Security Target

RENESAS

RA8T1

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

All information contained in these materials, including products and product specifications, represents information on the product at the time of publication and is subject to change by Renesas Electronics Corp. without notice. Please review the latest information published by Renesas Electronics Corp. through various means, including the Renesas Electronics Corp. website (http://www.renesas.com).

Renesas Electronics
www.renesas.com

Rev.1.1 Sep.25.2024

RA8T1

Security Target for SESIP Profile, PSA Certified Level 3 RoT Component

Contents

Figures

Tables

1 Introduction

The “RA8T1 Security Target for SESIP Profile, PSA Certified™ Level 3 RoT Component” describes the RA8T1 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 RoT Component Level 3
PP Version	Version 1.0 REL 2
Assurance Claim	SESIP Assurance Level 3 (SESIP 3)
Optional and additional SFRs	• Verification of Platform Identity • Secure Update of Platform • Physical Attacker Resistance • Secure Initialization of Platform • Software Attacker Resistance: Isolation of Platform • Cryptographic Operation • Cryptographic Random Number Generation • Cryptographic Key Generation • Cryptographic Key Store • Secure Communication Support • Secure Communication Enforcement

Table 1: SESIP Profile Reference

1.2 Platform Reference

The platform is uniquely identified by its hardware and/or software references, depending on the platform type.

Reference	**Value**
Platform Name	RA8T1 MCU Group
Platform Version	A
Platform Identification	Commercial Name: RA8T1 MCU Group Part Numbers: 1024 KB program flash: R7FA8T1xFxxxx #xxx 2048 KB program flash: R7FA8T1xHxxxx #xxx
	Flexible Software Package (FSP) v5.4.0
Platform type	General purpose microcontroller

Table 2: Platform Reference

1.3 Included Guidance Documents

The following documents are included with the platform:

Reference	Name	Version
[RA8T1 HUM]	RA8T1 Group User’s Manual: Hardware, RA01UH1016EJ0110	V1.10
[FSP User Manual]	RA Flexible Software Package Documentation	V5.4.0
[Secure Key Injection AP]	Injecting and Updating Secure User Keys for RA Family - Application Project, R11AN0496EU0200	V2.0.0
[Plaintext Key Injection AP]	Injecting Plaintext User Keys – Application Project, R11AN0473EU200	V2.0.0

Table 3: Guidance Documents

All items can be downloaded from the Renesas web site (www.renesas.com).

1.4 Platform Functional Overview and Description

1.4.1 Platform Type

RA8T1 MCU Group are general purpose MCUs that contain the RSIP-E51A security engine, an on-chip isolated subsystem comprising:

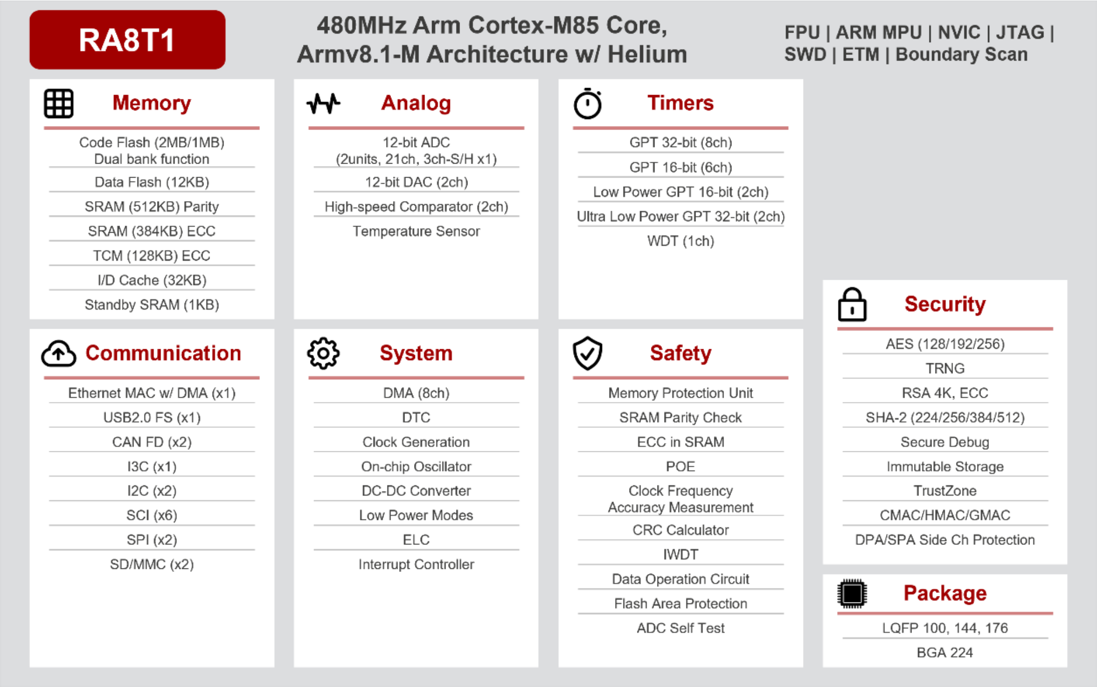
- A cryptographic engine, providing hardware-accelerated cryptography
- A True Random Number Generator
- Dedicated RAM, to isolate all operations from the rest of the chip
- A secure key handling mechanism, enabling the secure storage of keys outside the security engine
- An Access Management Circuit, which shuts down the security engine in the event of an illegal access attempt
- A bus interface for communicating with the components of the chip
- A Hardware Root Key (HRK) used as part of a KDF for secure key injection

The certified Platform is anticipated to provide a basis for further composite security evaluations.

1.4.2 Physical Scope

The physical scope of the platform consists of the RA8T1 MCU Group products as described by the [RA8T1 HUM] hardware user's manual.

FIGURE 1-1 RA8T1 MCU GROUP BLOCK DIAGRAM shows the block diagram of the MCU Group.



RA8T1

480MHz Arm Cortex-M85 Core,
Armv8.1-M Architecture w/ Helium

FPU | ARM MPU | NVIC | JTAG |
SWD | ETM | Boundary Scan

Memory
- Code Flash (2MB/1MB) Dual bank function
- Data Flash (12KB)
- SRAM (512KB) Parity
- SRAM (384KB) ECC
- TCM (128KB) ECC
- I/D Cache (32KB)
- Standby SRAM (1KB)

Analog
- 12-bit ADC (2units, 21ch, 3ch-S/H x1)
- 12-bit DAC (2ch)
- High-speed Comparator (2ch)
- Temperature Sensor

Timers
- GPT 32-bit (8ch)
- GPT 16-bit (6ch)
- Low Power GPT 16-bit (2ch)
- Ultra Low Power GPT 32-bit (2ch)
- WDT (1ch)

Communication
- Ethernet MAC w/ DMA (x1)
- USB2.0 FS (x1)
- CAN FD (x2)
- I3C (x1)
- I2C (x2)
- SCI (x6)
- SPI (x2)
- SD/MMC (x2)

System
- DMA (8ch)
- DTC
- Clock Generation
- On-chip Oscillator
- DC-DC Converter
- Low Power Modes
- ELC
- Interrupt Controller

Safety
- Memory Protection Unit
- SRAM Parity Check
- ECC in SRAM
- POE
- Clock Frequency Accuracy Measurement
- CRC Calculator
- IWDT
- Data Operation Circuit
- Flash Area Protection
- ADC Self Test

Security
- AES (128/192/256)
- TRNG
- RSA 4K, ECC
- SHA-2 (224/256/384/512)
- Secure Debug
- Immutable Storage
- TrustZone
- CMAC/HMAC/GMAC
- DPA/SPA Side Ch Protection

Package
- LQFP 100, 144, 176
- BGA 224

Figure 1-1 RA8T1 MCU Group Block Diagram

FIGURE 1-2 PLATFORM EVALUATION PHYSICAL SCOPE shows the physical scope of the evaluation. The RSIP-E51A security engine contained within the RA8T1 MCU Group provides the security features listed in section 1.4.1 PLATFORM TYPE.

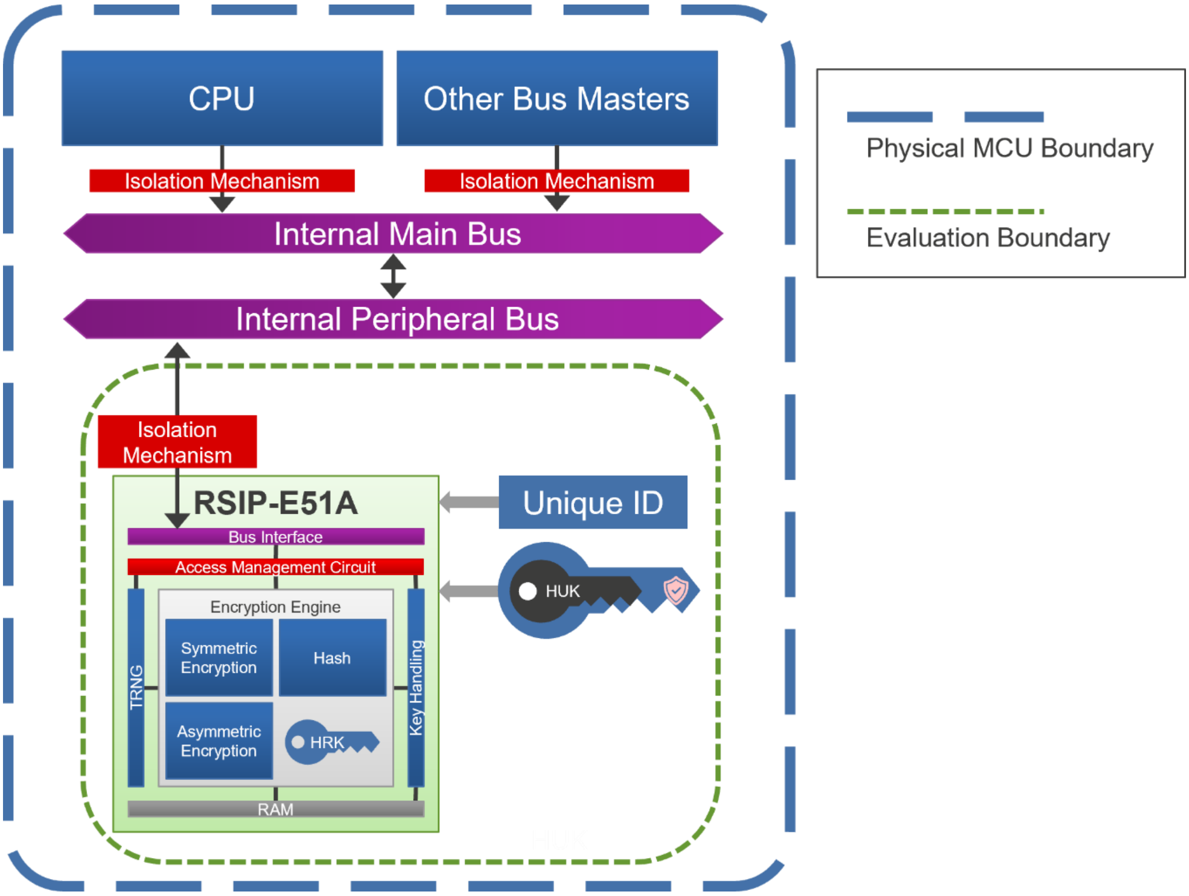


Figure 1-2 Platform Evaluation Physical Scope

The software to use the platform is provided by the Renesas RA Family Flexible Software Package (FSP). The TOE scope is depicted in FIGURE 1-3 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-E51A security engine plus on-chip support hardware as shown above
- Low-level HAL Drivers for the RSIP security engine
- PSA Crypto API implementation included in the TrustedFirmware-M port included in the FSP

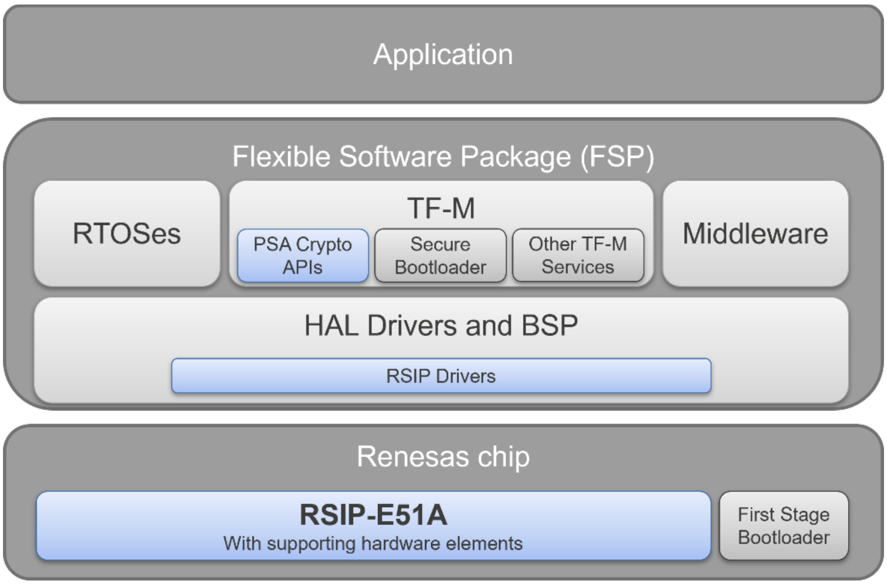


Figure 1-3 TOE Scope

Items that are not within scope for this evaluation are:

- All other features and peripherals of the MCU that are not explicitly identified in FIGURE 1-3 TOE SCOPE and listed above.
- All other modules in the Flexible Software Package.
- Any application software created by the end-product developer.

Guidance documentation for the security engine is included in the Renesas chip Hardware User Manual [RA8T1 HUM], which is available for public download from the Renesas web site (www.renesas.com). Renesas microcontrollers are available via Renesas's normal sales channels. The Flexible Software Package (FSP) is also available for public download from the Renesas web site (www.renesas.com).

1.4.3 Usage and Major Security Features

The RA8T1 MCU Group is based on the Arm® Cortex®-M85 (CM85) core, delivering breakthrough performance of over 3000 CoreMark points at 480 MHz, with fully deterministic, low latency, real-time operation that enables customers' most demanding application needs. These are general-purpose MCU devices and address diverse high-performance and compute-intensive applications in Industrial Automation, Home Appliances, Smart Home, Consumer, Building/Home Automation and Medical/Healthcare market segments.

The Renesas RA8T1 MCU Group contains the RSIP-E51A 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 GMAC 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, 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 MCU. The security engine's Hardware Root Key (HRK) enables secure key injection and update.

The RA8T1 MCU Group also incorporates Arm TrustZone technology as a hardware isolation mechanism, further isolating the access to all cryptographic operations and sensitive data to protect against both physical and logical attacks.

The platform is delivered with software drivers that implement the PSA Crypto APIs, allowing simple integration into a wide variety of target applications.

1.4.4 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.	[Secure Key Injection AP] section 2.2 [Plaintext Key Injection AP] section 2.1
TRUSTED_USERS	Actors in charge of platform management, for instance for signature of firmware update, are trusted.	The end product developer must configure the peripheral security attribution correctly to place the security engine in the SPE, as per [RA8T1 HUM] section 37.2.3.6.
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 [RA8T1 HUM] section 46.4.6 and described in the ST in section 3.2.1 VERIFICATION OF PLATFORM IDENTITY, the platform's unique ID is provisioned as part of the Renesas manufacturing process.

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 a flaw and generate any needed update and distribute it, Renesas 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 concerned 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 might 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 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 contains a 16-byte read-only register that contains an ASCII representation of the device part number. The PNRn Part Numbering Registers are documented in section 46.4.6 PNRN: PART NUMBERING REGISTER in [RA8T1 HUM]. A part number listing is given in section 1.3 PART NUMBERING in [RA8T1 HUM].

The PNRn registers are located at addresses 0x0300_80F0 through 0x0300_80F3. The first seven ASCII digits of the PNRn register must read “R7FA8T1” to indicate that the device is an RA8T1 MCU. The other ASCII digits represent non-security related items such as package type, packing, operating temperature, and code flash memory size.

The contents of the PNRn are as follows (“x” is used to represent a “don’t care” value for security-related functionality):

Address	ASCII Representation (Little Endian)
0x0300_80F0	R7FA
0x0300_80F1	8T1x
0x0300_80F2	xxxx
0x0300_80F3	xxxx

Table 5: Part Numbering Register Values

The part number information is written as part of the production process, and the production testing procedures verify the value has been written correctly.

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 platform does not support the update or patching of the security features that are in scope for this evaluation. Justification for why the hardware does not support secure updates is provided as part of section 3.1.1 FLAW REPORTING PROCEDURE (ALC_FLR.2).

3.2.3 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 1-2 PLATFORM EVALUATION PHYSICAL SCOPE. The Access Management Circuit will shut down the security engine in the event of improper access via the CPU or the debugger. Multiple verifications to confirm correct sequential operation are conducted during each cryptographic operation, providing protection against fault injection and Differential Fault Analysis (DFA) attacks.

3.3 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 go to **a state where no other operation except optionally SECURE UPDATE OF PLATFORM (section 3.2.2) can be performed**.

Conformance Rationale:

Secure initialization of the platform is guaranteed by the Access Management Circuit of the security engine. Initialization to conduct each and every specific cryptographic function must be done via a secure mechanism using integrity check data that has been encrypted with the HRK of the TOE. Failure of the secure initialisation will result in the Access Management Circuit shutting down all access to the security engine. This ensures secure initialization of the platform.

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:

As shown in FIGURE 1-2 PLATFORM EVALUATION PHYSICAL SCOPE, the security engine is isolated within the platform by being physical isolated on the chip, with all communication taking place over a single bus interface that is isolated via a hardware isolation mechanism.

The RSIP-E51A security engine is integrated into the RA8T1 microcontroller, using the Arm TrustZone technology provided by the Cortex-M85 core as the hardware isolation mechanism. The security engine must be defined to be in the Secure region, such that only the Secure Processing Environment can access it, providing protection from an attacker running application code. In addition, it is further protected by an Access Management Circuit, which will shut down the security engine in the event of an illegal access attempt.

3.3.3 Cryptographic Operation

The platform provides the application with Operations in TABLE 6 functionality with algorithms in TABLE 6 as specified in specifications in TABLE 6 for key lengths described in TABLE 6 and modes described in TABLE 6.

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 SP800-38C (CCM) NIST SP800-38D (GCM, GMAC)	128, 192, 256 bits	ECB, CBC, CTR, CCM, GCM, CMAC, GMAC
RSA	Signature generation, signature verification	IETF RFC 8017 FIPS PUB 186-5	2048, 3072, 4096 bits	N/A
ECC	Signature generation, signature verification	FIPS PUB 186-5	Curves: NIST P-256, P-384, P-521; secp256k1; Brainpool P256r1, P384r1	N/A
SHA	Hash	FIPS PUB 180-4	N/A	SHA-224, SHA-256, SHA-384, SHA-512

Table 6: Cryptographic Operations

Conformance rationale:

The above crypto operations are supported by the security engine (RSIP-E51A), as documented in section 38 in [RA8T1 HUM].

The security engine is thoroughly tested by simulation during the design phase and by device characterization of the actual silicon. Each die undergoes production test prior to shipment to ensure proper functionality of each MCU.

The application provides cryptographic key material and plaintext/ciphertext to the security engine using software APIs provided in the Flexible Software Package. The security engine performs the low-level cryptographic operations. Operations such as padding and signature schemes are performed by software

APIs. The result of the operation (e.g. ciphertext, plaintext, hash, or verification result) is returned to the application.

3.3.4 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 engine. The TRNG implementation consists of an SP800-90A compliant DRBG that is fed by an SP800-90B compliant seed, which is generated from an entropy source. Each TRNG request generates a 128-bit random number.

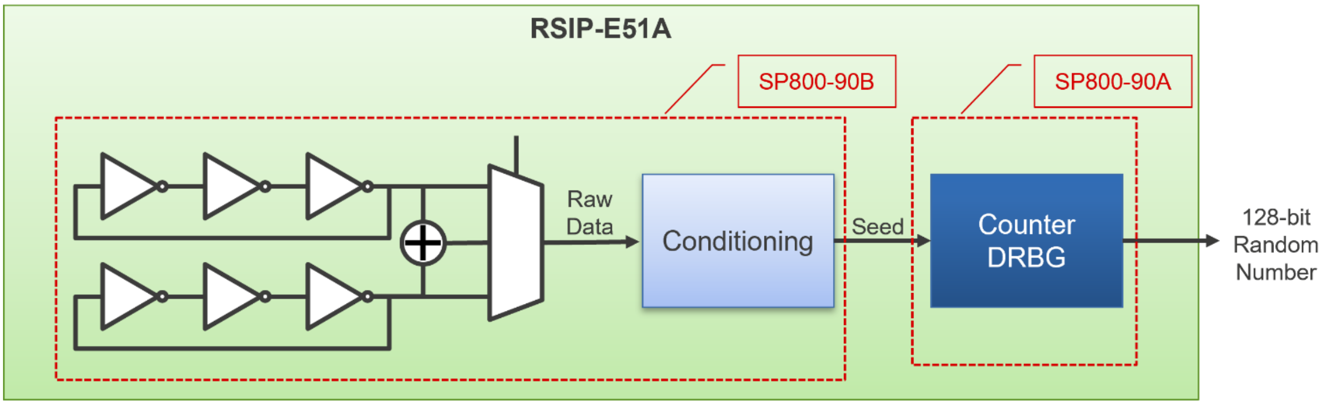


Figure 3-1 True Random Number Generation Block Diagram

As shown in FIGURE 3-1 TRUE RANDOM NUMBER GENERATION BLOCK DIAGRAM, the raw data for the seed is obtained by XOR-ing the output of two ring oscillators. This output is tested, and any conditioning required for SP800-90B compliance is applied. These tests are performed by the Renesas Shared Security Competency Centre, and the results are published on the Renesas web site. The seed is fed into a Counter DRBG, which is planned to be submitted for NIST CAVP certification, similar to the existing certification for the Renesas SCE9 (Cryptographic Algorithm Validation Program | CSRC (nist.gov)).

The security engine is thoroughly tested by simulation during the design phase and by device characterisation of the actual silicon. Each die undergoes production test prior to shipment to ensure proper functionality of each MCU.

3.3.5 Cryptographic Key Generation

The platform provides the application with a way to generate cryptographic keys for use in cryptographic operations in TABLE 7 as specified in specifications in TABLE 7 for key lengths described in TABLE 7.

Conformance rationale:

The following table identifies the cryptographic key types and key lengths that can be generated by the RSIP-E51A security engine.

Algorithm	**Specification**	**Key lengths**
AES	NIST FIPS PUB 197	128, 192, 256 bits
RSA	IETF RFC 8017 FIPS PUB 186-5	2048, 3072, 4096 bits
ECC – SEC and Brainpool prime curves	FIPS PUB 186-5	256, 384, 521 bits

Table 7: Cryptographic Key Generation

3.3.6 Cryptographic Key Store

The platform provides the application with a way to store ***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*** 3.3.3 CRYPTOGRAPHIC OPERATION.

Conformance rationale:

Unlimited secure key storage is provided by the secure key handling mechanism of the security engine. Secure keys are stored in wrapped format, ensuring authenticity, integrity, and confidentiality by using AES in CCM mode (NIST SP800-38C) with an MCU-unique 256-bit key derived from the MCU's HUK. By leveraging the MCU's HUK, this mechanism binds the wrapped key to the specific MCU 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 security engine - there is no mechanism for the security engine to decrypt the wrapped key, and the HUK is accessible only by the security engine.

There is no dedicated storage area for keys within the scope of this evaluation. A specific platform implementation may choose to dedicate an area to key storage.

Secure keys comprise:

- Keys that are generated inside the security engine.
- Keys that are securely injected. This function is performed leveraging the Hardware Root Key of the security engine.
- Keys that were originally provided as plaintext keys but have been wrapped by the security engine.

3.4 Additional Security Functional Requirements

3.4.1 Secure Communication Support

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

The secure communication channel authenticates ***command and data transfers between the security engine and chip bus masters*** and protects against ***disclosure, modification, replay, and erasure*** of messages between the endpoints, using ***physical isolation and command sequence integrity verification***.

Conformance Rationale:

All communication with the security engine takes place over a single bus interface, which is protected by an Access Management Circuit. Security engine does not contain direct-access registers for performing cryptographic operations; instead, security engine interaction is performed through a set of control and data transfer registers. Verification codes must be sent to the Access Management circuit prior to any requested operation, and the command sequence for that operation must align with the verification code. Any corruption of the verification codes or modification of the command sequence will result in the Access Management Circuit shutting down all access to the security engine.

To limit security engine access to the Secure Processing Environment, the bus interface used to communicate with the security engine is protected by the Arm TrustZone hardware isolation mechanism. FIGURE 1-2 PLATFORM EVALUATION PHYSICAL SCOPE shows the on-chip architecture and physical isolation of the security engine on the chip.

The combination of on-chip implementation, physical isolation on the chip, Arm TrustZone protection, and the Access Management Circuit protects command and data transfers against disclosure, modification, replay, and erasure.

3.4.2 Secure Communication Enforcement

The platform ensures that the application can only communicate with **trusted subsystems** over the secure communication channel(s) supported by the platform using ***an on-chip peripheral bus and Arm TrustZone protection***.

Conformance Rationale:

Since the RSIP-E51A security engine is an on-chip Trusted Subsystem, it is protected against physical probing of a PCB and MCU pin manipulation. All accesses to the security engine must go through the on-chip peripheral bus. Access to the security engine is further protected by Arm TrustZone, ensuring that only the Secure Processing Environment can interact with the security engine. This interaction is further protected by the Access Management Circuit of the security engine, which will shut down the security engine in the event of an illegal access attempt, as described by section **3.4.1 SECURE COMMUNICATION SUPPORT**. For a block diagram showing the on-chip architecture that enforces secure communication, see **FIGURE 1-2 PLATFORM EVALUATION PHYSICAL SCOPE**.

4 Mapping and Sufficiency Rationales

4.1 SESIP3 Sufficiency

Assurance Class	Assurance Family	Covered by
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section 1 Introduction and title page of the Security Target
	Rationale: 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 2 Security Objectives for the operational environment of the Security Target
	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 3 Security Requirements and Implementation of the Security Target
	Rationale: The SFRs addressed by the TOE and described in “Security Requirements and Implementation” are listed in “SESIP Profile Reference”.	
	ASE_TSS.1 TOE Summary Specification	Section 3 Security Requirements and Implementation of the Security Target
	Rationale: All SFRs are listed per definition, and for each SFR the implementation and verification are defined in “Base PP Security Functional Requirements”, “SFRs for PSA-RoT Component”, and “Additional Security Functional Requirements”.	
ADV: Development	ADV_FSP.4 Complete functional specification	[RA8T1 HUM]
	Rationale: The RA8T1 Group User’s Manual contains the functional specification of the RSIP-E51A.	
	ADV_IMP.3 Complete mapping of the implementation representation of the TSF to the SFRs	[FSP User Manual] and the FSP source code
	Rationale: The FSP User Manual contains the mapping of the implementation of the TOE Security Functions to the SFRs described in the relevant sections of the Security Target. The FSP source code 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	[RA8T1 HUM] [FSP User Manual]
	Rationale: The RA8T1 Group User’s Manual and the RA Flexible Software Package documentation describe the operation of the RoT Component and how to utilize the component in an end application.	
	AGD_PRE.1 Preparative procedures	[Secure Key Injection AP] [Plaintext Key Injection AP]
	Rationale: The [Secure Key Injection AP] describes the process for and includes examples of securely injecting application keys. The [Plaintext Key Injection AP], which describes the process for and includes examples of injecting plaintext application keys, can also be used with the PSA Crypto APIs.	

ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE	[RA8T1 HUM] [FSP User Manual]
	Rationale: The presence of the RSIP-E51A security engine is determined by the definition of the specific MCU Group and documented by the MCU Group's Hardware User Manual. The complete MCU part number, including MCU Group, is typically available on the silkscreen of the chip and available via the mechanisms described in section 3.2.1 VERIFICATION OF PLATFORM IDENTITY. Application-level software support to utilise the security engine is described in the [FSP User Manual].	
	ALC_CMS.1 TOE CM Coverage	[RA8T1 HUM]
	Rationale: The Hardware User Manual for the MCU Group specifies the presence (or lack) of the security engine. Modification of a component of the MCU Group will be reflected in the version of the MCU part number described in section 3.2.1 VERIFICATION OF PLATFORM IDENTITY. The complete manifest of MCU contents is maintained by Renesas in accordance with internal design process requirements.	
	ALC_FLR.2 Flaw reporting procedures	Section 3.1.1 FLAW REPORTING PROCEDURE (ALC_FLR.2) of the Security Target
	Rationale: The flaw reporting and remediation procedure is described in "Flaw Reporting Procedure (ALC_FLR.2)".	
ATE: Tests	ATE_IND.1 Independent testing: conformance	Evaluator testing and review of provided test logs as per this Security Target
	Rationale: The platform evaluator will determine whether the provided evidence is suitable to meet the requirement.	
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis	Vulnerability assessment and testing carried out by the laboratory
	Rationale: The platform evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE. Penetration testing is performed by the platform evaluator assuming an attack potential of Enhanced-Basic.	

Table 8 : Assurance Mapping and Sufficiency Rationales

4.2 PSA Security Functions Mapping

PSA Security Function	Covered by SESIP SFR
F.INITIALIZATION	Secure Initialization of Platform
F.SOFTWARE_ ISOLATION	Software Attacker Resistance: Isolation of Platform
F.SECURE_STATE	Software Attacker Resistance: Isolation of Platform
	Secure Initialization of Platform
F.CRYPTO	Cryptographic Operation
	Cryptographic KeyStore
	Cryptographic Random Number
	Cryptographic Key Generation
F.ATTESTATION	Verification of Platform Identity
F.PHYSICAL	Physical Attacker Resistance
Additional security functionality	Secure Communication Support
	Secure Communication Enforcement

Table 9: Functionality Mapping and Sufficiency Rationales

5 Reference Documents

Reference	Name	Version
[PSA Crypto API]	PSA Certified Crypto API, IHI0086	V1.2
[SP800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	rev 1, June 2015
[SP800-90B]	Recommendation for the Entropy Sources Used for Random Bit Generation	January 2018

Table 10: Reference Documents

6 Abbreviations

Term	Definition
BSP	Board Support Package
DFA	Differential Fault Analysis
ECC	Elliptic Curve Cryptography
FSP	Renesas RA Family Flexible Software Package
HAL	Hardware Abstraction Layer
HRK	Hardware Root Key
HUK	Hardware Unique Key
HUM	Hardware User’s Manual
HRK	Hardware Root Key
MCU	Microcontroller
MPU	Microprocessor
NSPE	Non-secure Processing Environment
PCB	Printed Circuit Board
PKI	Public Key Infrastructure
PSA-RoT	PSA Root of Trust
PSIRT	Product Security Incident Response Team
QAD	Quality Assurance Division
RoT	Root of Trust
RSIP	Renesas Security IP
SFR	Security Functional Requirement
SoC	System-on-Chip
SPA/DPA	Simple Power Analysis / Differential Power Analysis
SPE	Secure Processing Environment
ST	Security Target
TF-M	Trusted Firmware-M
TOE	Target of Evaluation

Revision History

Rev.	Date	Description	
		Page	**Summary**
1.0	Jul.19.2024	—	Initial release
1.1	Sep.25.2024	15	Corrected reference error

Security Target

Renesas Electronics Corporation