

Renesas Electronics Corporation

RA8M1 Security Management Module

FIPS 140-3 Non-Proprietary Security Policy
Revision 1.01

Table of Contents

1 General	5
1.1 Overview	5
1.2 Security Levels	5
2 Cryptographic Module Specification	5
2.1 Description	5
2.2 Tested and Vendor Affirmed Module Version and Identification	7
2.3 Excluded Components	8
2.4 Modes of Operation	8
2.5 Algorithms	8
2.6 Security Function Implementations	10
2.7 Algorithm Specific Information	14
2.8 RBG and Entropy	14
2.9 Key Generation	14
2.10 Key Establishment	15
2.11 Industry Protocols	15
3 Cryptographic Module Interfaces	15
3.1 Ports and Interfaces	15
4 Roles, Services, and Authentication	15
4.1 Authentication Methods	15
4.2 Roles	16
4.3 Approved Services	16
4.4 Non-Approved Services	24
4.5 External Software/Firmware Loaded	24
5 Software/Firmware Security	24
5.1 Integrity Techniques	24
5.2 Initiate on Demand	24
6 Operational Environment	24
6.1 Operational Environment Type and Requirements	24
7 Physical Security	25
7.1 Mechanisms and Actions Required	25
8 Non-Invasive Security	25
9 Sensitive Security Parameters Management	25
9.1 Storage Areas	25
9.2 SSP Input-Output Methods	25
9.3 SSP Zeroization Methods	26

9.4 SSPs	27
10 Self-Tests.....	33
10.1 Pre-Operational Self-Tests	33
10.2 Conditional Self-Tests.....	34
10.3 Periodic Self-Test Information.....	36
10.4 Error States	37
11 Life-Cycle Assurance	37
11.1 Installation, Initialization, and Startup Procedures.....	37
11.2 Administrator Guidance	38
11.3 Non-Administrator Guidance.....	38
11.4 Design and Rules	38
11.5 Maintenance Requirements	38
11.6 End of Life	38
12 Mitigation of Other Attacks	38

List of Tables

Table 1: Security Levels	5
Table 2: Tested Module Identification – Hardware	7
Table 3: Modes List and Description	8
Table 4: Approved Algorithms	10
Table 5: Vendor-Affirmed Algorithms	10
Table 6: Non-Approved, Allowed Algorithms with No Security Claimed.....	10
Table 7: Security Function Implementations.....	14
Table 8: Entropy Certificates	14
Table 9: Entropy Sources.....	14
Table 10: Ports and Interfaces	15
Table 11: Authentication Methods.....	16
Table 12: Roles.....	16
Table 13: Approved Services	24
Table 14: Mechanisms and Actions Required	25
Table 15: Storage Areas	25
Table 16: SSP Input-Output Methods.....	26
Table 17: SSP Zeroization Methods.....	26
Table 18: SSP Table 1	29
Table 19: SSP Table 2.....	33
Table 20: Pre-Operational Self-Tests	34
Table 21: Conditional Self-Tests	36
Table 22: Pre-Operational Periodic Information.....	36
Table 23: Conditional Periodic Information.....	37
Table 24: Error States.....	37

List of Figures

Figure 1 RA8M1 (R7FA8M1AHECBD) Chip.....	6
Figure 2 Block Diagram.....	6
Figure 3 Tamper-evident Coating on Chip.....	25

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the RA8M1 Security Management Module from Renesas Electronics Corporation. It describes how the module meets the requirements of Security Level 2 as defined in FIPS 140-3.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	2
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

RA8M1 Security Management Module is a hardware cryptographic module certified at FIPS 140-3 Security Level 2. RA8M1 is general-purpose microcontroller designed for industrial, IOT, and infrastructure applications, embedded with robust security features. This module is provided as a reference for developing FIPS 140-3-compliant modules using the RA8M1. By referring to the design of this module, it becomes easier to address FIPS requirements when developing cryptographic modules using the RA8M1 in customer environments.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics:

N/A for this module.

Cryptographic Boundary:

The cryptographic boundary is defined as the perimeter of the IC package as shown in Figure 1.



Figure 1 RA8M1 (R7FA8M1AHECBD) Chip

Tested Operational Environment's Physical Perimeter (TOEPP):

The block diagram of the RA8M1 Security Management Module is shown Figure 2. This module provides the services required by FIPS 140-3 and can execute those services by entering string commands via UART. The services provided by the module are implemented in Crypto Firmware. When developing FIPS 140-3 compliant products using RA8M1, implementing only the User Application part can make the certification process easier.

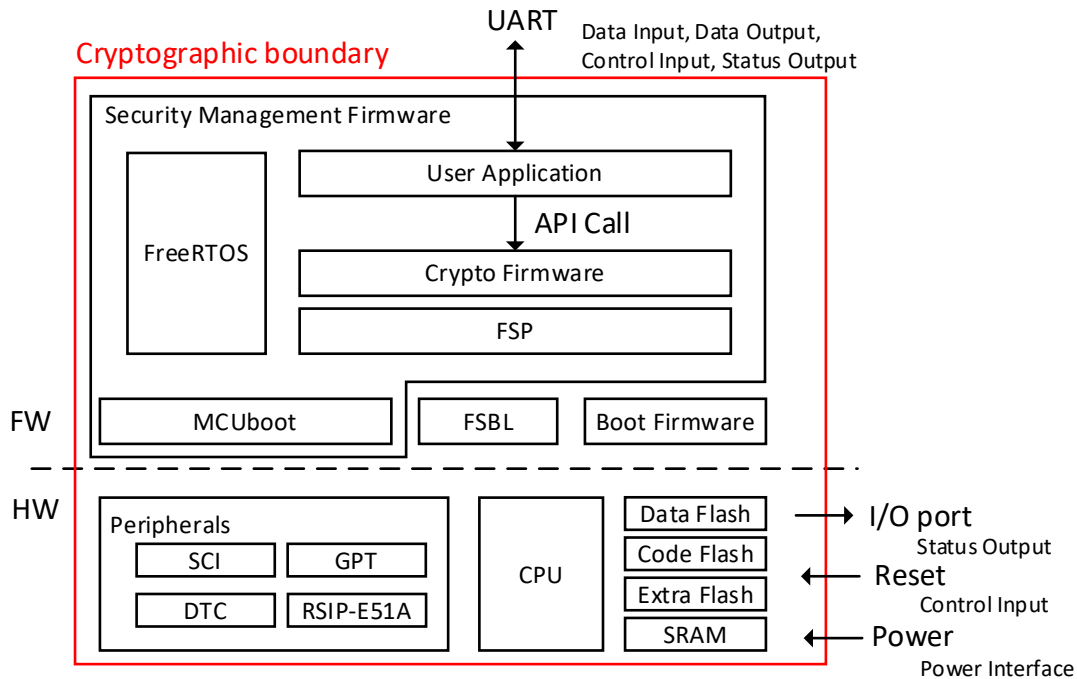


Figure 2 Block Diagram

Component	Description
FW	
Security Management Firmware	Implement functionality that complies with FIPS 140-3 requirements, using the Crypto Firmware API as its interface.
User Application	Parses serial data received via UART and performs the corresponding cryptographic service. This module is designed to serve as a reference for developing cryptographic modules that conform to CMVP, requiring modifications only to the User Application.

Component		Description
	Crypto Firmware	Provides the following services to meet FIPS 140-3 requirements - FSM - User authentication - Module version and status display - Cryptographic services - Self-test
	FreeRTOS	Task scheduling
	FSP	RA Flexible Software Package
	MCUboot	For pre-operational self-test, FW Load Test, and part of CASTs
FSBL		First Stage Boot Loader. Verifies the integrity and authenticity of an MCUboot
Boot Firmware		For module initialization.
HW		
Peripherals		-
	GPT (General PWM Timer)	For measuring command time out.
	RSIP-E51A (Renesas Secure IP)	For cryptographic services
	SCI (Serial Communication Interface)	For data input/output, control input and status output.
	DTC (Data Transfer Controller)	For data transfer via SCI
CPU		Arm Cortex-M33
Data Flash		Flash memory for data store
Code Flash		Flash memory for code store
Extra Flash		Access Restricted Flash Memory
SRAM		Static Random Access Memory

*CAVP certified (A7184) RSIP-E51A Protected Mode for RA Family v 2.1.0 consists of RSIP-E51A, and FSP that is included in Security Management Firmware version 1.01.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
RA8M1 Security Management Module	R7FA8M1AHECBD	Security Management Firmware version: 1.01, FSBL: R7FA8M1AHECBD, Boot Firmware Version: V3.6.32	Arm® Cortex®-M85	

Table 2: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 Excluded Components

- **Boot Firmware**
The Boot Firmware is used only during the initialization of the module, and after the initialization is complete, it can't be used permanently due to the Device Lifecycle Management capability of the RA8M1. Therefore, it is an excluded firmware component.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	Approved security services are available.	Approved	The successful completion of a service

Table 3: Modes List and Description

The module starts as an approved mode of operation after starting up in Single-Chip mode. To start in Single-Chip mode, set the voltage on the MD pin of RA8M1 to “High” and release reset.

Mode Change Instructions and Status:

N/A for this module.

Degraded Mode Description:

N/A for this module.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-CTR, AES-ECB	A7184	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CCM	A7184	Key Length - 128, 256	SP 800-38C

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A7184	Direction - Generation, Verification Key Length - 128, 256	SP 800-38B
AES-GCM	A7184	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256	SP 800-38D
AES-KW	A7184	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 256 Payload Length - Payload Length: 128, 256	SP 800-38F
Conditioning Component AES-CBC-MAC SP800-90B	A7184	Key Length - 256 Payload Length - Payload Length: 1024	SP 800-90B
Counter DRBG	A7184	Prediction Resistance - No Supports Reseed - No Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0 Returned Bits - 128	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A7184	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A7184	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A7184	Component - No Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA2-512/224, SHA2-512/256	FIPS 186-5
HMAC-SHA2-256	A7184	MAC - MAC: 256 Key Length - Key Length: 256	FIPS 198-1
HMAC-SHA2-384	A7184	MAC - MAC: 384 Key Length - Key Length: 384	FIPS 198-1
HMAC-SHA2-512	A7184	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1
KDF SP800-108	A7184	KDF Mode - Counter MAC Mode - CMAC-AES128, CMAC-AES256 Supported Lengths - Supported Lengths: 128, 256 Fixed Data Order - Before Fixed Data Counter Length - 8	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Supports Empty IV - No Requires Empty IV - No Custom Key In Length - 0	
RSA KeyGen (FIPS186-5)	A7184	Key Generation Mode - probable Modulo - 2048, 3072, 4096 p mod 8 - 0 Primality Tests - 2pow100 q mod 8 - 0 Fixed Public Exponent - 010001 Info Generated By Server - No Private Key Format - standard Public Exponent Mode - fixed	FIPS 186-5
RSA SigGen (FIPS186-5)	A7184	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1	FIPS 186-5
RSA SigVer (FIPS186-5)	A7184	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5, pss Mask Function - mgf1 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA2-256, SHA2-384, SHA2-512	A7184	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	SP800-133r2 Section 4, example1

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES-128 CBC-MAC	no security claimed	For interoperability, performed along with inputting User key.

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES encryption/decryption	BC-UnAuth	Encryption/decryption using AES ciphers	key strength:128, 256 bit	AES-ECB: (A7184) AES-CBC: (A7184) AES-CTR: (A7184)
Authenticated AES encryption/decryption	BC-Auth	Authenticated encryption/decryption using AES ciphers	key strength:128, 256 bit	AES-CCM: (A7184) AES-GCM: (A7184)
AES-CMAC generation/verification	MAC	AES CMAC generation / verification	key strength:128, 256 bit	AES-CMAC: (A7184)
HMAC generation/verification	MAC	HMAC generation / verification	key length:256, 384, 512 bit	HMAC-SHA2-256: (A7184) HMAC-SHA2-384: (A7184) HMAC-SHA2-512: (A7184)
RSA Signature Generation and Verification	DigSig-SigGen DigSig-SigVer	RSA Signature generation / Verification	signature Type:PKCS 1.5, pss key length:2048, 3072, 4096 bit	RSA SigGen (FIPS186-5): (A7184) RSA SigVer (FIPS186-5): (A7184) SHA2-256: (A7184)
ECDSA Signature Generation and Verification	DigSig-SigGen DigSig-SigVer	ECDSA Signature generation / Verification	curve:P-256, P-384, P-521	ECDSA SigGen (FIPS186-5): (A7184) ECDSA SigVer (FIPS186-5): (A7184) SHA2-256: (A7184) SHA2-384: (A7184) SHA2-512: (A7184)
AES Key Generation	CKG	AES key generation	key strength:128, 256 bit	CKG: ()

Name	Type	Description	Properties	Algorithms
HMAC Key Generation	CKG	HMAC key generation	Key length:256, 384, 512bit	CKG: ()
RSA Key Pair Generation	AsymKeyPair-KeyGen CKG	RSA key pair generation	modulo:2048, 3072, 4096	RSA KeyGen (FIPS186-5): (A7184) CKG: ()
ECDSA Key Pair Generation	AsymKeyPair-KeyGen CKG	ECDSA key pair generation	curve:P-256, P-384, P-521	ECDSA KeyGen (FIPS186-5): (A7184) CKG: ()
SHA	SHA	Sha message digest		SHA2-256: (A7184) SHA2-384: (A7184) SHA2-512: (A7184)
Random Number Generation	DRBG	Random number generation	Security strength:256 bit	Conditionin g Component AES-CBC- MAC SP800-90B: (A7184) Counter DRBG: (A7184)
FW update	UNK	Update Security Management Firmware excluding the MCUboot	curve:P-256	ECDSA SigVer (FIPS186-5): (A7184)
User Authentication	UNK	Authenticate users with a challenge response	curve :P-256	ECDSA SigVer (FIPS186-5): (A7184) Counter DRBG: (A7184)
KEK for HUK deriving	KBKDF	Derive a KEK for HUK	key strength:256 bit	KDF SP800-108: (A7184)
User key decryption for key update	BC-UnAuthDecryp t	Decryption of user keys for input to the module	key strength:128 bit	AES-CBC: (A7184) AES-128 CBC-MAC: ()

Name	Type	Description	Properties	Algorithms
KTS User key wrapping	KTS-Wrap	Encryption of user keys for secure storage in the module	IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides 256 bits of security strength	AES-CCM: (A7184)
KTS User key unwrapping	KTS-Unwrap	Decryption of user keys for output from the module	IG D.G:approved method from IG D.G Caveat:Key establishment methodology provides 256 bits of security strength	AES-CCM: (A7184)
KTS Keywrap	KTS-Wrap	Encryption of user keys for secure output from the module.	IG D.G:approved or allowed method from IG D.G Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-KW: (A7184)
KTS Keyunwrap	KTS-Unwrap	Decryption of user keys for secure input to the module.	IG D.G:approved or allowed method from IG D.G Caveat:Key establishment methodology provides between 128	AES-KW: (A7184)

Name	Type	Description	Properties	Algorithms
			and 256 bits of security strength	

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

- AES-GCM encryption is in compliance with IG.C.H Scenario 2. When the AES-GCM encryption service is executed, a 96-bit IV is generated from the approved DRBG inside the cryptographic module. This specification assures that the probability of being called with the same key and the same IV is less than 2^{32} . As previously mentioned, this module generates the IV using a DRBG and sends the IV to the service caller without managing it internally; therefore, it was not considered a PSP.
- RSA Signature Generation/Verification is in compliance with IG C.F. RSA signature generation supports a modules length of 2048 bits, and RSA signature verification supports modules length of 2048, 3072 and 4096 bits.
- The module does not establish SSPs using an approved key transport scheme (KTS). However, it does offer approved authenticated algorithms that can be used by an external operator/application as part of an approved KTS.

2.8 RBG and Entropy

Cert Number	Vendor Name
E288	Renesas Electronics Corporation

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Entropy Source	Physical	R7FA8M1AHECBD	256 bit	256 bit	A7184

Table 9: Entropy Sources

Entropy Information:

The module has an analog noise source and conditions it using AES-256-CBC-MAC for output. Each 128-bit output sample provides a minimum entropy of 128 bits, which means full entropy.

RNG Information:

Use the entropy source output as a seed to generate random numbers with AES-256 CTR-DRBG.

2.9 Key Generation

This module uses a DRBG compliant with SP800-90A Rev.1 to generate AES, RSA and ECDSA keys. The random numbers used for the cryptographic keys are obtained from the DRBG.

It performs cryptographic key generation(CKG) in accordance with SP800-133r2 Section 4, example1. CKG uses the output values of the CTR-DRBG described in NIST SP800-90A as keys.

2.10 Key Establishment

N/A for this module.

2.11 Industry Protocols

N/A for this module.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
UART TXD	Data Output Status Output	Output of Service Execution
UART RXD	Data Input Control Input	Input for Service Execution
P600	Status Output	Set High means that Operator is authenticated.
P414	Status Output	Set High means that zeroization is completed.
P107	Status Output	This port is error indicator, Toggle: CO Self-Test Error, Set High: PO Self-Test Error
Reset	Control Input	Reset
Clock	Control Input	Clock
Power	Power	3.3V power

Table 10: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Challenge response authentication	The challenge-response method is implemented for user authentication. When the user authentication service is executed, the module sends a 128-bit challenge. The ECDSA P-256 signature is sent back in response to	User Authentication	The target strength is 1/1,000,000. The probability that a random attempt will succeed, or a false acceptance will occur depends on the ECDSA P-256 strength.	The target strength is 1/100,000. Since the module generates a 1 ms wait for each authentication attempt. Therefore, the probability that multiple attacks within a given

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	this challenge, and if the signature is correct, the authentication is successful.		Therefore, the probability is $1/2^{128}$, which is less than 1/1,000,000.	minute will be successful is $60,000/2^{128}$, which is less than 1/100,000.

Table 11: Authentication Methods

This module provides identity-based authentication, with the authentication method embedded in challenge response authentication using 128-bit random number. It stores authentication information, including ID, role and authentication public key, linked together. Only one user can be logged in at the same time.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Identity	Crypto Officer	Challenge response authentication
User	Identity	User	Challenge response authentication

Table 12: Roles

This module supports two roles: User and CO(Crypto Officer) role. The maintenance role isn't implemented.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Open	Initialize the module and Enables use of services.	"Crypto Firmw are initialized successfully" via UART	-	-	KEK for HUK deriving	CO - RTL Key: E - KEK for HUK: G,E,Z - HUK: W - DRBG seed: G - DRBG internal state (V, Key): G,W,E User - RTL Key: E - KEK for HUK: G,E,Z - HUK: W - DRBG seed: G - DRBG internal state (V, Key): G,W,E Unauthenticated - RTL Key: E - KEK for HUK: G,E,Z - HUK: W - DRBG seed: G - DRBG internal state (V, Key): G,W,E
Close	Disables use of services.	none	-	-	None	CO User Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
User authentication	Challenge response authentication using ECDSA P-256 Signature verification.	P600 Set High	User ID; signature	-	User Authentication	Unauthenticated - ECDSA-P256-USER-PUBLIC-KEY: E - ECDSA-P256-CO-PUBLIC-KEY: E - DRBG internal state (V, Key): W,E - HUK: E
Add User	Add the new user.	none	User ID; encrypted ECDSA-P256-USER-PUBLIC-KEY	-	User key decryption for key update	CO - ECDSA-P256-USER-PUBLIC-KEY: W - KEY-UPDATE-KEY: E - HUK: E - AES-CBC-MAC-KEY: E
Delete User	Delete specified user data	none	User ID	-	None	CO - ECDSA-P256-CO-PUBLIC-KEY: Z
Display User List	Display User List	none	-	-	None	CO User
Firmware update	Update the Security Management Firmware	none	new firmware; signature	-	FW update	CO - MCUBOOT_IMAGE_SIGNING_LOAD_KEY: E
Show module version	Show module version	none	-	module id / version	None	CO User Unauthenticated
Show module status	Show current module status, logged-in user and error log for self-test.	none	-	module status	None	CO User Unauthenticated
Random number generation	Perform Random number generation	"random number:" via UART	-	Random numbers	Random Number Generation	CO - DRBG internal state (V, Key): W,E User - DRBG internal state (V, Key): W,E
Symmetric	Generate AES or HMAC key	"Wrapped	-	Wrapped	AES Key Generation	CO - DRBG internal state

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
key generation		AES-128 key:", "Wrapped AES-256 key:", "Wrapped HMAC-256 key:", "Wrapped HMAC-384 key:", "Wrapped HMAC-512 key:" via UART		AES-KEY, Wrapped HMAC-KEY	HMAC Key Generation KTS User key wrapping	(V, Key): W,E - AES-KEY: G - HMAC-KEY: G - HUK: E
Asymmetric key generation	Generate RSA or ECDSA key	"Wrapped rsa-2048 private key:", Wrapped rsa-2048 public key:", "Wrapped rsa-3072 private key:", "Wrapped rsa-3072 public key:", "Wrap	-	Wrapped RSA-PRIVATE-KEY, Wrapped RSA-PUBLIC-KEY, Wrapped ECDSA-PRIVATE-KEY, Wrapped ECDSA-PUB	RSA Key Pair Generation ECDSA Key Pair Generation KTS User key wrapping	CO - DRBG internal state (V, Key): W,E - RSA-PRIVATE-KEY: G - RSA-PUBLIC-KEY: G - ECDSA-PRIVATE-KEY: G - ECDSA-PUBLIC-KEY: G - HUK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		ped rsa- 4096 private key:", "Wrap ped rsa- 4096 public key:", "Wrap ped ecdsa- p256 private key:", "Wrap ped ecdsa- p256 public key:", "Wrap ped ecdsa- p384 private key:", "Wrap ped ecdsa- p384 public key:", "Wrap ped ecdsa- p521 private key:", "Wrap ped ecdsa- p521 public key:" via UART		LIC- KEY		

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Key update	Update the keys(AES/HMAC/RSA/ECDSA) stored in Data Flash	None	encrypted AES-KEY, encrypted HMAC-KEY, encrypted RSA-PRIVATE-KEY, encrypted RSA-PUBLIC-KEY, encrypted ECDSA-PRIVATE-KEY, encrypted ECDSA-PUBLIC-KEY	Wrapped AES-KEY, Wrapped HMAC-KEY, Wrapped RSA-PRIVATE-KEY, Wrapped RSA-PUBLIC-KEY, Wrapped ECDSA-PRIVATE-KEY, Wrapped ECDSA-PUBLIC-KEY	User key decryption for key update KTS User key wrapping	CO - AES-KEY: W - HMAC-KEY: W - RSA-PRIVATE-KEY: W - RSA-PUBLIC-KEY: W - ECDSA-PRIVATE-KEY: W - ECDSA-PUBLIC-KEY: W - KEY-UPDATE-KEY: E - HUK: E - AES-CBC-MAC-KEY: E
AES encryption	Performe AES ECB/CBC/CTR/CCM/GCM encryption	"aes enc result:" , "aesccm enc result:" , "aesgcm enc result:" via UART	Wrapped AES-KEY; plain text	ciphertext	AES encryption/decryption Authenticated AES encryption/decryption KTS User key unwrapping	CO - AES-KEY: W,E - HUK: E User - AES-KEY: W,E - HUK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES decryption	Performe AES ECB/CBC/CTR/CCM/GCM decryption	"aes dec result:" , "aesccm dec result:" , "aesgcm dec result:" via UART	Wrapped AES-KEY; cipher text	plain text	AES encryption/decryption Authenticated AES encryption/decryption KTS User key unwrapping	CO - AES-KEY: W,E - HUK: E User - AES-KEY: W,E - HUK: E
AES KeyWrap	Performe AES key wrap	"aesk w wrap result:" via UART	AES-CCM wrapped AES-KEY used for wrapping, AES-CCM wrapped AES-KEY to be wrapped	AES-KW wrapped AES-KEY	KTS User key unwrapping KTS Keywrap	CO - AES-KEY: W,E - HUK: E User - AES-KEY: W,E - HUK: E
AES KeyUnwrap	Performe AES key unwrap	"aesk w unwrap result:" via UART	AES-CCM wrapped AES-KEY used for unwrapping, AES-KW wrapped AES-KEY to be	AES-CCM wrapped AES-KEY	KTS User key wrapping KTS User key unwrapping KTS Keyunwrap	CO - AES-KEY: W,E - HUK: E User - AES-KEY: W,E - HUK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			unwrapped			
AES CMAC Generation	Perform AES CMAC generation	"MAC:" via UART	Wrapped AES-KEY; message	MAC value	AES-CMAC generation/verification KTS User key unwrapping	CO - AES-KEY: W,E - HUK: E User - AES-KEY: W,E - HUK: E
AES CMAC Verification	Perform AES CMAC verification	"MAC:" via UART	Wrapped AES-KEY; message; MAC value	"True" or "False"	AES-CMAC generation/verification KTS User key unwrapping	CO - AES-KEY: W,E - HUK: E User - AES-KEY: W,E - HUK: E
RSA Signature Generation	Perform RSA Signature Generation	"signature:" via UART	Wrapped RSA-PRIVATE-KEY; message	signature	RSA Signature Generation and Verification KTS User key unwrapping	CO - RSA-PRIVATE-KEY: W,E - HUK: E User - RSA-PRIVATE-KEY: W,E - HUK: E
RSA Signature Verification	Perform RSA Signature Verification	"signature:" via UART	Wrapped RSA-PUBLIC-KEY; message; signature	"True" or "False"	RSA Signature Generation and Verification KTS User key unwrapping	CO - RSA-PUBLIC-KEY: W,E - HUK: E User - RSA-PUBLIC-KEY: W,E - HUK: E
ECDSA Signature Generation	Perform ECDSA Signature Generation	"signature:" via UART	Wrapped ECDSA-PRIVATE-KEY; message	signature	ECDSA Signature Generation and Verification KTS User key unwrapping	CO - ECDSA-PRIVATE-KEY: W,E - HUK: E User - ECDSA-PRIVATE-KEY: W,E - HUK: E
ECDSA Signature Verification	Perform ECDSA Signature Verification	"signature:" via UART	Wrapped ECDSA-PUBLIC-KEY	"True" or "False"	ECDSA Signature Generation and Verification	CO - ECDSA-PUBLIC-KEY: W,E - HUK: E User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Verification			C-KEY; message; signature		KTS User key unwrapping	- ECDSA-PUBLIC-KEY: W,E - HUK: E
HMAC Generation	Perform HMAC Generation	"MAC:" via UART	Wrapped HMAC-KEY; message	MAC value	HMAC generation/verification KTS User key unwrapping	CO - HMAC-KEY: W,E - HUK: E User - HMAC-KEY: W,E - HUK: E
HMAC Verification	Perform HMAC Verification	"MAC:" via UART	Wrapped HMAC-KEY; message; MAC value	"True" or "False"	HMAC generation/verification KTS User key unwrapping	CO - HMAC-KEY: W,E - HUK: E User - HMAC-KEY: W,E - HUK: E
SHA Hash Generation	Perform SHA Hash Generation	"message digest:" via UART	message	digest	SHA	CO User
Zeroization	Perform CSP Zeroization	P414 Set High	-	-	None	CO - RTL Key: Z - MCUBOOT_IMAGE_SIGNING_LOAD_KEY: Z
pre operational self test	Perform ondemand pre-operational self test	none	-	-	KEK for HUK deriving	CO - RTL Key: E - KEK for HUK: G,E - HUK: W User - RTL Key: E - KEK for HUK: G,E - HUK: W Unauthenticated - RTL Key: E - KEK for HUK: G,E - HUK: W
On-demand selftest	Perform ondemand conditional self test	"Conditional test completed"	-	-	KEK for HUK deriving	CO - RTL Key: E - KEK for HUK: G,E,Z - HUK: W - DRBG seed: G - DRBG internal state

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		via UART				(V, Key): G,W,E User - RTL Key: E - KEK for HUK: G,E,Z - HUK: W - DRBG seed: G - DRBG internal state (V, Key): G,W,E

Table 13: Approved Services

4.4 Non-Approved Services

N/A for this module.

This module doesn't support non-approved algorithms.

4.5 External Software/Firmware Loaded

The Firmware load function via UART interface is implemented. ECDSA P-256 signature verification is performed during the firmware load test. This load function replaces Security Management Firmware excluding the MCUboot. To maintain certification, the firmware to be loaded must be validated.

5 Software/Firmware Security

5.1 Integrity Techniques

The firmware integrity test is executed after the module's power off/on (this may also mean reset hereafter). It is performed by FSBL and MCUboot according to the following procedures.

- FSBL verifies the MCUboot's integrity using EDC(CRC32). Since FSBL is implemented in mask ROM, it is not applicable to integrity testing.
- MCUboot verifies the integrity of the Security Management Firmware, excluding the MCUboot itself, using ECDSA P-256

5.2 Initiate on Demand

This module can execute an on-demand test by executing the power off/on or selftest command.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

N/A for this module.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-evident coating on chip	Every month	Confirmation that there is no visual damage

Table 14: Mechanisms and Actions Required

The chip is treated with an opaque coating designed to provide tamper evidence.

The module consists of standard, production-quality ICs, designed to meet commercial-grade specifications, and uses standard passivation techniques for the entire chip.



Figure 3 Tamper-evident Coating on Chip

8 Non-Invasive Security

N/A for this module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Code Flash	Flash memory for code store	Static
Data Flash	Flash memory for data store	Static
Extra Flash	Access Restricted Flash Memory	Static
RSIP-E51 Internal register	Internal registers of RSIP	Dynamic
RAM	RAM	Dynamic

Table 15: Storage Areas

The Boot Firmware, which is an excluded component, is stored in Extra Flash.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Key update (input)	UART	Data Flash	Encrypted	Manual	Electronic	User key decryption

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
						for key update
Key update (output)	Data Flash	UART	Encrypted	Automated	Electronic	KTS User key wrapping
Cryptographic service parameter (input)	UART	RAM	Encrypted	Automated	Electronic	KTS User key unwrapping
Add User (input)	UART	Data Flash	Encrypted	Manual	Electronic	User key decryption for key update
Key generation (output)	RSIP-E51 Internal register	UART	Encrypted	Automated	Electronic	KTS User key wrapping
AES KeyWrap(output)	UART	UART	Encrypted	Automated	Electronic	KTS Keywrap
AES KeyUnwrap(input)	UART	UART	Encrypted	Automated	Electronic	KTS Keyunwrap
Initialization Process (input)	UART	Data Flash	Encrypted	Manual	Electronic	User key decryption for key update

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Service	Erase the Code Flash area containing the RSIP driver that includes the 'RTL Key', which serves as the root of SSP protection. Additionally, erase the Data Flash area containing the 'MCUBOOT_IMAGE_SIGNING_LOAD_KEY', which is a public key for the firmware load test.	Overwrite the flash area with 0xFF.	CO
power off/on	The SSP held in the RSIP-E51 internal register is volatilized by cutting power with power off/on. Additionally, when the initialization process is performed, RSIP-E51 internal register is set to "0". Turning the power off and on triggers the initialization process as zeroization.	Clear RSIP-E51 internal register to 0	CO, User

Table 17: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
RTL Key	AES-128 key used for deriving the KEK for HUK	128 - 128	Symmetric Key - CSP	Generated at factory.		KEK for HUK deriving
KEK for HUK	AES-256 key used to encrypt the HUK for storage in the RA8M1	256 - 256	Symmetric Key - CSP	KEK for HUK deriving		AES-CCM (A7184)
HUK	Hardware Unique Key for each device	256 - 256	Symmetric Key - CSP	Generated at factory.		KTS User key wrapping KTS User key unwrapping
DRBG internal state (V, Key)	DRBG internal state	384 - 256	DRBG internal state - CSP	Counter DRBG (A7184)		Random Number Generation
DRBG seed	Seed used for DRBG Instantiation.	384 - 256	DRBG seed - CSP	Counter DRBG (A7184)		Counter DRBG (A7184)
KEY-UPDATE-KEY	Key used to update the user key	128 - 128	Symmetric Key - CSP	Generated outside the module.		User key decryption for key update
AES-KEY	128/256-bit key used for AES encryption/decryption in ECB/CBC/CTR/GCM/CCM modes, generating/verifying AES CMAC, and KeyWrap/KeyUnwrap	128, 256 - 128, 256	Symmetric Key - CSP	AES Key Generation		AES encryption/decryption Authenticated AES encryption/decryption AES-CMAC generation/verification KTS Keywrap

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						KTS Keyunwrap
RSA-PRIVATE-KEY	RSA private key used for signature generation	2048, 3072, 4096 - 112, 128, 150	Private Key - CSP	RSA Key Pair Generation		RSA Signature Generation and Verification
RSA-PUBLIC-KEY	RSA public key used for signature verification	2048, 3072, 4096 - 112, 128, 150	Public Key - PSP	RSA Key Pair Generation		RSA Signature Generation and Verification
ECDSA-PRIVATE-KEY	ECDSA private key used for signature generation	256, 384, 521 - 128, 192, 256	Private Key - CSP	ECDSA Key Pair Generation		ECDSA Signature Generation and Verification
ECDSA-PUBLIC-KEY	ECDSA public key used for signature verification	256, 384, 521 - 128, 192, 256	Public Key - PSP	ECDSA Key Pair Generation		ECDSA Signature Generation and Verification
ECDSA-P256-CO-PUBLIC-KEY	ECDSA public key for Crypto Officer used for user authentication	256 - 128	Public Key - PSP	Generated outside the module.		User Authentication
ECDSA-P256-USER-PUBLIC-KEY	ECDSA public key for User used for user authentication	256 - 128	Public Key - PSP	Generated outside the module.		User Authentication

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
HMAC-KEY	HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Keys used for generation/verification	256, 384, 512 - 256+	Symmetric Key - CSP	HMAC Key Generation		HMAC generation/verification
MCUBOOT_IMAGE_SIGNING_LOAD_KEY	ECDSA public key for the firmware load test	256 - 128	Public Key - PSP	Other		FW update
AES-CBC-MAC-KEY	Key used for interoperability with inputting User key	128 -	Symmetric Key - Neither	Other		AES-128 CBC-MAC

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
RTL Key		Code Flash:Obfuscated		Zeroization Service	
KEK for HUK		RSIP-E51 Internal register:Plaintext	Until power off/on	power off/on	RTL Key:Derived From HUK:Decrypts
HUK		Extra Flash:Encrypted		N/A	AES-KEY:Encrypts RSA-PRIVATE-KEY:Encrypts RSA-PUBLIC-KEY:Encrypts ECDSA-PRIVATE-KEY:Encrypts ECDSA-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					PUBLIC-KEY:Encry pts ECDSA- P256-CO- PUBLIC- KEY:Encry pts ECDSA- P256- USER- PUBLIC- KEY:Encry pts HMAC- KEY:Encry pts KEY- UPDATE- KEY:Decr ypts AES- KEY:Decr ypts RSA- PRIVATE- KEY:Decr ypts RSA- PUBLIC- KEY:Decr ypts ECDSA- PRIVATE- KEY:Decr ypts ECDSA- PUBLIC- KEY:Decr ypts ECDSA- P256-CO- PUBLIC- KEY:Decr ypts ECDSA- P256-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					USER-PUBLIC-KEY:Decrypts HMAC-KEY:Decrypts
DRBG internal state (V, Key)		RSIP-E51 Internal register:Plaintext	Until power off/on	power off/on	
DRBG seed		RSIP-E51 Internal register:Plaintext	Until power off/on	power off/on	
KEY-UPDATE-KEY	Initialization Process (input)	Data Flash:Encrypted		N/A	AES-KEY:Decrypts RSA-PRIVATE-KEY:Decrypts RSA-PUBLIC-KEY:Decrypts ECDSA-PRIVATE-KEY:Decrypts ECDSA-PUBLIC-KEY:Decrypts ECDSA-P256-CO-PUBLIC-KEY:Decrypts ECDSA-P256-USER-PUBLIC-KEY:Decrypts HMAC-

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					KEY:Decrypts HUK:Encrypted by
AES-KEY	Key update (input) Key update (output) Cryptographic service parameter (input) Key generation (output) AES KeyWrap(output) AES KeyUnwrap(input)	Data Flash:Encrypted		N/A	HUK:Encrypted by AES-KEY:Encrypted by AES-KEY:Encrypts AES-KEY:Decrypts
RSA-PRIVATE-KEY	Key update (input) Key update (output) Cryptographic service parameter (input) Key generation (output)	Data Flash:Encrypted		N/A	HUK:Encrypted by
RSA-PUBLIC-KEY	Key update (input) Key update (output)	Data Flash:Encrypted		N/A	HUK:Encrypted by
ECDSA-PRIVATE-KEY	Key update (input) Key update (output) Cryptographic service parameter (input) Key	Data Flash:Encrypted		N/A	HUK:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	generation (output)				
ECDSA-PUBLIC-KEY	Key update (input) Key update (output) Cryptographic service parameter (input) Key generation (output)	Data Flash:Encrypted		N/A	HUK:Encrypted by
ECDSA-P256-CO-PUBLIC-KEY	Initialization Process (input)	Data Flash:Encrypted		N/A	HUK:Encrypted by
ECDSA-P256-USER-PUBLIC-KEY	Add User (input)	Data Flash:Encrypted		N/A	HUK:Encrypted by
HMAC-KEY	Key update (input) Key update (output)	Data Flash:Encrypted		N/A	HUK:Encrypted by
MCUBOOT_IMAGE_SIGNING_LOAD_KEY	Initialization Process (input)	Data Flash:Plaintext		Zeroization Service	
AES-CBC-MAC-KEY	Initialization Process (input)	Data Flash:Encrypted		N/A	HUK:Encrypted by

Table 19: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
CRC-32	32 bit	Error Detection Code	SW/FW Integrity	Input via UART can be accepted	Firmware integrity test for MCUboot is performed by using CRC32 at every power-on-reset.
ECDSA P256	ECDSA P256, SHA2-256	ECDSA P256	SW/FW Integrity	Input via UART can	Firmware integrity test for Security Management Firmware, excluding the

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
		signature verification		be accepted	MCUboot itself, is performed by using ECDSA P256 signature verification at every power-on-reset.

Table 20: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KDF SP800-108 (A7184)	Key length: 256 bit	KAT	CAST	"Conditional test completed." via UART	KDF	Execution of Open or Execution of On-demand selftest
AES CCM enc (A7184)	Key length: 128 bit	KAT	CAST	"Conditional test completed." via UART	Encrypt	Execution of Open or Execution of On-demand selftest
AES CCM dec (A7184)	Key length: 128 bit	KAT	CAST	"Conditional test completed." via UART	Decrypt	Execution of Open or Execution of On-demand selftest
Counter DRBG (A7184)	-	KAT	CAST	"Conditional test completed." via UART	instantiate function, generate function	Execution of Open or Execution of On-demand selftest
Entropy Source Health Test	-	fault detection test	CAST	"Conditional test completed." via UART	health test	Execution of Open or Execution of On-demand selftest
AES-GCM (A7184)	Key length: 128 bit	KAT	CAST	"Conditional test completed." via UART	Encrypt	Execution of Open or Execution of On-demand selftest
AES-ECB (A7184)	Key length: 128 bit	KAT	CAST	"Conditional test completed." via UART	Decrypt	Execution of Open or Execution of On-demand selftest

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-5) (A7184)	Signature Type: RSASSA-PKCS1-V1_5, Modulo: 2048, Hash: SHA2-256	KAT	CAST	"Conditional test completed." via UART	Sign	Execution of Open or Execution of On-demand selftest
RSA SigVer (FIPS186-5) (A7184)	Signature Type: RSASSA-PKCS1-V1_5, Modulo: 2048, Hash: SHA2-256	KAT	CAST	"Conditional test completed." via UART	Verify	Execution of Open or Execution of On-demand selftest
SHA2-256 (A7184)	-	KAT	CAST	"Conditional test completed." via UART	Hash	Execution of Open or Execution of On-demand selftest
SHA2-512 (A7184)	-	KAT	CAST	"Conditional test completed." via UART	Hash	Execution of Open or Execution of On-demand selftest
HMAC-SHA2-256 (A7184)	Key length: 256 bit	KAT	CAST	"Conditional test completed." via UART	HMAC Gen, HMAC Verify	Execution of Open or Execution of On-demand selftest
ECDSA SigGen (FIPS186-5) (A7184)	Curve: P-256, Hash: SHA2-256	KAT	CAST	"Conditional test completed." via UART	Sign	Execution of Open or Execution of On-demand selftest
ECDSA SigVer (FIPS186-5) (A7184)	Curve: P-256, Hash: SHA2-256	KAT	CAST	"Conditional test completed." via UART	Verify	Before Pre-Operational Self-Tests, and Execution of Open or Execution of On-demand selftest
RSA KeyGen	Key length: 2048, 3072, 4096 bit	PCT	PCT	Output tested key	Key Pair Gen	Execution of RSA key pair

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
(FIPS186-5) (A7184)				pair via UART.		generation services
ECDSA KeyGen (FIPS186-5) (A7184)	Key length: 256, 384, 521 bit	PCT	PCT	Output tested key pair via UART.	Key Pair Gen	Execution of ECDSA key pair generation services
FW Load Test	ECDSA p256 signature	Signature Verify	SW/FW Load	"fwupdate success" via UART	FW Load Test	Execution of fwupdate command

Table 21: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
CRC-32	Error Detection Code	SW/FW Integrity	On Demand	Manually
ECDSA P256	ECDSA P256 signature verification	SW/FW Integrity	On Demand	Manually

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF SP800-108 (A7184)	KAT	CAST	On Demand	Manually
AES CCM enc (A7184)	KAT	CAST	On Demand	Manually
AES CCM dec (A7184)	KAT	CAST	On Demand	Manually
Counter DRBG (A7184)	KAT	CAST	On Demand	Manually
Entropy Source Health Test	fault detection test	CAST	On Demand	Manually
AES-GCM (A7184)	KAT	CAST	On Demand	Manually
AES-ECB (A7184)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-5) (A7184)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-5) (A7184)	KAT	CAST	On Demand	Manually
SHA2-256 (A7184)	KAT	CAST	On Demand	Manually
SHA2-512 (A7184)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A7184)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigGen (FIPS186-5) (A7184)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A7184)	KAT	CAST	On Demand	Manually
RSA KeyGen (FIPS186-5) (A7184)	PCT	PCT	-	-
ECDSA KeyGen (FIPS186-5) (A7184)	PCT	PCT	-	-
FW Load Test	Signature Verify	SW/FW Load	-	-

Table 23: Conditional Periodic Information

The on-demand pre-operational test can be executed by power off/on.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
PO Self-Test Error State	Error state caused by failure of self-test executed by FSBL or MCUboot	In the case where the self-test executed by FSBL or MCUboot encounters an error.	power off/on	P107 Set High
CO Self-Test Error State	Error state caused by failure of self-test executed by User Application	In the case where the self-test executed by User Application encounters an error.	power off/on	P107 toggles between low and high at 0.5 second intervals

Table 24: Error States

This module transitions to an error state if it fails the self-test.

PO Self-Test is performed by FSBL that performs CRC-32 Test, and by MCUboot that performs ECDSA P256 Test, FW Load Test, and ECDSA SigVer(FIPS186-5) Test. Other self-tests are executed by User Application.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Renesas Electronics provides the evaluation board for the module, the EK-RA8M1, and the firmware executable file to customers.

- EK-RA8M1
<https://www.renesas.com/en/products/microcontrollers-microprocessors/ra-cortex-m-mcus/ek-RA8M1-evaluation-kit-RA8M1-mcu-group>

- Security Management Firmware (ra8m1_security_management_module.zip)

After obtaining the above, please initialize the module following the steps below by CO. The details of the procedure are described in the user setup manual

“RA8M1_SMM_Setting_Manual_rev.1.0.docx”.

Note that this operation is proceeded with using a NON-networked GPC. Connect the GPC to the module via a serial port of the EK-RA8M1.

- 1 Set Up the EK-RA8M1
 - 1.1 Connect the PC and EK-RA8M1
 - 1.2 Check the Boot Firmware version
- 2 Write the user keys
- 3 Write the executable firmware
- 4 Authenticate using the default CO public key
- 5 Update the default CO public key
- 6 Change the Device Lifecycle

The Boot Firmware included in the module is written to the Extra Flash area of the RA8M1 at the time of product shipment.

The Boot Firmware version can be checked using RFP (Renesas Flash Programmer). By executing a command with the "-sig" option in RFP.

<pre>rfp-cli -d RA -t jlink -sig</pre>
--

The other component version can be outputted by "Show module version" service.

11.2 Administrator Guidance

Refer to the RA8M1_SMM_Usage_Guidance_rev.1.0.docx

Note that using the "Add User" service or using the "key update" services must be proceeded with using a NON-networked GPC connect to the module via a serial port of the EK-RA8M1.

11.3 Non-Administrator Guidance

Refer to the RA8M1_SMM_Usage_Guidance_rev.1.0.docx

11.4 Design and Rules

N/A for this module.

11.5 Maintenance Requirements

N/A for this module.

11.6 End of Life

The following procedures are used to ensure secure sanitization and destruction of cryptographic module.

1. Secure sanitization
Execute the "zeroization" command in the CO role to zeroize the unprotected SSPs and then reset the module.
2. Secure destruction
Destroy the RA8M1 (R7FA8M1AHECBD) to fragments smaller than 2 mm².

12 Mitigation of Other Attacks

N/A for this module.