Security Policy

RX65N-2MB Security Management Module

FIPS 140-2 Non-Proprietary Security Policy

Document Version: Ver. 1.02
Revision Data: Dec. 10. 2020

Renesas Electronics
www.renesas.com

Table of Contents

1. Cryptographic Module Specification

This document sets forth the non-proprietary security policy pertaining to the RX65N-2MB Security Management Module, a cryptographic module manufactured by Renesas Electronics Corporation. The cryptographic functions of the module are implemented in the Trusted Secure IP (TSIP) security hardware IP developed by Renesas Electronics Corporation and firmware (TSIP driver). The TSIP integrates a cryptographic engine and a random number generator circuit, and it is controlled by TSIP driver that enables execution of cryptographic algorithms, key management, secure boot, and secure firmware updating. Fig. 1-1 shows the external appearance of the module, and Fig. 1-2 illustrates the module architecture.

This document is provided as a reference for developers creating FIPS 140-2–compliant products using the RX65N-2MB.

The approved version is shown in 1.2. An environment used as reference model uses the module mounted on Renesas Starter Kit+ for RX65N-2MB(see Fig. 1-3, Fig. 1-4). On the module, the system keys have already been installed. The module implementing User Application using this module needs to obtain certification separately.

Fig. 1-1 RX65N-2MB (R5F565NEHDFC) Chip

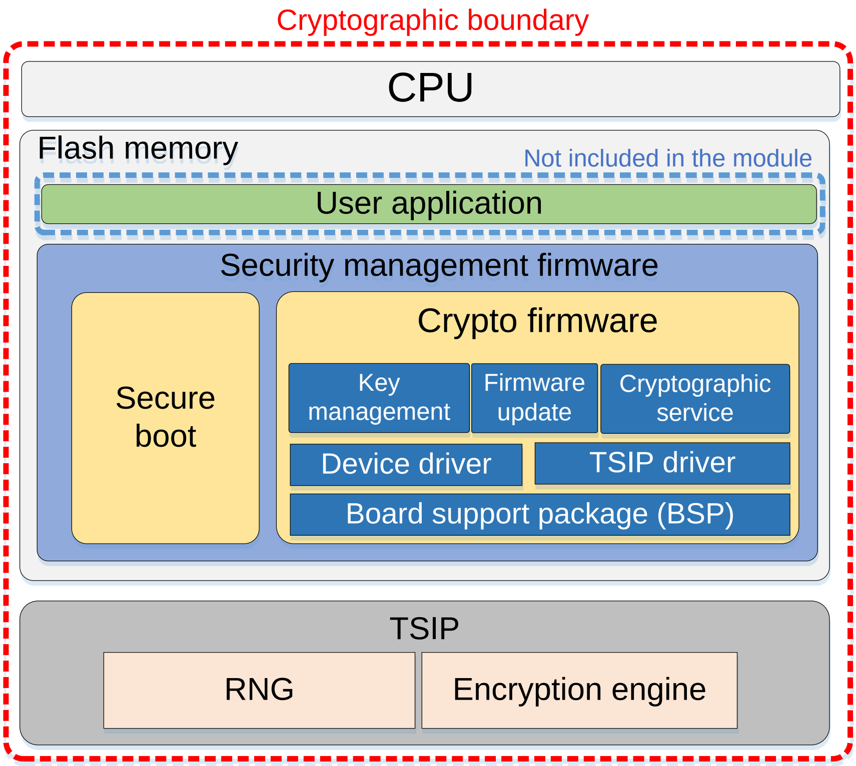

Fig. 1-2 Module Architecture

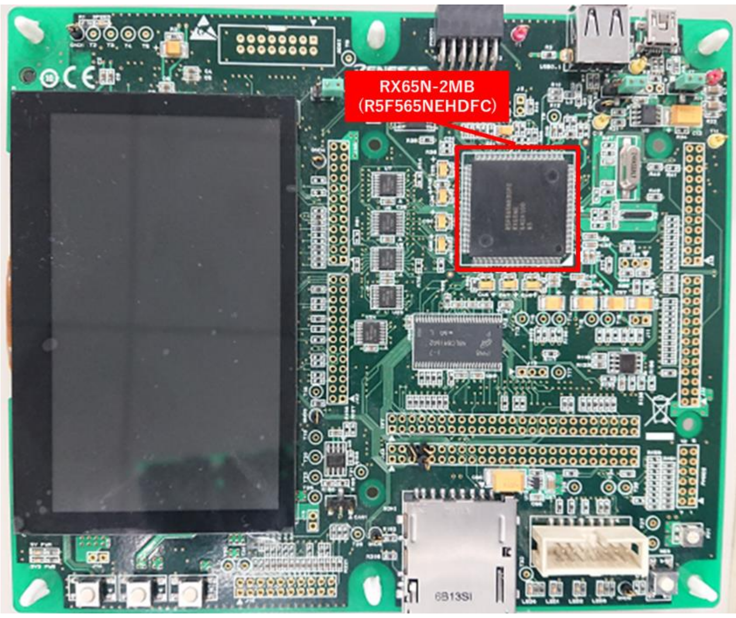

Fig. 1-3 Top View of Renesas Starter Kit+ for RX65N-2MB

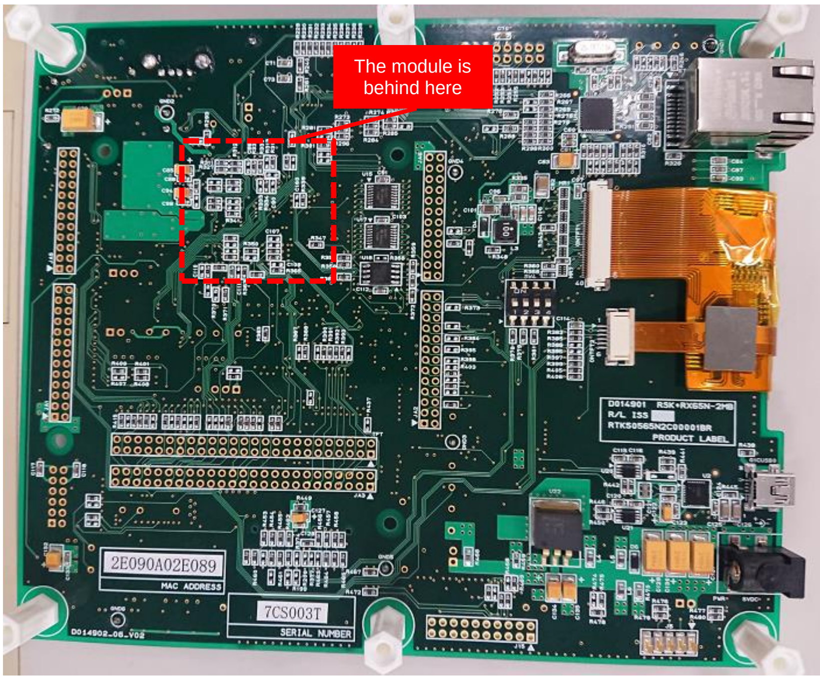

Fig. 1-4 Bottom View of Renesas Starter Kit+ for RX65N-2MB

1.1 Security Levels

The RX65N-2MB Security Management Module operates at security level 3 as defined under FIPS 140-2. Table 1-1 lists the security levels of the areas for which security requirements are specified in FIPS 140-2.

Table 1-1 Security Levels

Security Requirement	Security Level
Cryptographic module specification	3
Port and interface	3
Roles, services, and authentication	3
Finite state model	3
Physical security	3
Operational environment	N/A
Cryptographic key management	3
EMI/EMC	3
Self-test	3
Design assurance	3
Mitigation of other attacks	N/A

1.2 Hardware Part No. and Firmware Versions

Table 1-2 Hardware and Firmware Versions

Hardware Part No.	Firmware Version	
	Secure Boot	Crypto Firmware
R5F565NEHDFC	Ver. 1.00	Ver. 1.00

1.3 Approved Security Functions and Modes of Operation

1.3.1 Approved Security Functions

Table 1-3 lists the FIPS-approved cryptographic functions supported by the module.

When the module is power-on and the power-up self-test is successful, it enters the FIPS-approved mode and an operator can use the following cryptographic functions.

If an operator performs the Get Status service and the module response it, this also shows that the module is in the approved mode of operation.

Table 1-3 Approved Security Functions

CAVP	Algorithm	Prerequisite	Mode/Method	Standard	Key Length	Usage
C953	AES	-	ECB, CBC	FIPS-197, SP800-38A	128, 256	Encryption/decryption
		-	GCM	FIPS-197, SP800-38D	128, 256	Authenticated encryption
		-	CMAC	FIPS-197, SP800-38B	128, 256	Message authentication
		-	CCM	FIPS-197, SP800-38C	128, 256	Authenticated encryption
C953[1]	RSA	SHA-256	RSASSA-PKCS-v1_5	FIPS 186-4	2048	Signature generation
		SHA-1 SHA-256			1024, 2048	Signature verification
C953	SHA-1 SHA-256	-	-	FIPS-180-3	-	Hash value generation
C953	CTR_DRBG	AES	-	SP800-90A	128	Random number generation
C953	KBKDF	CMAC AES	Counter mode	SP800-108	128	Key-based key derivation

1.3.2 Allowed Security Functions

The module supports allowed cryptographic functions shown in Table 1-4.

Table 1-4 Allowed cryptographic functions

Algorithm	Usage
NDRNG	CTR_DRBG seed generation Tested with SP800-22

[1] RSA signature Generation with SHA-1 has also obtained CAVP certification but the module doesn't provide service using that cryptographic function.

1.3.3 Non-Approved Security Functions

Services support the approved or allowed cryptographic functions of the module only. Therefore, non-approved cryptographic functions are not supported.

1.4 Components and Cryptographic Boundary

1.4.1 Cryptographic Boundary

The cryptographic boundary of this module is a perimeter of the IC chip shown in Fig. 1-1. The physical boundary is described by the red dotted line in Fig. 1-2. The logical cryptographic boundary is represented by the red dotted line excluding “User Application” surrounded by the blue dotted line in Fig. 1-3.

1.4.2 Hardware Components

Fig. 1-5 shows the hardware components of the RX65N-2MB. The physical form of the module is a single chip, and the gray dotted line in Fig. 1-5 represents the physical cryptographic boundary. The firmware of the module is stored in the flash memory within physical boundary, and performs processing using the RX CPU.

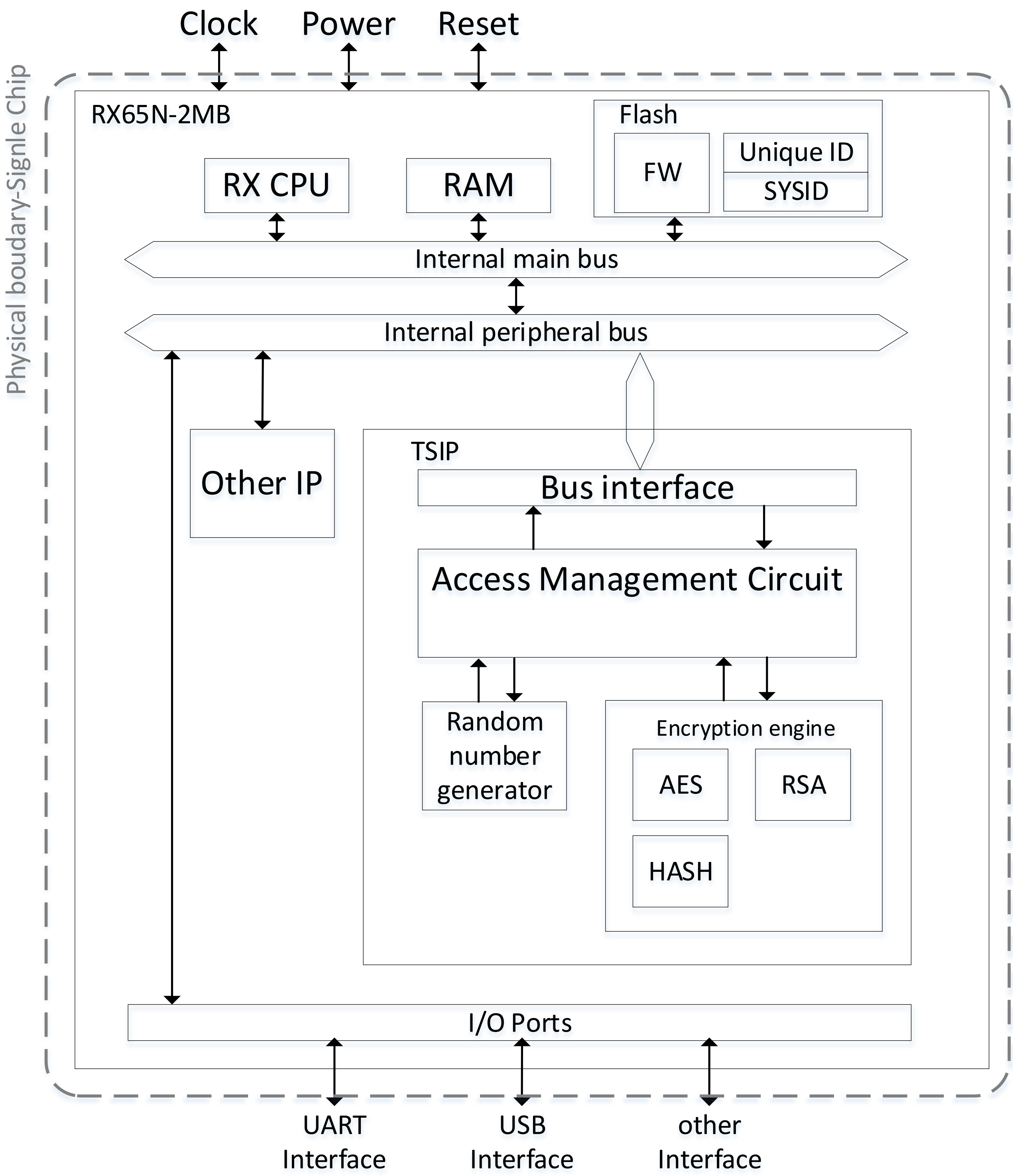

Fig. 1-5 Hardware Components

1.4.3 Firmware Components

Security management firmware is provided as part of the module to enable the TSIP to execute cryptographic services appropriately. The firmware is composed of Secure Boot, which performs startup processing, and Crypto Firmware, which performs processing after startup. Fig. 1-2 shows the firmware architecture.

2. Ports and Interfaces

Table 2-1 lists the relationship between physical ports and logical interfaces of the RX65N-2MB. As shown in Fig. 1-5, the data I/O interfaces for UART, USB, etc., are all implemented by means of I/O ports. The I/O ports function as general-purpose I/O ports, peripheral module inputs and outputs, interrupt input pins, or bus control pins according to register settings matching the characteristics of the user system. For details, refer to RX65N Group, RX651 Group User's Manual: Hardware (https://www.renesas.com/us/en/doc/products/mpumcu/doc/rx_family/r01uh0590ej0210-rx651.pdf).

Table 2-1 The relationship between physical ports and logical interfaces

Logical Interface Definition	Ports
Control Input	Clock
	Reset
	I/O ports (USB interface)
Status Output	I/O ports (LED interface[2], etc.)
Data Input	I/O ports (UART interface, USB interface)
Data Output	I/O ports (UART interface, USB interface)
Power	Power

Also, the module has interfaces to User Application as follows:

Control input interface: Firmware API calls

Status output interface: Firmware API return values

Data input interface: Firmware API input arguments

Data output interface: Firmware API output arguments

[2] These ports of the module mounted on Renesas Starter Kit+ for RX65N-2MB are connected to the LEDs on the board.

3. Roles, Services, and Authentication

3.1 Roles

The module supports two roles: a crypto officer role and a user role. Each of these roles are authenticated by means of an ID and password. There is no support for a maintenance role.

3.1.1 Crypto Officer Role

The crypto officer role can perform services related to approved security functions, services not related to security, firmware updates, adding users, and CSP zeroization.

3.1.2 User Role

The user role can perform services related to approved security functions, services not related to security and firmware updates.

3.2 Services

Table 3-1 shows the roles corresponding to the services supported by the module. All services are run by means of crypto firmware APIs. The roles that can perform each service are shown in the Role column. The CSPs/PSPs column lists the CSPs/PSPs accessed by each service. For details of CSPs, refer to Table 5-1, CSP List. For details of PSPs, refer to Table 5-2 PSP List.

- No role required — Usable whether or not a role is assigned.
- CO — Available when in CO role.
- User — Available when in User role.

- R— Read from internal storage.
- W— Write to internal storage.
- EX—Execute.
- Z— Zeroize.

Table 3-1 Services

Service Name	Description	Role	CSPs/PSPs
Power Up Self-Test	Runs automatically after module startup. Refer to section 7.1 for the test items.	No role required	user_aes128_program_mac_key：EX
Get Status	Displays the FSM status.	No role required	N/A
Get User List	Displays a list of users.	No role required	N/A
Indicate Error	Displays the error status. Outputs a signal from pin 93 when an error occurs.	No role required	N/A
Set Crypto Officer Password	Sets the password for the crypto officer role at initial module startup.	CO	Decryption_key_for_user_aes128_password_key：W, R user_aes128_password_key：R Password：W
User Authentication	Authenticate the user using its ID and password.	No role required	Decryption_key_for_user_aes128_response_mac_key：W, R user_aes128_response_mac_key：R Password：R, EX
Add User	Adds a user.	CO	Decryption_key_for_user_aes128_password_key：W, R user_aes128_password_key：R Password：W
Firm Update	Updates the firmware. Executes a load test on the firmware to be updated. Refer to the section 7.2.1 for the test detail.	CO User	Decryption_key_for_user_aes128_program_mac_key：W, R user_aes128_program_mac_key：R session_key0：W, EX session_key1：W, EX
CSP zeroization	Zeroizes the CSPs. Removes the TSIP driver from the flash memory.	CO	Key derivation root key：Z
TSIP Open	Enables the TSIP functions.	CO User	N/A
TSIP Close	Disables the TSIP functions.	CO User	N/A
AES Encryption / Decryption	Encrypts/Decrypts using AES. Mode：ECB, CBC, GCM, CCM Key length：128 / 256 bit	CO User	Decryption_key_for_user_aes128_key：W, R user_aes128_key：R, EX or Decryption_key_for_user_aes256_key：W, R user_aes256_key：R, EX
AES-CMAC MAC Generation / Verification	Generates/Verifies a MAC using AES-CMAC. Key length：128 / 256 bit	CO User	Decryption_key_for_user_aes128_key：W, R user_aes128_key：R, EX or Decryption_key_for_user_aes256_key：W, R user_aes256_key：R, EX

RSASSA-PKCS-V1.5 Signature Generate / Verification	Generates/Verifies a signature using RSASSA-PKCS-V1.5. Signature generation: 2048-bit Signature verification: 1024-bit or 2048-bit	CO User	MAC_key_for_user_rsa1024_ne_key：W, R Decryption_key_for_user_rsa1024_nd_key：W, R user_rsa1024_ne_key：R, EX user_rsa1024_nd_key：R, EX or MAC_key_for_user_rsa2048_ne_key：W, R Decryption_key_for_user_rsa2048_nd_key：W, R user_rsa2048_ne_key：R, EX user_rsa2048_nd_key：R, EX
Hash value generate	Generates a hash value using SHA-1 or SHA-256.	CO User	N / A
Random Number Generate	Outputs a 128-bit random numbers. Executes a continuous random number generator test for the random numbers output. Refer to the section 7.2.2 for the test detail.	CO User	DRBG internal state：R, W

3.3 Authentication

ID-based user authentication is required in order to use an approved cryptographic service. The authentication method is challenge-response. When a user makes a login request to the module, the user receives a 16-byte random number. The user calculates the response data from the received random number and the user's own password by the following calculating formula and inputs it to the response verification API. An error will occur if the User Authentication service is executed after user authentication has completed. If another user needs to login, it's necessary to logout.

Response value (128 bits) = AES-128 CMAC (Key, SHA-256 (password) || random (128 bits))

User ID: Character string consisting of 8 to 16 characters
Password: Character string consisting of 8 to 16 characters
Challenge code: 16-byte random number

Table 3-2 Authentication Description

Authentication Method	Probability of a Single Successful Random Attempt	Probability of a Successful Attempt within a Minute
Challenge response authentication method	1/2^128 The probability that a random attempt will succeed, or a false acceptance will occur depends on the 128-bit MAC value. Therefore, the probability is 1/2^128, which is less than 1/1,000,000.	60,000/2^128 Since authentication requires more than 1ms, in a worst-case scenario, the module can perform 60,000 per minute. Therefore, the probability that multiple attacks within a given minute will be successful is 60,000/2^128, which is less than 1/100,000.

4. Physical Security

The RX65N-2MB is a commercial-grade IC as defined under FIPS 140-2, and it is designed to meet the physical security requirements of level 3. The RX65N-2MB is treated with a hard, opaque coating designed to leave evidence of tampering. This coating is hard enough to prevent easy access to the circuit layer of the chip. Any physical attack that involves removing the chip from the module will damage the chip and render the functions of the cryptographic module unusable.

The physical security described above is guaranteed under the conditions used for testing. The module has been tested at ambient temperature, and it is not guaranteed to provide physical security conforming to security level 3 at other temperatures.

5. Cryptographic Key Management

5.1 CSPs and PSPs

The CSPs and PSPs used by the cryptographic module are shown below.

5.1.1 CSP List

Table 5-1 lists the CSPs used by the module.

Table 5-1 CSP list

CSP Identifier	Description
User Keys	User keys enable the user application to use cryptographic services (encrypting/decrypting, generating/verifying signatures, and message authentication). The types of User Keys are listed below. ・user_aes128_key Key used when running an AES algorithm with a key length of 128 bits. ・user_aes256_key Key used when running an AES algorithm with a key length of 256 bits. ・user_aes128_program_mac_key Key for decrypting a session keys (session_key0, session_key1) for firmware updating and calculating firmware MAC values. ・user_aes128_password_key Key for decrypting a password when starting Set Crypto Officer Password service or Add User service. ・user_aes128_usertable_mac_key Key for calculating user table area[3] MAC values. ・user_aes128_response_mac_key Key for calculating user authentication’s response. ・user_rsa1024_nd_key Private key used when running an RSA algorithm with a key length of 1,024 bits. ・user_rsa2048_nd_key Private key used when running an RSA algorithm with a key length of 2,048 bits. size - 128 / 256bit for AES, 1024 / 2048bit for RSA

[3] User table area is the area on the Flash memory storing User IDs and Passwords.

	Entry – Enter during manufacturing Output - n/a Storage - Internal register of TSIP[4] (plain) Flash memory(encrypted) Zeroization – volatile memory: Power off
Password	Password used in user authentication. size - 128bit Entry - Enter in encrypted form with Set Crypto Officer Password service or Add User service. Output - n/a Storage – RAM, Internal register of TSIP (plain) Flash memory (hashed) Zeroization – volatile memory: Power off
SP800-90A DRBG seed	Seed input to the deterministic random bit generator. size - 256bit Entry - n/a Output - n/a Storage – Internal register of TSIP Zeroization – Power off
SP800-90A DRBG internal state ("V" and "Key")	Internal state of SP800-90A DRBG. size - 256bit Entry – n/a Output - n/a Storage - Internal register of TSIP Zeroization - Power off
session_key0 (load firmware decryption key)	Key used to decrypt the firmware to be updated. size - 128bit Entry - Enter in encrypted format in Firm Update service.

[4] Internal register of TSIP is a volatile memory.

	Output - n/a Storage - Internal register of TSIP (plain) RAM (encrypted) Zeroization – Power off
session_key1 (load firmware MAC key)	Key used to calculate MAC value for firmware to be updated. size - 128bit Entry – Enter in encrypted format in Firm Update service. Output - n/a Storage - Internal register of TSIP (plain) RAM (encrypted) Zeroization – Power off
User Key Decryption Keys	Decryption key for User Keys as CSP. Derived for each User Keys. ・Decryption_key_for_user_aes128_key ・Decryption_key_for_user_aes256_key ・Decryption_key_for_user_aes128_program_mac_key ・Decryption_key_for_user_aes128_password_key ・Decryption_key_for_user_aes128_usertable_mac_key ・Decryption_key_for_user_aes128_response_mac_key ・Decryption_key_for_user_rsa1024_nd_key ・Decryption_key_for_user_rsa2048_nd_key size - 128bit Entry –n/a(Derived within the cryptographic module) Output - n/a Storage - Internal register of TSIP (plain) Zeroization – Power off
User Key MAC Keys	AES CMAC calculation key for User Keys as PSP. Derived for each User Keys. ・MAC_key_for_user_rsa1024_ne_key ・MAC_key_for_user_rsa2048_ne_key

	size - 128bit Entry –n/a (Derived within the cryptographic module) Output - n/a Storage - Internal register of TSIP (plain) Zeroization – Power off
Key Derivation Root Key	Root key for deriving the User Key Decryption Keys and User Key MAC Keys. size - 128bit Entry - Enter during manufacturing Output - n/a Storage - Internal register of TSIP (plain) Flash memory (Obfuscated[5])) Zeroization – volatile memory: Power off Flash memory: Execute CSP zeroization service

[5] At the time of storage, the key value is processed with data based on the device-specific information.

5.1.2 PSP List

Table 5-2 lists the PSPs used by the module.

Table 5-2 PSP List

PSP Identifier	Description
User Keys	User keys enable the user application to use cryptographic services (encrypting/decrypting, generating/verifying signatures, and message authentication). The types of public keys amongst User Keys are listed below. • user_rsa1024_ne_key Key used when running an RSA algorithm with a key length of 1,024 bits. • user_rsa2048_ne_key Key used when running an RSA algorithm with a key length of 2,048 bits. Size: 1,024 or 2,048 bits Entry: Enter during manufacturing Output: n/a Storage: Flash memory

5.2 Random Number Generation

The DRBG used for random number generation is CTR_DRBG using AES-128 without a derived function. DRBG seed uses NDRNG output. The NDRNG consists of the oscillator of the entropy source and the circuit of the conditioning component CBC-MAC (AES-128). The minimum entropy of the entropy source is 7.98 bits per 8 bits. NDRNG is implemented to provide the full entropy (256bit) required for seed of CTR_DRBG by passing the conditioning component.

5.3 Key Zeroization

The key derivation root key on the Flash memory is zeroized when the CSP zeroization service is executed. When the CSP zeroization service is executed, the zeroization process starts immediately, and the Flash area storing the CSP is erased (overwritten with 1s).

User Keys and Password, which are CSPs on the Flash memory, are not subject to zeroization because they are encrypted by AES-128 CCM and hashed by SHA-256 respectively, which are approved security functions. Each CSP in the volatile memory is zeroized immediately after the power is turned off.

6. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators provides an exemption from its requirements for peripheral devices and subassemblies sold as components to manufacturers. The present module must undergo EMI/EMC testing if it will be incorporated into a product.

7. Self-Tests

The module performs power-up self-tests and conditional self-tests in accordance with the requirements of FIPS 140-2.

7.1 Power-Up Self-Tests

The module runs the self-tests described below after power-on or a power-on reset. If a failure occurs in any of the power-up self-tests, the module enters an error state in which all of the cryptographic services are unusable. If the power-up self-tests complete successfully, the cryptographic services of the module become usable. To perform an on demand self-test, turn off / on the module power again or reset the module.

7.1.1 Cryptographic Algorithm Test

As one of its power-up self-tests, the module runs known-answer tests (KATs) using the following cryptographic algorithms:

- AES encryption and decryption, in ECB, CBC, GCM, CCM modes, using 128- and 256-bit key sizes.
- MAC generation and verification in CMAC mode, using 128- and 256-bit key sizes.
- Hash generation with SHA-1 and SHA-256.
- RSA signature generation with 2048-bit modulus, using RSASSA-PKCS-v1_5.
- RSA signature verification with 1024-bit and 2048-bit modulus, using RSASSA-PKCS-v1_5.
- Random Number Generation using DRBG (SP 800-90A DRBG health testing for instantiate and generate functions)
- Key Derivation Function using CMAC AES-128 Counter mode.

7.1.2 Firmware Integrity Test

After a power-on reset, the module runs a secure boot program and performs a firmware integrity test. The Crypto Firmware is verified by the MAC value using AES-128 CMAC algorithm, and the Secure Boot is verified by the hash value using SHA-1 algorithm.

The User Application is verified by the MAC value using the AES-128 CMAC algorithm together with the Crypto Firmware.

7.2 Conditional Tests

7.2.1 Firmware Load Test

The module performs a firmware load test when updating the firmware. The reliability of the loaded firmware is verified by the MAC value using the AES-128 CMAC algorithm. The firmware loaded may include User Application as well as Crypto Firmware.

Note: Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

7.2.2 Continuous Random Number Generator Test

A continuous random number generator test is run before the DRBG, an approved random number generator, is used. This test checks whether or not the generated output block is equal to the random number block generated previously, and if they differ, the output block is used as a random number.

8. Mitigation of Other Attacks

The cryptographic module is not designed to mitigate specific attacks.

9. Guidance

9.1 Crypto Officer Guidance

- Receipt and initial settings

This module is distributed in a state implemented in the Renesas Starter Kit + for RX65N-2MB. If there is no problem with the received kit, connect to the PC immediately and update the Crypto Officer password from the default value.

See" RX65N-2MB Security Management Module" User Guide Rev.1.0" for details.

- Ports and interfaces

Refer to "RX65N Group, RX651 Group User's Manual: Hardware, RENESAS 32-Bit MCU, RX Family/RX600 Series, Rev.2.30. Jun 2019" for the hardware ports and interface of this module.

Refer to the" RX65N-2MB Security Management Module, Rev.1.00, 2019.09.19" for the logical interface used by the User Application.

- Usage Guidelines
    - Keys used for each cryptographic service

    When executing cryptographic service, the necessary keys are used depending on the processing of each service. Even if an User Application directly accesses the key stored in the Flash memory, the key cannot be used.

    - Using of AES-GCM

    When using GCM in this module, the IV generation method shall comply with IG A.5 Scenario 2. Use the Random Number Generate service to generate an IV inside the module's physical boundary. The IV needs to be a random string that length is at least 96-bits obtained from the service. This method is based on the RBG-based Construction specified in NIST SP 800-38D section 8.2.2.

9.2 User Guidance

- Ports and interfaces

Refer to" RX65N Group, RX651 Group User's Manual: Hardware, RENESAS 32-Bit MCU, RX Family/RX600 Series, Rev.2.30. Jun 2019" for the hardware ports and interface of this module.

Refer to the" RX65N-2MB Security Management Module, Rev.1.00, 2019.09.19" for the logical interface used by the User Application.

- Usage Guidelines
    - Keys used for each cryptographic service

    When executing cryptographic service, the necessary keys are used depending on the processing of each service. Even if an User Application directly accesses the key stored in the Flash memory, the key cannot be used.

    - Using of AES-GCM

    When using GCM in this module, the IV generation method shall comply with IG A.5 Scenario 2. Use the Random Number Generate service to generate an IV inside the module's physical boundary. The IV needs to be a random string that length is at least 96-bits obtained from the service. This method is based on the RBG-based Construction specified in NIST SP 800-38D section 8.2.2.

10. Glossary

Terms	Description
RX65N-2MB	Product No.: R5F565NEHDFC (equipped with encryption function, code flash: 2 MB, pin count: 176)
TSIP	Trusted Secure IP
CPU	Central Processing Unit
RNG	Random Number Generator
FIPS	Federal Information Processing Standards
API	Application Programming Interface
UART	Universal Asynchronous Receiver/Transmitter
MAC	Message Authentication Code
DRBG	Determine Random Bit Generator
NDRNG	Non-Deterministic Random Number Generator
CSP	Critical Security Parameter
PSP	Public Security Parameter
KAT	Known Answer Test