 Other certification

1.5 Platform functional overview and description

1.5.1 Platform Type

General-purpose Microprocessors with Arm® Cortex®-A55 CPUs with Security IP and TrustZone® technology.

1.5.2 Physical Scope

The RZ/G2L microprocessor includes a Cortex®-A55 (1.2 GHz) CPU, 16-bit DDR3L/DDR4 interface, 3D graphics engine with Arm® Mali-G31 and video codec (H.264). It also has many interfaces such as camera input, display output, USB 2.0, and Gbit-Ether, making it ideal for applications such as entry-class industrial human-machine interfaces (HMIs) and embedded devices with video capabilities.

Based on RZ/G2L, we have a lineup of general-purpose MPUs with excellent compatibility that allow customers to select the appropriate model for their application. They are RZ/G2LC which is a model without Video Codec Engine, RZ/G2UL which is a Single-Core model without 3D graphics, and RZ/V2L which is a model equipped with AI-Dedicated Accelerator.

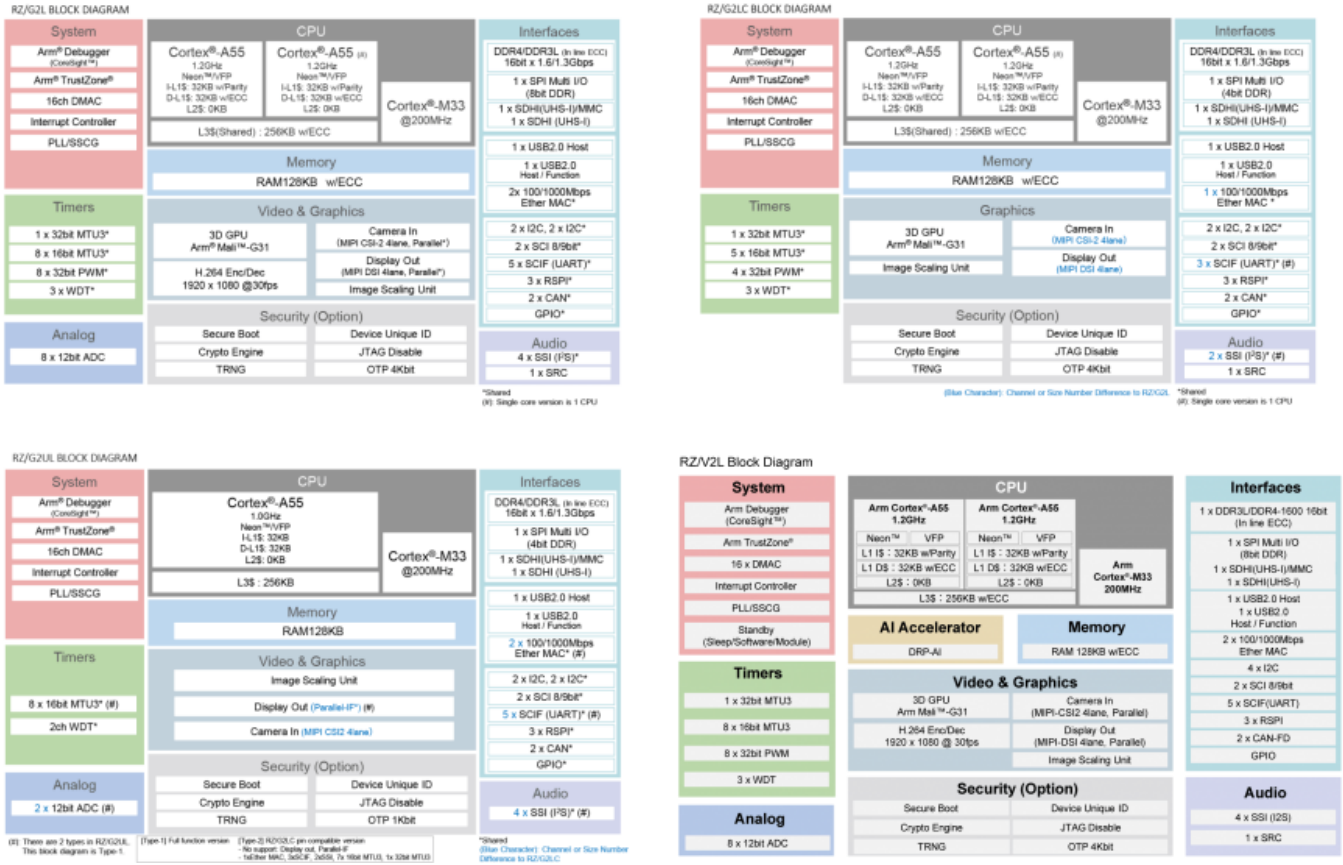

Figure 1 RZ/G2L, RZ/G2LC, RZ/G2UL and RZ/V2L Block Diagram

These chips have two types of devices, security devices and normal devices to meet the security requirements in the current industrial products. The normal device cannot work security features. Security features are provided by Security IP named as “Trusted Secure IP” in the guidance documents and ARMv8 Cryptography Extensions. The Security Package for RZ MPU targets the security device of all these chips and only security devices are identified as platform in Table 2 Platform reference.

The TOE scope is depicted in Figure 2 TOE scope. The blue parts are within the evaluation scope and the gray parts are outside of the evaluated scope. The out of scope part comprises the Security Package for RZ MPU. Guidance documentation for the RZ MPU is listed in section 1.3 Included guidance documents and is available for public download from the Renesas web site (www.renesas.com).

The physical scope includes only the RZ MPU itself, with the functional blocks identified in Figure 1 RZ/G2L, RZ/G2LC, RZ/G2UL and RZ/V2L Block Diagram.

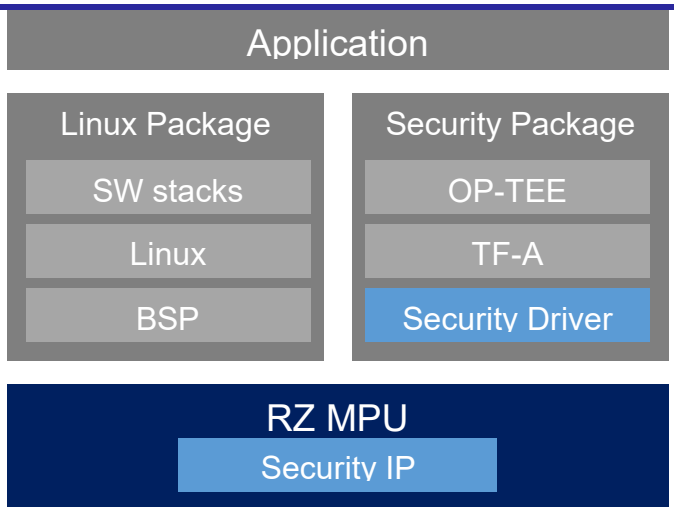

Figure 2 TOE scope

1.5.3 Logical Scope

The logical scope includes the hardware and software interfaces necessary for the application and platform software to utilize the hardware. The Security Package includes reference implementation of Trusted Firmware-A and OP-TEE as samples, not only the driver for the security IP. Cryptographic functions, such as encryption/decryption, hashing, secure cryptographic key handling, and random number generation, and also secure boot are performed by the security IP, shown in Figure 2 TOE scope. Security features of the security IP can be executed by calling Security Driver functions via APIs that are reference-implemented in OP-TEE OS. These features are described in detail in "RZ_SCE_Driver_Usage" listed in section 1.3 Included guidance documents.

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

Immutable Platform Root of Trust:

The immutable Platform RoT is provided by Security IP and OTP. A hash of the RoT Public Key (ROTPK) is stored in OTP. The boot ROM inside the mask ROM extracts the ROTPK from the signed certificate stored in Non-Volatile Memory (NVM) and passes it along with the hash read from the OTP to the security IP. The security IP calculates and compares the hash of the ROTPK in detail in 3. Secure Boot in R01AN6346EJ listed in section 1.3 Included guidance documents. The platform relies on Cortex®-A55 which supports TrustZone®. The SPE is executed in secure mode. Security IP and OTP is also set secure mode so that it cannot be accessed from Non-Secure Processing Environment (NSPE). The SPE can only access them via dedicated driver software in the Security Package.

Updateable Platform Root of Trust:

Updateable Platform RoT is provided for verification procedure of manifest data performed in the boot ROM. Manifest data is signed certificates stored in NVM. There is a code certificate with the public key for firmware (IMGPK) and a key certificate with ROTPK and a hash of IMGPK. The verification procedure starts with ROTPK verification and sequentially verifies up to the integrity of the firmware to achieve Chain of Trust (CoT) in detail in 3. Secure Boot in R01AN6346EJ listed in section 1.3 Included guidance documents.

Trusted Subsystem:

The platform incorporates the Security IP module to provide security functions. The module consists of an access management circuit, encryption engine, and random number generator. In combination with the Security IP driver, the Security IP can prevent eavesdropping (confidentiality), falsification of information (integrity), and impersonation (authenticity). Key information to be used in encrypting and decrypting data is only stored within the Security IP, and any external access can be shut out to obtain a system with strong security in detail in 45. Trusted Secure IP in R01UH0914EJ listed in section 1.3 Included guidance documents.

1.5.4 Usage and Major Security Features

The platform consists of unique hardware security features designed to enable best-in-class security for a broad range of connected devices.

The platform is intended to be used by product developers who need to protect valuable assets from a wide range of remote and physical attacks.

The main security features of the platform are as follows:

- Access Control
- Secure Boot
- Security Life Cycle
- Cryptographic function

Those features are described in SFRs, and usage is written in R01AN6346EJ listed in section 1.3 Included guidance documents.

1.5.5 Required Hardware/Software/Firmware

N/A

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.

- The end product developer shall ensure that the MPU is configured in the appropriate DLM state for the specific stage of the product's life cycle, as described by section 1.2 Device Life Cycle in R01AN6346EJ listed in section 1.3.
- The end product developer shall ensure that TrustZone® and the device MPUs are configured correctly for the application's memory isolation requirements, as described in section 4. Access Control in R01AN6346EJ listed in section 1.3.
- The end product developer shall ensure that TrustZone® and the device MPUs are configured correctly for the application's peripheral and pin isolation requirements, as described in section 4. Access Control in R01AN6346EJ listed in section 1.3.
- For optimal key protection, the end product developer shall install any externally-generated keys as per section 2. Provisioning in R01AN6346EJ listed in section 1.3.
- The end product developer performing the provisioning process described in section 2.1 Overview of Provisioning and 2.4 Key Wrap Service in R01AN6346EJ listed in section 1.3 must be trusted. Key wrap service provided by Renesas shown in the above section is trusted and operated in a security room which strictly controlled entry and exit.
- The integrity and uniqueness of LSI Device ID shown in section 6.3.42 LSI Device ID Register (SYS_DEVID) in R01UH0914EJ and CHIP product ID shown in section 2.2.2.1 CHIP product ID in R01AN6346EJ listed in section 1.3 as the unique identification of the platform are provided by Renesas. These fields are written as part of the production process, and the production testing procedures verify the values have been written correctly.

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is **SESIP2** as described in Section 4.1.

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 give 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.

The silicon and built-in factory programming bootloader of the platform cannot be updated or patched. However, a secure boot solution can be implemented in firmware that can verify the integrity and authenticity of the code running on the platform as well as any application updates. The update mechanism must be implemented by the customer. Renesas provides a sample implementation and works with multiple third-party partners to enable their security solutions to run on the Renesas platform. Those mechanisms are not within scope of this evaluation.

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/G2L rev1.0 and so on, that is a 32 bits register field as described in 6.3.42 LSI Device ID Register (SYS_DEVID) in R01UH0914EJ listed in section 1.3. 31 to 28 bit indicates the product version, and 27 to 0 bit indicates the product specific fixed value.

The platform contains Manifest Version that is a 4 Bytes field in the header field of each manifest data both of Key Certificate and Code Certificate, as described in 3.2 Manifest Specification in R01AN6346EJ listed in section 1.3. In addition, Code Certificate contains Image Version that is 4 Bytes field in the header field. Those value is referred from Boot ROM code and should be set appropriately by end product developers.

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 and their versions.

Conformance rationale:

The platform contains CHIP product ID that is a 64 bits OTP field. CHIP product ID is a unique ID for each chip set in Renesas. Initial Value depends 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 Attestation of Platform Genuineness

The platform provides an attestation of the “Verification of Platform Identity” and “Verification of Platform Instance Identity”, in a way that ensures that the platform cannot be cloned or changed without detection.

Conformance rationale:

The platform has Hardware Root Key (HRK) as shown in 2. Provisioning in R01AN6346EJ listed in section 1.3. The HRK is unique for each product and is written into access-controlled area in Security IP at the Renesas’ foundry and it is used to wrap User Factory Programming Key (UFPK) as shown in the above section. Renesas wraps the UFPK in Renesas site and sends the wrapped UFPK (W-UFPK) to the end product developer by PGP encryption email. The end product developer uses Security IP to unwrap the W-UFPK by the HRK. If unwrapping is failed, the end product developer can detect it is cloned or changed. Also, the end product developer can read platform identification shown in 3.2.1 Verification of Platform Identity and 3.2.2 Verification of Platform Instance Identity. These identifiers help to find the product is genuineness.

3.2.4 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 go to suspend boot.

Conformance rationale:

Boot ROM Code in the mask ROM is executed immediately after reset. Boot ROM Code executes Initial Program Loader (IPL) after confirming the integrity using Verification Function in the mask ROM. Each program executed by IPL can also be confirmed for integrity with Verification Function. Secure Boot confirms the integrity of the program image by verifying signature with the public key, as described in 3. Secure Boot in R01AN6346EJ listed in section 1.3. Also, encryption with common key is supported for program protection as option.

The process for enabling the security features of RZ MPU 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 2. Provisioning in R01AN6346EJ listed in section 1.3. That includes secure installation procedures for the public key used for program signature verification and the common key for program decryption.

3.2.5 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.

Conformance rationale:

The platform state is described in 1.2 Device Life Cycle in R01AN6346EJ listed in section 1.3. The initial state of the chip is “Chip Manufacture (CM)”. When Renesas manufactures the chip, Renesas then sets the chip as either:

- the normal chip: setting the state to "Security Disable (SD)",

- security chip: setting the state to "Device Manufacture (DM)",

depending on the device manufacturer request. This setting is set by bonding i.e., hardware is fixed to either one state and cannot be changed by software after setting.

A chip set to "Security Disable (SD)" state will not activate the Security IP. Security IP can be used on the chip set to "Device Manufacture (DM)" state, but to use security functions such as Secure Boot, a specific field of OTP (i.e. "Secure Boot enable") must be enabled. The OTP is configured by device manufacturers, and the state where the security function is configured enable by OTP is the state "Security Enable (SE)". Only in this state, the Boot ROM Code executes the Secure Boot.

Since state update is operated by bonding and OTP configuration, the parameters cannot be changed once they are set. And, the parameters that determine SD or DM, and DM or SE are just a bit and have no other value.

~~3.2.6 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.~~

The platform does not support the update or patching of hardware nor internal boot firmware. It does offer features that enable a customer to implement secure update mechanisms for the own code. Justification for why this platform does not support secure updates is provided as part of section 3.1.1 Flaw Reporting Procedure (ALC_FLR.2) in this document.

3.2.7 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.

Conformance rationale:

The platform contains an Arm® Cortex®-A55 core based on the Armv8-A architecture with Arm® TrustZone® technology. TrustZone® allows the application developer to isolate assets and services in a Trusted region, with Untrusted code only able to utilise those services that have been explicitly made available for use.

3.2.8 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.

Conformance rationale:

The platform contains an Arm® Cortex®-A55 core based on the Armv8-A architecture with Arm® TrustZone® technology. TrustZone® allows the application developer to isolate assets and services in a Trusted region, with Untrusted code only able to utilise those services that

have been explicitly made available for use. Security IP and OTP that make up PSA-RoT are separated from the application RoT service by setting the security attribute to secure mode.

3.2.9 Cryptographic Operation

The platform provides the application with the following functionality with the specified algorithms as specified in relevant specifications for key lengths and modes shown in below.

AES: Compliant with NIST FIPS PUB 197 algorithms

- Key sizes: 128, 192, or 256 bits
- Block sizes: 128 bits
- Block cipher mode of operation
  - ECB, CBC, CTR: Compliant with NIST SP 800-38A section 6.1, 6.2 and 6.3
  - CMAC: Compliant with NIST SP 800-38B section 5.2
  - CCM: Compliant with NIST SP 800-38C section 6
  - GCM: Compliant with NIST SP 800-38D section 5.1
  - XTS: Compliant with NIST SP 800-38E
  - GCTR: Compliant with NIST SP 800-38D section 6.5

RSA: Compliant with FIPS PUB 186-4 section 5

- Key sizes: Up to 4096 bits
- Block sizes: Up to 4096 bits

HASH: Compliant with FIPS PUB 180-4

- Support for SHA1, SHA224/SHA256, GHASH
- Block sizes: 512 bits

ECC

- Compatible with ECDSA(FIPS PUB 186-4 section 6) and ECDH(NIST SP800-56A section 5.7)
- Data block length: 256 bits

Conformance rationale:

The above cryptographic operations are supported by the Security IP. Algorithms that can actually be used by applications are limited to the following according to driver specifications described in the "RZ_SCE_Driver_Usage" listed in section 1.3.

AES

- ECB 128/256bit
- CBC 128/256bit
- CTR 128/256bit

RSA

- RSAES-PKCS1-V1_5 1024/2048bit
- RSAES-PKCS1-V1_5 4096bit (Encryption only)
- RSASSA-PKCS1-V1_5 1024/2048bit
- RSASSA-PKCS1-V1_5 4096bit (Verification only)

ECC

- ECDSA secp192r1/secp224r1/secp256r1/BrainpoolP512r1

Hash Functions

- SHA-2 (SHA-256/224)

Message Authentication Code

- AES-CMAC 128/256bit

3.2.10 Cryptographic Random Number Generation

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

Conformance rationale:

The platform implements random number generation by utilising the True Random Number generation capability of the Security IP. The TRNG implementation consists of an SP800-90A referenced DRBG that is fed by an SP800-90B referenced seed, which is generated from an SP800-22 rev.1A validated entropy source. Each TRNG request generates a 128-bit or 256-bit random number.

3.2.11 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in *AES* as specified in *NIST FIPS PUB 197* for key lengths *128 and 256 bits*.

Conformance rationale:

AES key generation is performed by creating a random number consisting of the required number of bits to act as the encryption/decryption key capability is described in detail in section 3.2.10 Cryptographic Random Number Generation. Each TRNG request generates a 128-bit random number. Keys of lengths greater than 128-bits are created by multiple random number generations.

3.2.12 Cryptographic KeyStore

The platform provides the application with a way to store *the cryptographic keys* 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 section 3.2.9 Cryptographic Operation*.

Conformance rationale:

The platform implements a secure key store by leveraging the secure key handling capabilities of the Security IP. The access management circuit inside the Security IP ensures that the cryptographic operations taking place inside the Security IP do not require any sensitive information to be exposed on a CPU or externally-accessible bus as described in 45. Trusted Secure IP in R01UH0914EJ listed in section 1.3. In case of irregular access to the Security IP due to a falsified program or runaway execution of a program, this circuit blocks all subsequent access and stops the output of data from the Security IP. The procedures that actually be used by applications are according to API specifications of the driver described in the "RZ_SCE_Driver_Usage" listed in section 1.3. Those APIs to generate keys to use each cryptographic operation generates a wrapped key from a random number in the Security IP. Accordingly, user key input is unnecessary. By encrypting data using the wrapped key is output by those APIs, dead copying of data can be prevented.

3.3 Additional Security Functional Requirements

~~3.3.1 Secure Communication Support~~

~~The platform provides the application with one or more secure communication channel(s).~~

The platform does not support this SFR.

~~3.3.2 Secure Communication Enforcement~~

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

The platform does not support this SFR.

3.4 Optional Security Functional Requirements

~~3.4.1 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>*.~~

The platform does not support this SFR.

3.4.2 Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust Services)

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

Conformance rationale:

Security IP is a security entity with a hardware unique key (HUK). Unauthorized access to the HUK is prevented by the access management circuit within the security IP. The platform prevents compromising through only Security IP can use this HUK for cryptographic functions. Application RoT Services can use Security IP functions only via specific interfaces implemented using Trusted Execution Environment (TEE). It means code as the compromised application RoT service cannot compromise the integrity and confidentiality of the other application parts directly if they have been encrypted with Security IP.

~~3.4.3 Secure Encrypted Storage (internal storage)~~

~~The platform ensures that all data stored by the application can be encrypted as specified in 3.2.9 Cryptographic Operation with a platform instance unique key of key length shown in 3.2.9 Cryptographic Operation.~~

The platform does not support this SFR. Secure storage should be supported using functionality specified in 3.2.9 Cryptographic Operation. But this SFR requires automated encryption like on-the-fly encryption.

~~3.4.4 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.~~

There is the JTAG authentication mode which can be set as that all debugger connection is prohibit. For end products, it is offered to set “prohibit connection” mode the debug feature to be deactivated. Therefore, this SFR is removed in the ST.

~~3.4.5 Secure Storage (internal storage)~~

~~The platform ensures that all data stored by the application can be protected to ensure its authenticity and integrity as specified in 3.2.9 Cryptographic Operation with a platform instance unique key of key length shown in 3.2.9 Cryptographic Operation.~~

The platform does not support this SFR. This SFR is unnecessary for TOE because the NSPE never references the data in the SPE storage.

~~3.4.6 Secure External Storage~~

~~The platform ensures that all data stored outside the direct control of the platform can be protected such that the authenticity, integrity, confidentiality and binding to the platform instance is ensured.~~

The platform does not support this SFR. This SFR is unnecessary for TOE because data that should be protected from SPE to external storage is not saved.

3.4.7 Limited Physical Attacker Resistance

The platform detects or prevents attacks by an attacker with physical access before the attacker compromises ***Verification of Platform Identity, Verification of Platform Instance Identity, Secure Initialization of Platform, Attestation of Platform State, Software Attacker Resistance: Isolation of Platform and Cryptographic KeyStore***.

Conformance rationale:

The platform prevents compromising the SFR 3.2.2 Verification of Platform Instance Identity by OTP. The OTP prevents an attacker from being able to modify the platform instance identity. Also, the platform prevents compromising the SFRs 3.2.4 Secure Initialization of Platform and 3.2.5 Attestation of Platform State by OTP. Their SFRs behave according to the state set in the fields in the OTP. Same as OTP, the platform identity is written in read-only register. So, the platform prevents compromising the SFR 3.2.1 Verification of Platform Identity.

The platform prevents compromising the SFR 3.2.7 Software Attacker Resistance: Isolation of Platform enforcing TrustZone® isolation. Trustzone® assigns security attributes to each memory and peripheral, these attributes are fixed at program loading and cannot be changed by the application. And this loader ensures integrity and authenticity with Secure Boot.

The platform prevents compromising the SFR 3.2.4 Secure Initialization of Platform by the Security IP. The Security IP is a security entity with a hardware unique key (HUK). Unauthorized access to the HUK is prevented by the access management circuit within the security IP as described in 45. Trusted Secure IP in R01UH0914EJ listed in section 1.3. The platform prevents compromising through only security IPs can use this HUK to encrypt and decrypt keys used by their SFRs.

4 Mapping and sufficiency rationales

4.1 Assurance

Assurance Class	Assurance Family	Covered by
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section “Introduction”
	Rationale: The ST reference is in “SESIP profile reference”, the TOE reference in “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”
	Rationale: 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”
	Rationale: All SFRs in SESIP Profile for PSA Certified Level 2 V1.0 REL 01 are taken to the Security Target. And SFRs which aren’t supported are removed using strike-through.	
	ASE_TSS.1 TOE Summary Specification	Section “Security Requirements and Implementation”
	Rationale: All SFRs are listed per definition, and for each SFR the implementation and verification are defined in Security Functional Requirements.	
ADV: Development	ADV_FSP.4 Complete functional specification	• R01AN6346EJ: Security Package for RZ MPU Security User’s Manual Rev 3.1 • R01UH0914EJ: RZ/G2L Group, RZ/G2LC Group User’s Manual: Hardware Rev 1.10
	Rationale: The evaluator will validate suitability of the provided evidence.	
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	• R01AN6346EJ: Security Package for RZ MPU Security User’s Manual Rev 3.1
	Rationale: The document describes the operation of the platform and how to use the platform to create an end application. The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.	
	AGD_PRE.1 Preparative procedures	• R01AN6346EJ: Security Package for RZ MPU Security User’s Manual Rev 3.1 • R11AN0556EJ: RZ/G2L and RZ/G2LC SMARC EVK Security Start-up Guide Rev 1.21 • R01US0553EJ: RZ/G Verified Linux Package Version 3.0.0-update1 Release Note Rev 1.03 • RZ_SCE_Driver_Usage
	Rationale: These documents describe how to prepare the platform as part of an end product. The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.	

Assurance Class	Assurance Family	Covered by
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section “Flaw Reporting Procedure (ALC_FLR.2)
	Rationale: The flaw reporting and remediation procedure is described.	
ATE: Tests	ATE_IND.1 Independent testing: conformance	N/A
	Rationale: The evaluator will perform independent testing.	
AVA: Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis	N/A
	Rationale: The evaluator will perform penetration testing.	

Table 5 Assurance Mapping and Sufficiency Rationales

4.2 Functionality

PSA Security Function	Covered by SESIP SFR	Rationale
F.INITIALIZATION	Secure Initialization of Platform	Full coverage
F.SOFTWARE_ ISOLATION	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Full coverage
	(Optional) Software Attacker Resistance: Isolation of Application Parts (between each of the Application Root of Trust Services)	Full coverage
F.SECURE_ STORAGE	Secure Encrypted Storage (internal storage)	Not provided by TOE
	Secure Storage (internal storage)	Not provided by TOE
	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage
	Secure External Storage	Not provided by TOE
F.FIRMWARE_ UPDATE	Secure Update of Platform	Removed using strike-through for the reason stated in “Flaw Reporting Procedure (ALC_FLR.2)

PSA Security Function	Covered by SESIP SFR	Rationale
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform (between SPE and NSPE)	Full coverage
	Software Attacker Resistance: Isolation of Platform (between PSA-RoT and Application Root of Trust Services)	Full coverage
	Partially covered by the SFR Secure Initialization of Platform.	Full coverage
F.CRYPTO	Cryptographic Operation	Full coverage
	Cryptographic KeyStore	Full coverage
	Cryptographic Random Number Cryptographic Random Number Generation	The evaluation of the random number generator shall follow a recognized methodology.
	Cryptographic Key Generation	Full coverage
F.ATTESTATION	Verification of Platform Identity	Unique identification of the platform
	Verification of Platform Instance Identity	Unique identification of the platform instance
	Attestation of Platform Genuineness	Removed using strike-through for the reason stated in 3.2.3 Attestation of Platform Genuineness.
	Attestation of Platform State	Full coverage
F.AUDIT	Audit Log Generation and Storage	Not provided by TOE
F.DEBUG	Secure Debugging	Removed using strike-through since it is offered that the debug feature to be deactivated

Table 6 Functionality Mapping and Sufficiency Rationales

5 Version history

Rev	Description	Date
1.0	First release	2022-11-11
1.1	Minor corrections reviewed by the certification body	2022-11-30
1.2	Fix and add descriptions as per feedback from the certification body: 1.5.2, 1.5.3, 3.2.1, 3.2.2, 3.2.3, 3.2.5, 3.4.5, 3.4.6, 3.4.7	2023-01-27
1.3	Add description as per feedback from the certification body: 3.2.9	2023-02-17
1.4	Remove the following SFR from the supported SFR: 3.2.3, 3.4.3, 3.4.5, 3.4.6	2023-03-07
1.5	Fix descriptions as per feedback from the certification body: 1.5.4, 2, 3.2.3	2023-06-05
1.6	Fix descriptions as per feedback from the certification body: 2, 3.2.3	2023-06-13