Security Target for the Renesas RA6M3 MCU Group

Based on [SESIP] methodology, version "Public Release v1.0"

Rev. 1.4
January 29, 2021

Contents

Table of Figures

1 Introduction

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

1.1 ST reference

See title page.

1.2 Platform reference

TOE name	Renesas RA6M3 MCU Group
TOE version	2
TOE identification	RA6M3
TOE Type	General purpose microcontroller for connected applications

1.3 Included guidance documents

The following documents are included with the platform:

Reference	**Name**	**Version**
R01UH0886EJ0100	Renesas RA6M3 Group User's Manual: Hardware	Rev 1.00
TN-RA*-A0003A/E	Errata for User's Manual: Hardware for SCE7	Rev 1.00
TN-RA*-A0009A/E	RA family, Addition of register definition for Flash	Rev 1.00
R20UT4813EJ0100	Renesas Flash Programmer v3.08 Flash memory programming software User’s Manual	RFP v3.08, UM v1.00
R11AN0449EU0120	Renesas RA Family Establishing and Protecting Device Identity using SCE7 and Security MPU	Rev 1.20
R11AN0416EU0120	Securing Data at Rest Utilizing the Renesas Security MPU Project	Rev 1.20
R01AN5347EU0110	Arm® Secure Boot Solution for RA6M3 MCU Group Project	Rev 1.10
R01AN5372EU0100	Renesas RA Family System Specifications for Standard	Rev 1.00

	Boot Firmware	
R01AN5367EU0100	Renesas RA Family Flash Memory Programming	Rev 1.00

1.4 (Optional) Other Certification

The product has previously been evaluated following [ARM PSA L1]:

Scheme	PSA Certified Level One
Certification body	TrustCB
Certification number	0716053549624-10010
Certificate date	01/10/2019

1.5 Platform functional overview and description

The flexible Renesas RA Family 32-bit MCUs are industry leading 32-bit MCUs with the Arm® Cortex®-M33, -M23 and -M4 processor cores and PSA certification. RA delivers key advantages compared to competitive Arm Cortex-M MCUs by providing stronger embedded security, superior CoreMark® performance, and ultra-low power operation. PSA certification provides customers the confidence and assurance to quickly deploy secure IoT endpoint and edge devices, and smart factory equipment for Industry 4.0.

The Renesas RA6M3 group of microcontrollers (MCUs) uses the high-performance Arm® Cortex®-M4 core and offers a TFT controller with 2D accelerator and JPEG decoder. Additionally, the RA6M3 MCU offers Ethernet MAC with individual DMA and USB high-speed interface to ensure high data throughput. The RA6M3 MCU is built on a highly efficient 40nm process and is supported by an open and flexible ecosystem concept—the Flexible Software Package (FSP), built on FreeRTOS—and is expandable to use other RTOSes and middleware. The RA6M3 is suitable for IoT applications requiring TFT, Ethernet, security, large embedded RAM, and USB High Speed (HS).

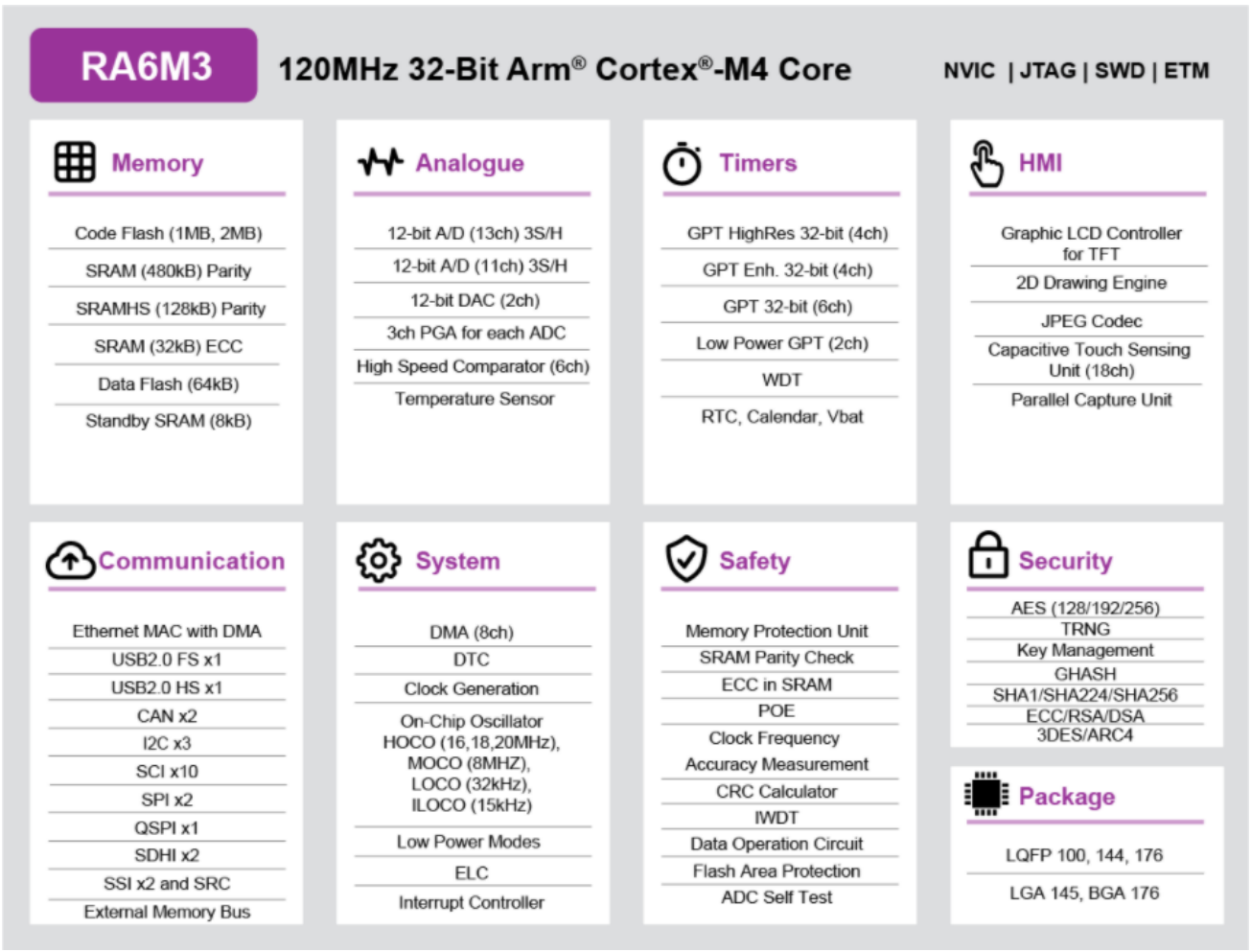

Figure 1 RA6M3 MCU Block Diagram

The RA Family Flexible Software Package (FSP) is an enhanced software package designed to provide easy-to-use, scalable, high-quality software for embedded system designs using Renesas RA family of Arm Microcontrollers. With the support of new Arm TrustZone and other advanced security features, FSP provides a quick and versatile way to build secure, connected IoT devices using production ready drivers, FreeRTOS™, and other middleware stacks.

FSP includes best-in-class HAL drivers with high performance and low memory footprint. Middleware stacks with FreeRTOS integration are included to ease implementation of complex modules like communication and security. The e² studio IDE provides support with intuitive configurators and intelligent code generation to make programming and debugging easier and faster.

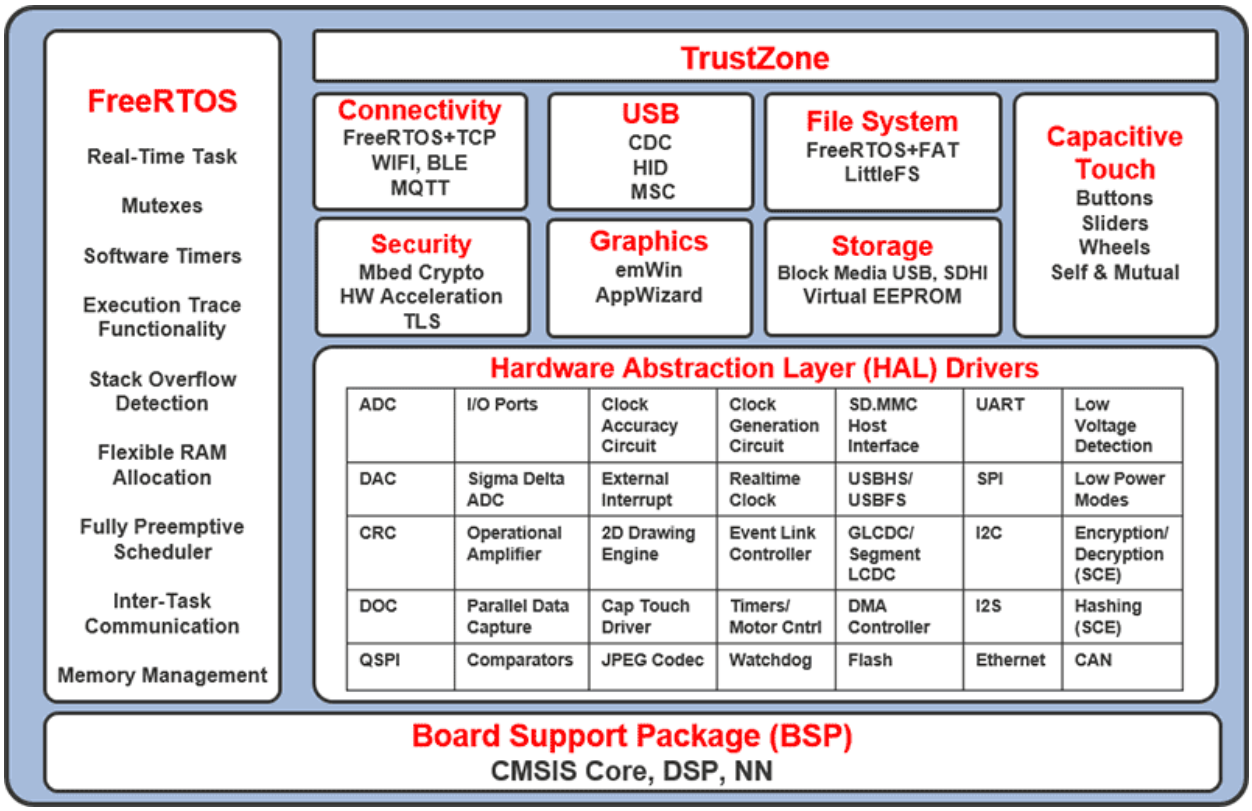

Figure 2 Flexible Software Package Block Diagram

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

The TOE 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 TOE are as follows:

- Arm Cortex-M4 32-bit core with a dedicated Security MPU as the hardware-enforced isolation mechanism
- Integrated Secure Crypto Engine (SCE7) providing AES, RSA, ECC, and hash generation in an isolated on-chip environment
- 128-bit unique identifier
- True Random Number Generator (TRNG)
- Secure unlimited key storage utilizing the 128-bit unique identifier and TRNG

The Secure Crypto Engine (SCE7) is a dedicated crypto subsystem contained within the MCU. Protected by an Access Management Circuit that can shut down the crypto engine upon illegal access attempts, the SCE7 performs all plaintext crypto operations using its own dedicated internal RAM, which is not accessible by any CPU-accessible bus. The advanced key storage and key handling capabilities of the SCE7 can ensure that no plaintext keys are ever stored in CPU-accessible RAM, code flash, or external storage.

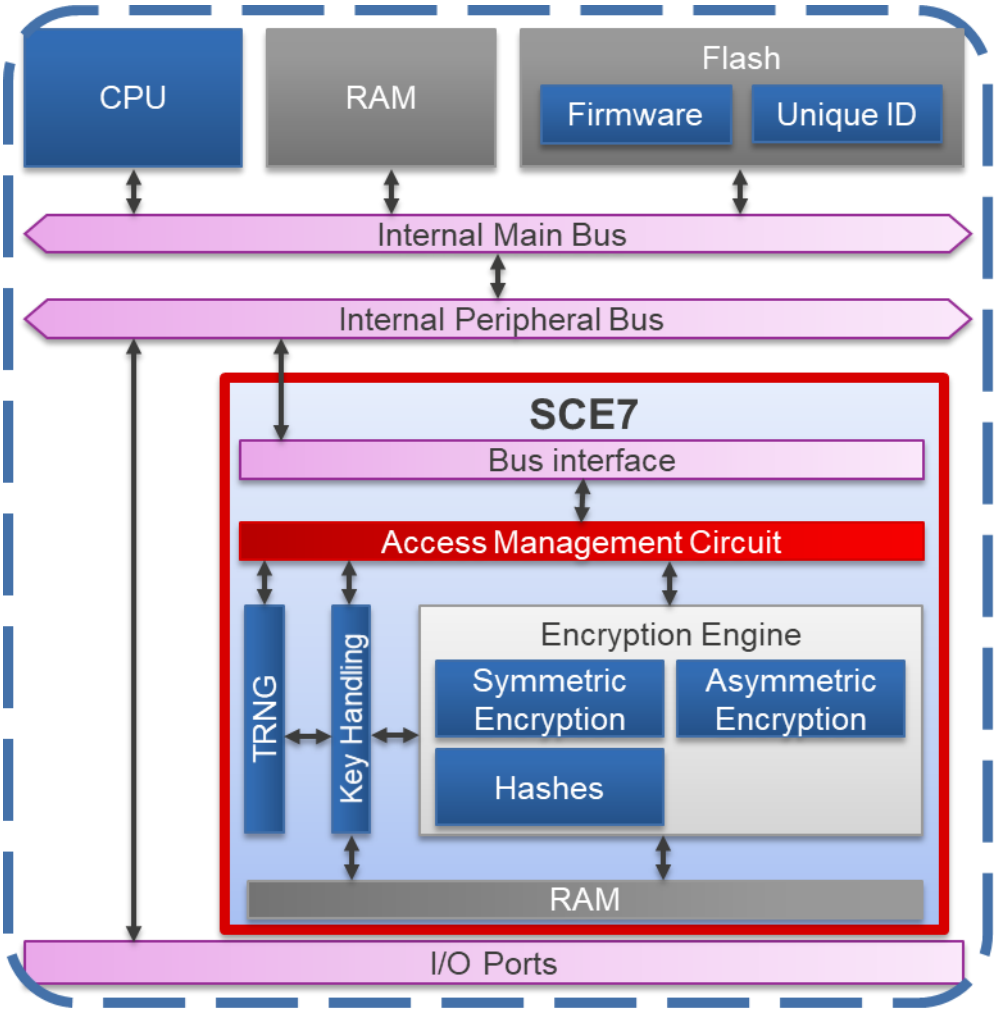

Figure 3 Secure Crypto Engine

The TOE scope is depicted in **Figure 4 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 Flexible Software Package (FSP) and any application software created by the end product developer.

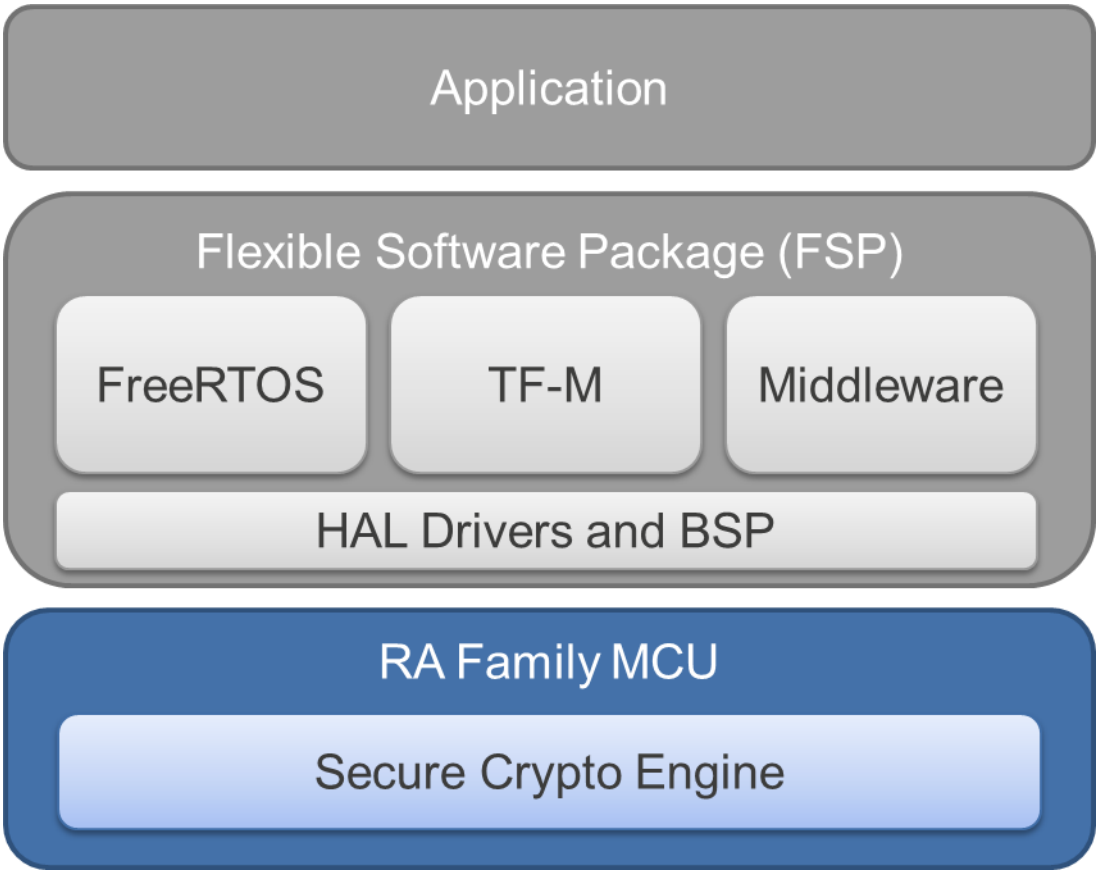

Figure 4 TOE Scope

The physical scope includes only the RA Family MCU itself, with the functional blocks identified in **Figure 1 RA6M3 MCU Block Diagram**. Guidance documentation for the MCU is listed in section **1.3 Included guidance documents** and is available for public download from the Renesas web site (www.renesas.com). RA Family MCUs are available via all of Renesas's normal sales channels. All RA Family MCUs contain the security features listed in this Security Target; no special part number nor personalization is required.

The logical scope includes the hardware and software interfaces necessary for the application and platform software to utilize the hardware. Cryptographic functions, such as encryption/decryption, hashing, secure cryptographic key handling, and random number generation, are performed by the Secure Crypto Engine (SCE7), shown in **Figure 4 TOE Scope** and detailed in **Figure 3 Secure Crypto Engine**. The remaining security features, including immutable MCU identification information, isolation mechanism, and external interface disabling, are provided by other silicon features on the MCU. These features are described in detail in the MCU documentation listed in section **1.3 Included guidance documents**.

Platform and application software is not in scope of this evaluation.

2 Security Objectives for the operational environment

2.1 Platform 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 in production, the MCU is configured to lock the external debugger and programmer interfaces, as described by sections ***2.11 OCD Emulator Connection*** and ***7.2.4 OCD/Serial Programmer ID Setting Register (OSIS)*** in the Hardware User Manual listed in section 1.3 above.

- The end product developer shall ensure that the device MPUs, in particular the Security MPU, are configured correctly for the application's memory isolation requirements, as described in section ***16 Memory Protection Unit*** in the Hardware User Manual and as described by the ***Securing Data at Rest Utilizing the Renesas Security MPU Project*** listed in section 1.3 above.

- For optimal key protection, the end product developer shall store sensitive keys as described in ***Renesas RA Family Establishing and Protecting Device Identity using SCE7 and Security MPU*** listed in section 1.3 above.

2.2 (Optional) Inherited Objectives for the Operational Environment

Not applicable.

3 Security requirements and implementation

3.1 Security Assurance Requirements

The claimed assurance requirements package is: **SESIP1** as defined in [SESIP].

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.

3.1.2 Vulnerability Survey (AVA_VAN.1)

In accordance with the requirement for a vulnerability analysis survey (AVA_VAN.1) the developer has performed a vulnerability survey and submits the following test results to demonstrate the consideration of publicized potential vulnerabilities relating to the TOE:

The Secure Crypto Engine, isolation mechanism, and programmer/debugger interface components of the platform were analysed to determine their vulnerability and attack potential. Side channel attacks, fault injection, abuse of the programmer/debugger interface, RNG attacks, and physical extraction of device information by decapping the device were considered and deemed to have an attack rating of 21 or greater. Attacks that are within scope for the SESIP1 assurance level are those attacks that have an attack rating of 0-15. Therefore, these attacks are out of scope for this evaluation.

Also, public databases were searched for publicly known vulnerabilities:

- Common Vulnerabilities and Exposures (CVE, https://cve.mitre.org)
- Common Weakness Enumeration (CWE, https://cwe.mitre.org)
- Common Attack Pattern Enumeration and Classification (CAPEC, http://capec.mitre.org/data/index.html)

No vulnerabilities were found.

The Arm Cortex-M4 core was also assessed for vulnerabilities, using the databases listed above. No CVEs have been reported, but CWE-1252 mentions the Arm Cortex-M4 in its initial IP configuration. This CWE has been addressed in the Renesas MCU by providing a set of four MPUs - Arm MPU, Bus Master MPU, Bus Slave MPU, and the Security MPU.

3.2 Security Functional Requirements

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 a 16-byte read-only register that contains an ASCII representation of the device part number. The PNRn Part Numbering Registers are documented in the Technical Update ***TN-RA*-A0009A/E***. A part number listing is given in section ***1.3 Part Numbering*** in the Hardware User's Manual (R01UH0886EJ0100).

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.~~

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.

3.2.3 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 a 16-byte read-only register that contains a 16-byte ID code that is guaranteed to be unique for each MCU. The UIDRn Unique ID Registers are documented in the Technical Update ***TN-RA*-A0009A/E***.

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

3.2.4 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, Software Attacker Resistance: Isolation of Platform, and/or Cryptographic KeyStore***.

Conformance rationale:

The platform prevents compromising the SFRs "Verification of Platform Identity" and "Verification of Platform Instance Identity" by placing these values in read-only flash. This prevents an attacker from being able to modify the platform or platform instance identity. These SFRs can be further protected by locking the OCD/Serial Programmer interface, which will prevent an attacker from being able to read these values. See the Technical Update ***TN-RA*-A0009A/E*** for information on the Part Number and Unique ID registers and section ***7.2.4 OCD/Serial Programmer ID Setting Register (OSIS)*** in the Hardware User's Manual (R01UH0886EJ0100) for more information.

The platform prevents compromising the SFR “Software Attacker Resistance: Isolation of Platform” by placing the Security MPU settings in flash and configuring the Security MPU with those settings prior to fetching the reset vector and executing any application code. These registers can be made immutable by using the platform’s Flash Access Window (FAW) to permanently disable the ability to erase and reprogram those registers, either externally or by an application, preventing an attacker from compromising the “Isolation of Platform” SFR. See sections ***16.6 Security MPU*** and ***7.2.3 Access Window Setting Register (AWS)*** in the Hardware User’s Manual (R01UH0886EJ0100) for more information.

The platform prevents compromising the SFRs “Cryptographic KeyStore” by having the capability to store all symmetric and asymmetric private keys in an MCU-uniquely wrapped format. Key wrapping guarantees the authenticity, integrity, and confidentiality of the key – if the wrapped key is altered, it becomes unusable on the MCU that wrapped it, and if it is copied to another MCU, that MCU cannot successfully unwrap it. The platform does not support unwrapping a wrapped key to expose the plaintext key. Wrapped keys stored on the MCU can be further protected by storing them in locked flashed to make them immutable and by locking the debugger/programmer interface. See sections ***46 Secure Crypto Engine (SCE7), 7.2.3 Access Window Setting Register (AWS),*** and ***7.2.4 OCD/Serial Programmer ID Setting Register (OSIS)*** in the Hardware User’s Manual (R01UH0886EJ0100) for more information.

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

The referenced silicon functionality 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.

3.2.5 Software Attacker Resistance: Isolation of Platform

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

Conformance rationale:

The platform contains a dedicated Security MPU, designed to allow the application developer to isolate assets and services in a Trusted region. Documentation of the Security MPU can be found in ***16.6 Security MPU*** of the Hardware User’s Manual (R01UH0886EJ0100). The ***Securing Data at Rest Utilizing the Renesas Security MPU*** Application Project (R11AN0416EU0120) gives information and guidance on how to utilize this feature in an application.

The isolation mechanism 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.

3.2.6 Cryptographic Operation

The platform provides the application with ***the cryptographic operations from Table 1*** functionality with ***the specified algorithms listed in Table 1*** as specified in ***relevant specifications shown in Table 1*** for key lengths ***listed in Table 1*** and modes ***listed in Table 1***.

Table 1 Cryptographic Operations

Algorithm	Operations	Key Length	Modes	Specification
AES	Encryption, decryption	128, 192, 256 bits	ECB, CBC, CTR, CMAC, CCM, GCM, XTS, GCTR	NIST FIPS PUB 197 NIST SP800-38A (ECB, CBC, CTR) NIST SP800-38D (GCM) IETF RFC 3610 (CCM)
RSA	Signature generation, signature verification, public-key encryption, private-key decryption	1024, 2048 bits	n/a	IETF RFC 8017 FIPS PUB 186-4
ECC	Signature generation, signature verification	Curves: NIST P-192, P-224, P-256, P-384; Brainpool P256r1, P384r1, P512r1	n/a	FIPS PUB 186-4
SHA2 Hash	SHA-224, SHA-256	n/a	n/a	FIPS PUB 180-4
HMAC	HMAC-SHA224, HMAC-SHA256 cryptographic hash	224, 256 bits	n/a	FIPS 198-1

Conformance rationale:

The above crypto operations are supported by the Secure Cryptographic Engine (SCE7), as documented in section ***46 Secure Cryptographic Engine (SCE7)*** in the Hardware User's Manual (R01UH0886EJ0100).

The Secure Cryptographic 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.

3.2.7 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, 192, 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. The platform's random number generation capability is described in detail in section **3.2.9 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.

The Secure Cryptographic 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.

3.2.8 Cryptographic KeyStore

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

Conformance rationale:

The platform implements a secure key store by leveraging the secure key handling capabilities of the Secure Crypto Engine (SCE7). An MCU block diagram highlighting the SCE7 is shown in ***Figure 3 Secure Crypto Engine***. The "Key Handling" block inside the Secure Crypto Engine ensures that the cryptographic operations taking place inside the SCE7 do not require any sensitive information to be exposed on a CPU- or externally-accessible bus.

The cryptographic operations of the platform are designed to work with wrapped keys. The Renesas proprietary key wrapping algorithms consist of encryption combined with authentication, which ensures confidentiality, integrity, and authenticity of the wrapped key. Keys that have been generated by or installed using the SCE7 are wrapped using an algorithm that incorporates the MCU's Unique ID. This ensures that even if the wrapped key is copied to another MCU, it cannot be successfully used by code running on that MCU, since only the Secure Crypto Engine of the MCU that wrapped the key can internally unwrap and use that key.

Renesas do not provide a mechanism to unwrap a wrapped key and provide the plaintext key outside of the Secure Crypto Engine; therefore, an application running on the same MCU that wrapped the key is not able to compromise the authenticity, integrity, nor confidentiality of the key. Keys can be further protected by utilising the Security MPU to isolate the key store from the application and by locking the flash blocks that contain any root keys to make them immutable.

Note that for compatibility with legacy systems, the platform supports the capability to use plaintext keys as well as wrapped keys. It is the responsibility of the application developer to properly utilise the secure key installation, generation, and storage capabilities of the platform to fully implement this SFR. Renesas provide software stacks and libraries that support wrapped key usage for various solutions, including a PSA Crypto API implementation and TLS stack. That software is out of scope for this evaluation.

The Secure Cryptographic 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.

3.2.9 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 this function by utilising the True Random Number generation capability of the Secure Crypto Engine inside the MCU. The TRNG implementation consists of an SP800-90A compliant DRBG that is fed by an SP800-90B compliant seed, which is generated from an SP800-22A compliant entropy source. Each TRNG request generates a 128-bit random number.

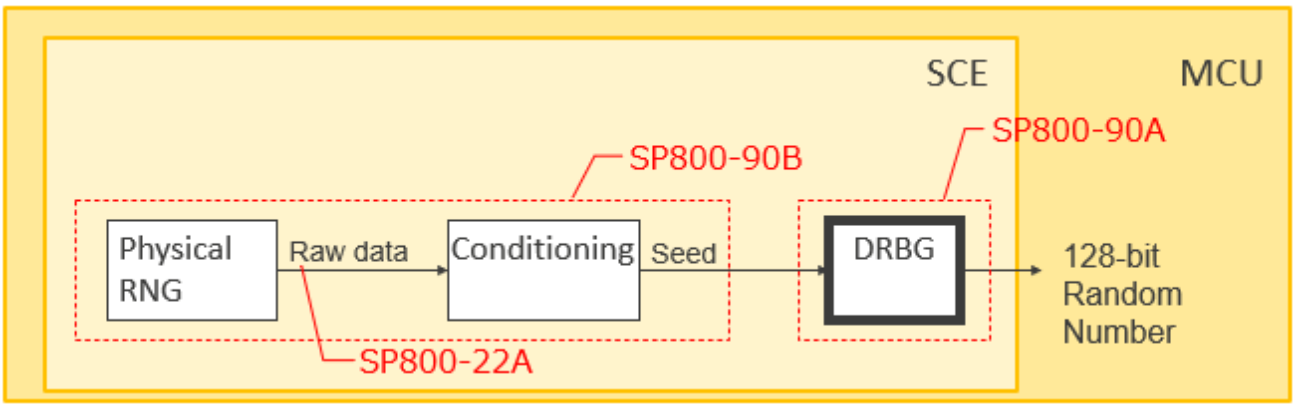

Figure 5 True Random Number Generation

The SCE7 Secure Crypto Engine contained in the Renesas RA6M3 MCU is identical to the SCE7 that is included in Renesas Synergy S5 and S7 Series MCUs. The SCE7 generates an SP800-22A compliant entropy source. It has been tested against and has passed the NIST Statistical Test Suite version 2.1.1, and found to have an entropy of 7.999987 bits per byte when tested with FourmiLab's Pseudorandom Number Sequence Test Program. The SCE7's SP800-90A compliant DBRG has passed NIST CAVP certification:

- Validation list: DRBG
- Certification number: 2152
- Certification link: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=26978

The Secure Cryptographic 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.

4 Mapping and sufficiency rationales

4.1 SESIP1 sufficiency

Assurance Class	Assurance Families	Covered by	Rationale
ASE: Security Target evaluation	ASE_INT.1 ST Introduction	Section "Introduction" and "Title"	The ST reference is in the Title, the TOE reference in the "Platform reference", the TOE overview and description in "Platform functional overview and description".
	ASE_OBJ.1 Security requirements for the operational environment	Section "Security Objectives for the operational environment"	The objectives for the operational environment in "Security Objectives for the operational environment" refers to the guidance documents.
	ASE_REQ.3 Listed Security requirements	Section "Security Functional Requirements"	All SFRs in this ST are taken from [SESIP]. "Verification of Platform Identity" is included. "~~Secure Update of Platform~~" is struck and documented as required.
	ASE_TSS.1 TOE Summary Specification	Section "Security requirements and implementation"	All SFRs are listed per definition, and for each SFR the implementation and verification are defined in Security Functional Requirements.
AGD: Guidance documents	AGD_OPE.1 Operational user guidance	• **R01UH0886EJ0100** *Renesas RA6M3 Group User's Manual: Hardware* • **TN-RA*-A0003A/E**	These documents describe the operation of the platform and how to use the platform to

		Errata for User's Manual: Hardware for SCE7 • **TN-RA*-A0009A/E** *RA family, Addition of register definition for Flash* • **R01AN5372EU0100** *Renesas RA Family System Specifications for Standard Boot Firmware*	create an end application.
	AGD_PRE.1 Preparative procedures	• **R20UT4813EJ0100** *Renesas Flash Programmer v3.08 Flash memory programming software User's Manual* • **R01AN5367EU0100** *Renesas RA Family Flash Memory Programming* • **R11AN0449EU0120** *Renesas RA Family Establishing and Protecting Device Identity using SCE7 and Security MPU* • **R11AN0416EU0120** *Securing Data at Rest Utilizing the Renesas Security MPU Project* • **R01AN5347EU0110** *Arm® Secure Boot Solution for RA6M3 MCU Group Project*	These documents describe how to prepare the platform as part of an end product.
ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures	Section "Flaw Reporting Procedure (ALC_FLR.2)"	The flaw reporting and remediation procedure is described.
AVA_VAN.1	AVA_VAN.1 Vulnerability survey	Section "Vulnerability	The vulnerability survey and

		Survey (AVA_VAN.1)”	associated test results are described.

5 References

[ARM PSA L1] ARM PSA Certified™ Level I Questionnaire, Document reference JSADEN0001, Version 1.0, dated 25/02/2019

[SESIP] GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.0, March 2020