RA4M1 MCU Group

Security Manual

Introduction

The RA4M1 MCU Group incorporates many features that can be used to protect the content and operation of the MCU when it is integrated into an end product. This document describes these features and provides general recommendations for their use. Associated application notes and other applicable documents that provide more details are listed for reference.

Since the RA4M1 is a general-purpose MCU, this Security Manual cannot provide specific guidance for all possible use cases, nor can it offer system-level security recommendations. It is highly recommended that the application developer conduct a security analysis of the system into which the RA4M1 is integrated and create a threat model and security policy for the system and for the RA4M1, for example, using the ISO/SAE 21434 Threat Analysis and Risk Assessment (TARA) approach. It is the application developer's responsibility to decide what RA4M1 security features are necessary for the end product and to implement them appropriately.

Although this Security Manual describes the best secure practices for configuring the RA4M1 at the time of its release, the microcontroller threat landscape is constantly changing and evolving. Please refer to the notice at the end of this document.

Contents

1. Introduction

1.1 Overview

This application note describes the security-related features of the RA4M1 MCU Group and guides how to utilize these features to create a product with the appropriate level of cybersecurity, tailored to the threat model for the intended application.

NOTE: Ultimately, it is up to the discretion of the application developer to determine how to design the security architecture of the end product and what security features to employ. Critical items related to the proper functioning of the MCU and potential security threats are highlighted in red sections.

1.2 Security Features

The RA4M1 MCU provides the following security-related features:

- MCU product and chip-unique identification
- Hardware-enforced isolation
- The SCE5 integrated security engine, providing cryptographic functions and secure key handling
- Immutable memory
- Various tamper detection features
- Debugger and programmer interface protection

The RA Flexible Software Package (FSP) is the Renesas software platform available for use with the RA4M1 MCU Group. The FSP provides support for security solutions that are often required to secure an end-product, including:

- Creation of a cryptographic identity
- Secure boot
- Secure firmware updates
- Secure internet connectivity

1.3 References

The following documents are referenced in this application note. These documents are available from the Renesas website www.renesas.com.

Reference	Document Name	Document Number or URL
[RA4M1 User Manual]	RA4M1 Group User's Manual: Hardware	R01UH0887
[SCE_TADI TU]	Technical Update, Update of Secure Cryptographic Engine Event	TN-RA*-A0153A/E
[FSP User Manual]	RA Flexible Software Package Documentation	RA Flexible Software Package Documentation: Introduction (renesas.github.io)
[Boot Firmware]	Renesas RA Family System Specifications for Standard Boot Firmware	R01AN5372
[SP800-22 Test Report]	NIST SP800-22r1a Random Number Statistical Test Report for RA4M1	R01AN6233EU0100
[SP800-90B Test Report]	NIST SP800-90B Entropy Assessment Report for RA4M1	R01AN6863EU0100

1.4 Additional Guidance Documentation

The following additional guidance documents are referenced in this application note. Please note that due to documentation update cycles, the RA4M1 MCU Group may not be explicitly referenced in the latest version of these documents. These documents are available from the Renesas website, www.renesas.com.

Reference	Document Name	Document Number
[Bootloader Basic]	RA4 Basic Secure Bootloader Using MCUboot and Internal Code Flash	R11AN0869
[Cloud OTA]	RA AWS Cloud Connectivity and Firmware Update OTA on CK-RA6M5 v2 with Ethernet	R11AN0915
[Bootloader Encrypted]	Booting Encrypted Image on RA4 using MCUboot and QSPI	R11AN0868
[Plaintext Key Injection]	Injecting Plaintext User Keys	R11AN0473
[SCE Modes]	Renesas Security Engine Operational Modes	R11AN0498
[Secure Data at Rest]	Security Data at Rest Utilizing the Renesas Security MPU	R11AN0416
[Secure Key Injection]	Injection and Updating Secure User Keys for RA Family	R11AN0496

1.5 Development Tools

Renesas provides the following tools to support the development of security solutions.

Reference	Name	URL
[FSP]	Flexible Software Package (FSP) for Renesas RA MCU Family with e^2 studio IDE	www.renesas.com/fsp
[RASC]	RA Smart Configurator	www.renesas.com/fsp
[SKMT]	Security Key Management Tool	https://www.renesas.com/software-tool/security-key-management-tool

1.6 Abbreviations and Legend

The following abbreviations are used in this document.

Abbreviation	Meaning
BSP	Board Support Package
CAC	Clock Frequency Accuracy Measurement Circuit
DHUK	Derived Hardware Unique Key
ECC	Elliptic Curve Cryptography
ECDH/ECDHE	Elliptic Curve Diffie Hellman (Ephemeral)
EDMAC	Ethernet DMA Controller
EPTPC	Ethernet PTP Controller
ETHERC	Ethernet MAC Controller
FSP	Flexible Software Package
HRK	Hardware Root Key
IDE	Interactive Development Environment
ISR	Interrupt Service Routine
JOP	Jump Oriented Programming
KAS	Key Agreement Scheme
LVD	Low Voltage Detection

MAC	Message Authentication Code or Media Access Control
MPU	Memory Protection Unit
RASC	RA Smart Configurator
RMA_KEY	Return Material Authorisation Key
RFP	Renesas Flash Programmer
ROP	Return-Oriented Programming
RTC	Realtime Clock
SCE	Secure Crypto Engine
SKMT	Security Key Management Tool
TRNG	True Random Number Generator
TSN	Temperature Sensor
UFPK	User Factory Programming Key
W-UFPK	Wrapped User Factory Programming Key

The following figure illustrates the concepts presented in this document.

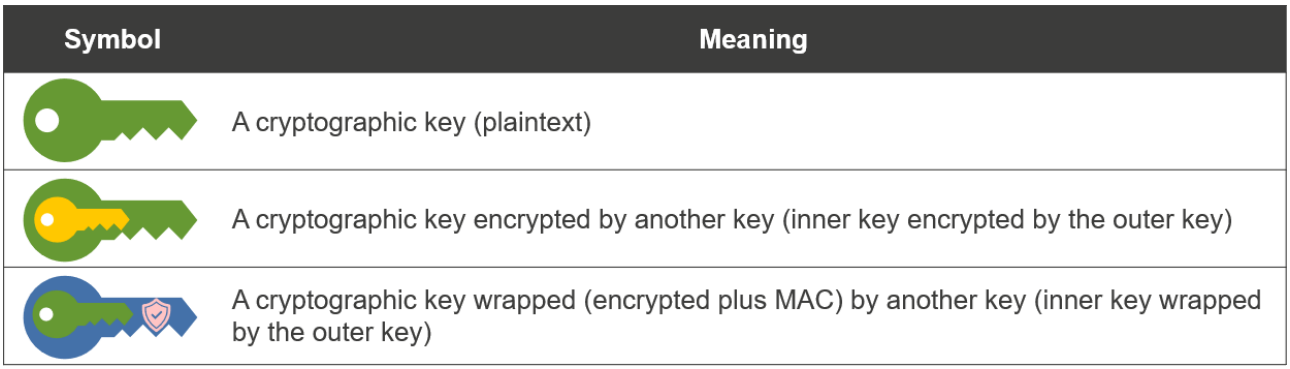

Figure 1. Graphical Representations of Cryptographic Keys

1.7 Software Platform

The RA Flexible Software Package (FSP) is a software package provided by Renesas for developing applications on RA Family MCUs. The FSP offers Board Support Packages, HAL drivers, and middleware for RA Family MCUs.

The FSP Platform Installer includes the e^2 studio IDE, toolchain, and FSP packs. Alternatively, the FSP Standalone Installer, along with the RA Smart Configurator, can be used with the IAR Embedded Workbench IDE or Arm Keil MDK.

These installers, plus additional information, can be found at www.renesas.com/fsp.

1.8 Vulnerability Reporting

Renesas is committed to proactively addressing any potential security vulnerabilities within our products. To report a security vulnerability, please visit www.renesas.com/psirt and follow the instructions on the webpage.

2. Identity

2.1 MCU Group Identity

The RA4M1 MCU Group chips contain a 16-byte read-only register that includes an immutable ASCII representation of the device part number. The PNRn Part Numbering Registers are documented in the [RA4M1 User Manual], including a part number listing.

This value can be obtained by using the FSP function `R_BSP_PartNumberGet()`.

For more details, refer to the following document:

- [RA4M1 User Manual]

2.2 Unique Identity

The RA4M1 MCU Group chips contain a 16-byte read-only register that includes an immutable 16-byte ID code (unique ID) for identifying the individual MCU. The UIDRn Unique ID Registers are documented in the [RA4M1 User Manual].

This value is guaranteed to be unique. It is serialised and therefore predictable, so it should not be used for identifying the end-product if a random or pseudorandom identifier is required.

This value can be obtained by using the FSP function `R_BSP_UniqueIdGet()`.

For more details, refer to the following document:

- [RA4M1 User Manual]

2.3 Cryptographic Identity

The RA4M1 MCU is not delivered with a provisioned cryptographic identity. Any cryptographic identity required by the application must be provisioned during production programming.

Since the SCE5 does not support asymmetric cryptography, cryptographic identities implemented as asymmetric key pairs must be supported by software-based cryptography.

For more details, refer to the following documents and sections of this document:

- [RA4M1 User Manual]
- [FSP User Manual]
- Section 5 SCE5 Cryptographic Functions
- Section 6 SCE5 Random Number Generation

3. Isolation

3.1 Security MPU

The RA4M1 includes a Security MPU, designed to provide hardware-enforced isolation to create secure and non-secure regions. This separation applies to:

- On-chip flash memory (i.e., code flash)
- SRAM
- Select MCU peripherals

For best security design practices, external memory should always be considered Non-secure.

The address range boundaries for the Security MPU are programmed in non-volatile flash and applied before the reset vector is fetched. This ensures that malicious code cannot override the boundaries.

No notification is provided for Security MPU violations. Illegal access attempts will simply fail.

The Security MPU does not restrict access points into the secure region. As a result, the Security MPU does not provide protection against Return Oriented Programming (ROP) attacks or Jump Oriented Programming (JOP) attacks.

Isolation using the Security MPU is not mandatory. It is the responsibility of the application developer to assess the security risks of a monolithic architecture, whether to utilize an isolation mechanism, and what services and peripherals to place in the Secure region.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [Secure Data at Rest]

3.2 Other Memory Protection Units (MPUs)

The RA4M1 MCU Group contains an Arm Cortex-M4 core with an Arm MPU and a Bus Master MPU.

The Arm MPU can be used to protect memory regions by defining access permissions for different privilege states. See the Arm Developer documentation for more information about how to use the Arm MPU: Armv8-M Memory Model and Memory Protection User Guide

The Bus Master MPU provides memory protection for bus masters other than the CPU, namely the DMA bus, the ETHER bus, and the GPX bus. If access to a protected region is detected, the Bus Master MPU generates an internal reset or a non-maskable interrupt.

The Bus Slave MPU monitors access to the bus slave functions. Refer to [RA4M1 User Manual] for the list of protected slave functions. If access to a protected region is detected, the Bus Slave MPU generates an internal reset or a non-maskable interrupt.

For more details, refer to the following documents:

- [RA4M1 User Manual]

3.3 SCE5

The SCE5 security engine is a cryptographic subsystem that is integrated into the MCU silicon, managed and protected by dedicated control logic. The cryptographic operations are physically isolated from the rest of the chip, with dedicated RAM for holding sensitive material (i.e., plaintext keys) during cryptographic operations. The SCE5 can be further protected by MPU isolation.

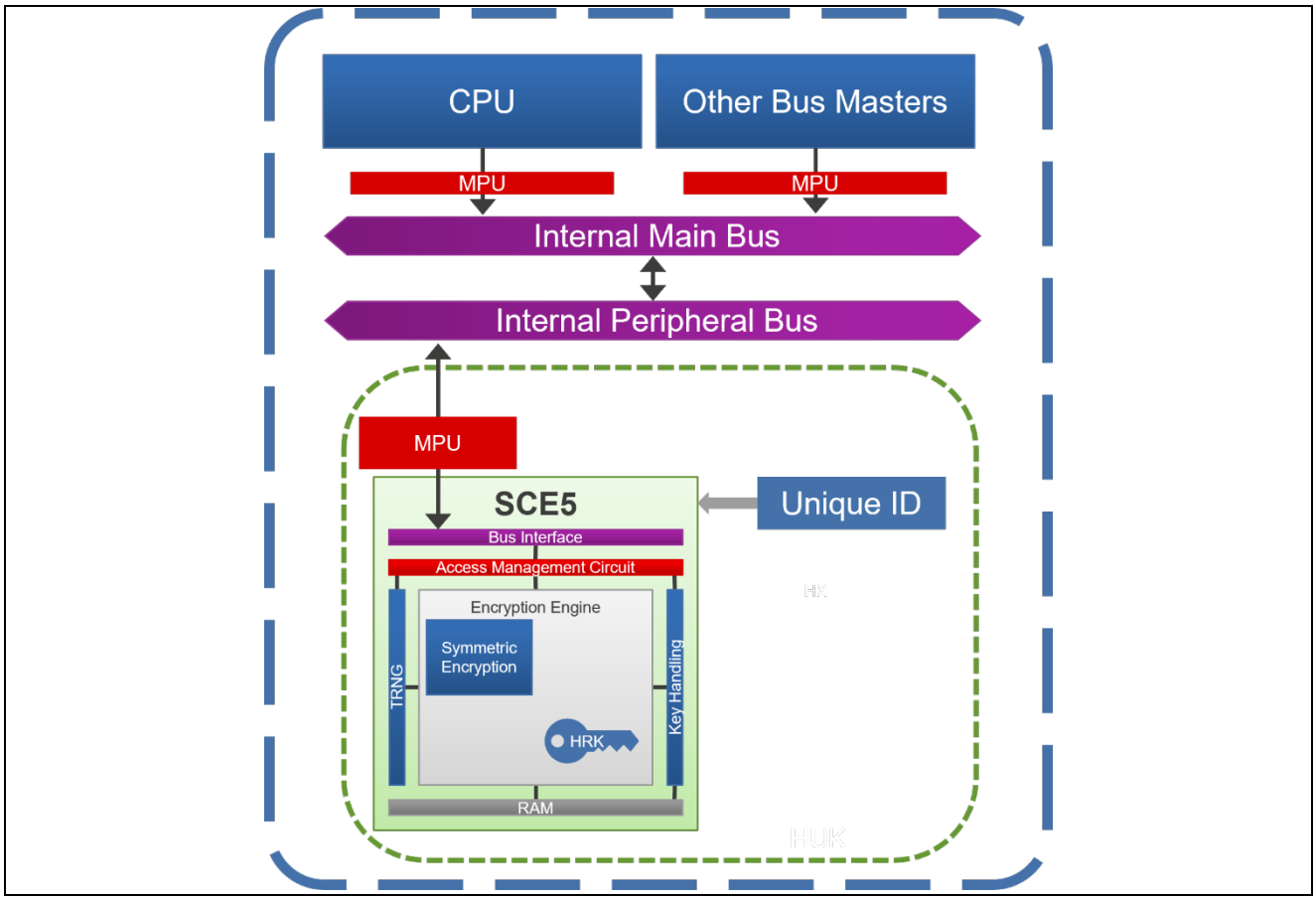

Figure 2. SCE5 On-chip Isolation

For more details, refer to the following documents and sections of this document:

- [RA4M1 User Manual]
- [SCE Modes]
- Section 4 SCE5 Secure Key Injection, Storage, and Usage
- Section 5 SCE5 Cryptographic Functions
- Section 8.2 SCE5 Protection Features

4. SCE5 Secure Key Injection, Storage, and Usage

4.1 SCE5 Operational Modes

The SCE5 functions only in Compatibility Mode.

For more details, refer to the following documents and sections of this document:

- [SCE Modes]
- [FSP User Manual]
- Section 8.2 SCE5 Protection Features

4.1.1 SCE5 Compatibility Mode Operation

Compatibility Mode is designed to facilitate integration with legacy systems and software while still supporting secure key injection, storage, and usage. In Compatibility Mode, plaintext private keys can be used for cryptographic functions, simplifying integration with third-party stacks and libraries.

Compatibility Mode is utilized through the PSA Certified Crypto APIs, ensuring alignment with the Arm ecosystem.

Refer to section 8.2 SCE5 Protection Features for more information about the protection features included in Compatibility Mode operation.

Since plaintext key material can be present and used in the application, it is essential that the developer evaluates and accepts any associated risks.

For security best practices, private keys that are stored in non-volatile memory should be stored securely, as explained in section 4.3 Secure and Plaintext Key Injection and Update. Depending on the threat model, it may be acceptable to store session keys in plaintext in RAM.

Plaintext private keys should be protected via other key protection mechanisms, such as isolation in the Secure region.

4.2 Secure Key Storage

The secure key storage mechanism utilizes the chip's Derived Hardware Unique Key, a 128-bit key that is unique to each chip and can be derived only by the SCE5 security engine. Application keys that have been wrapped with this key via a key injection or key update process can be stored securely at any location in any memory. This mechanism provides unlimited secure key storage and cloning protection.

For additional protection, it is recommended to store wrapped keys in the Secure region if the application utilizes the Security MPU.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]
- [Secure Key Injection]
- [Plaintext Key Injection]

4.3 Secure and Plaintext Key Injection and Update

The secure key injection process leverages the MCU's hardware root key, a key that is contained within the SCE5 security engine and is common across all chips. This key is used only for the secure key injection process. It is not used for secure storage of application keys, and it is not accessible outside the security engine.

To protect both the Renesas MCU Hardware Root Key and the developer's application keys, no sensitive key material is transferred between Renesas and the application developer. Instead, as shown in Figure 3. Secure Key Injection, the developer creates an intermediary key called a User Factory Programming Key (UFPK). This key is PGP-encrypted and sent to the Renesas Key Wrap Service, an automated secure server that wraps the UFPK (creating a W-UFPK), PGP-encrypts it, and returns it to the developer.

A non-trivial key that is not duplicated from Renesas examples or other publicly available cryptography references must be used for the UFPK.

Application keys are injected by providing both the W-UFPK and the UFPK-encrypted application key(s) to the SCE5. The security engine unwraps the W-UFPK to obtain the UFPK, then decrypts the encrypted application key. It then wraps the application key with the MCU's HUK. Figure 3. Secure Key Injection shows an overview of this process.

Key preparation steps where keys are exposed in plaintext must be performed in a secure environment.

It is recommended to use different UFPKs for prototype development with test keys and for production programming of mass production keys.

The RA4M1 cannot be personalized to accept only specific W-UPFKs for application key injection; therefore, the production programming flow must protect against malicious key injection. To guard against supply chain attacks, it is recommended to issue the “Initialize” boot firmware command to erase the chip before key injection.

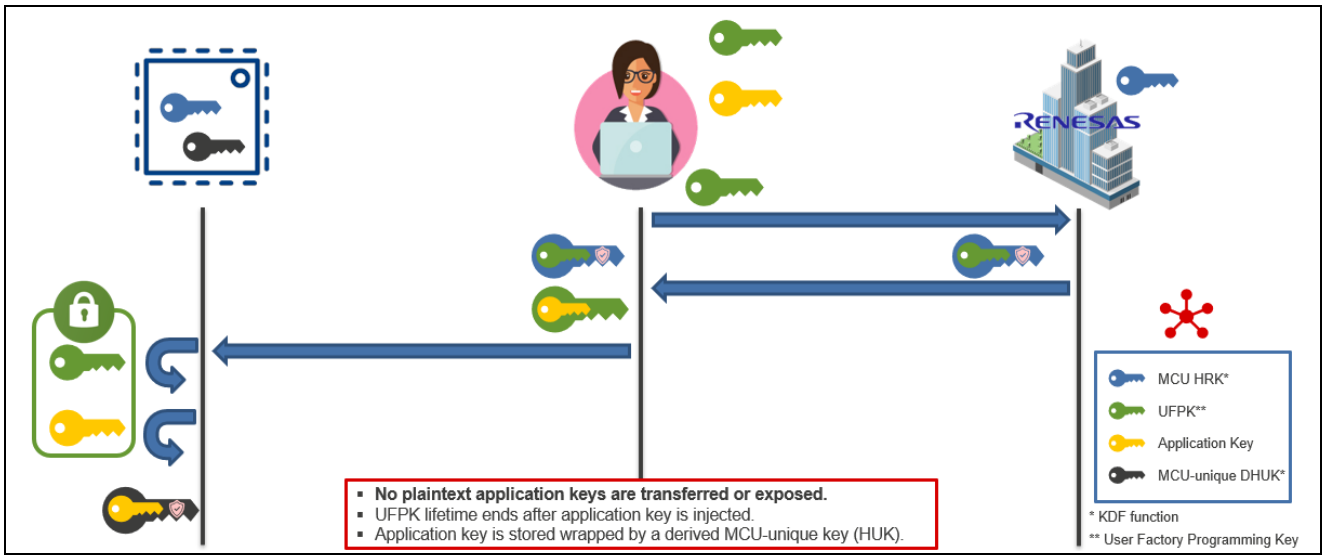

Figure 3. Secure Key Injection

On the RA4M1, in Compatibility Mode, both secure and plaintext key injection are performed using APIs contained in the FSP.

Renesas provides the following tools to support this process:

- Security Key Management Tool (SKMT) - This tool can create sample keys and prepare keys for secure key injection and secure key update.

The following sections provide more details about the secure and plaintext key injection and update processes.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]
- [SCE Modes]
- [Secure Key Injection]
- [Plaintext Key Injection]
- [SKMT]

4.3.1 SCE5 Compatibility Mode Key Injection

Keys used with Compatibility Mode must use the FSP Key Injection module and be either securely injected or injected as plaintext. The wrapped keys can then be used with the PSA Certified Crypto APIs.

Secure key injection is performed using the FSP Key Injection module. As shown in Figure 4. Compatibility Mode Secure Key Injection, the W-UFPK and encrypted application key are both provided to the API. The SCE driver uses the security engine to decrypt the application key and wrap it with the MCU's HUK. The application code must then store the key at a designated location in memory.

It is recommended not to include either secure key injection API code or any W-UFPKs in end-product firmware. This can be done by utilizing a programming tool that executes the secure key injection code from the MCU RAM or by erasing the flash memory that contains the secure key injection code.

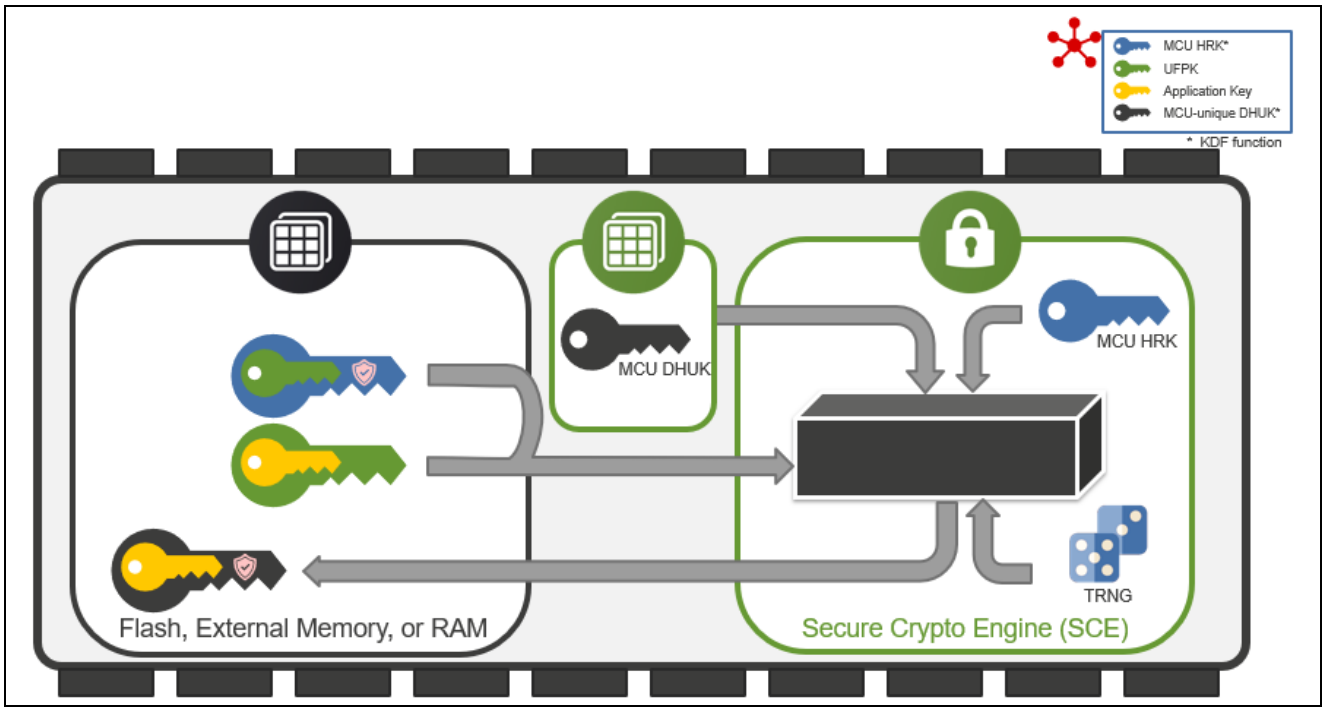

Figure 4. Compatibility Mode Secure Key Injection

Plaintext key injection is also performed using the FSP Key Injection module. As shown in Figure 5. Compatibility Mode Plaintext Key Injection, the plaintext application key is provided to the API. The SCE driver utilizes the security engine to encrypt the plaintext key using the MCU's HUK. The application code must then store the wrapped key at a designated location in memory.

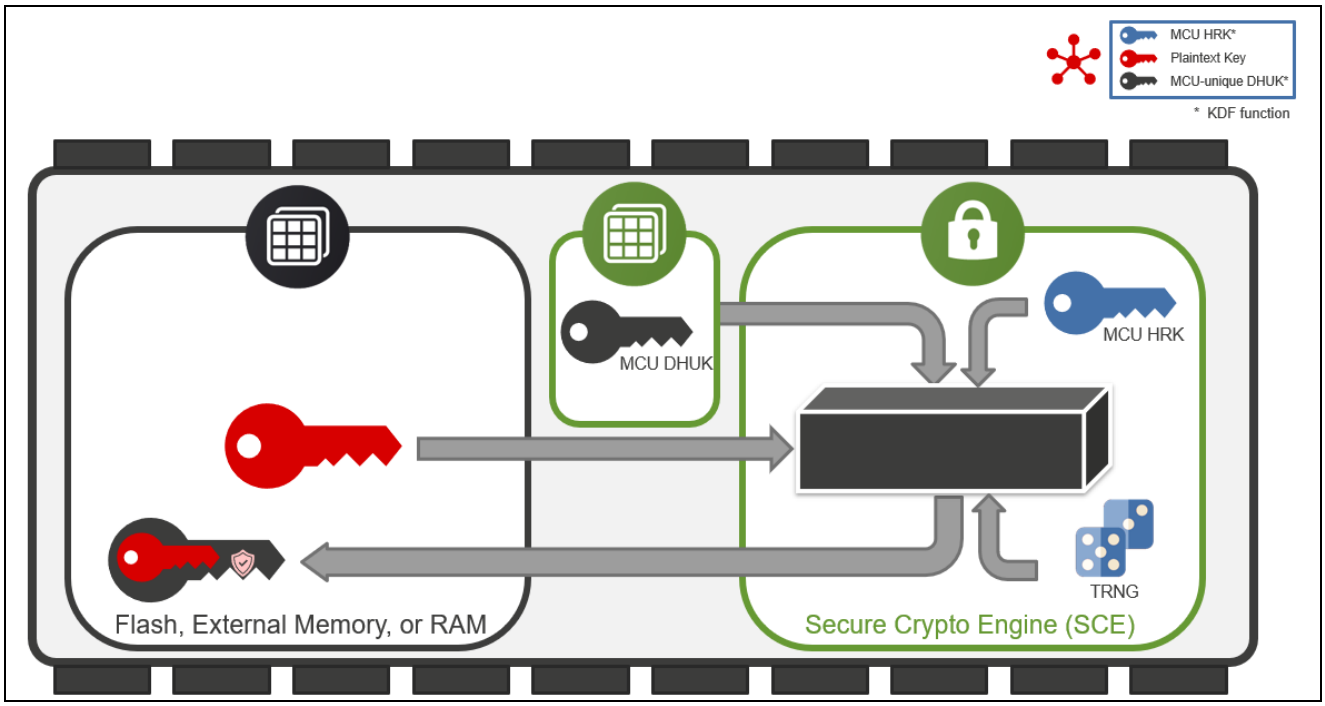

Figure 5. Compatibility Mode Plaintext Key Injection

There is no explicit support in Compatibility Mode for Key Update. It is recommended to securely inject one or more keys that will serve as Key-Update Keys and manually perform the decryption and plaintext key injection of the new key. See Figure 6. Compatibility Mode Key Update for an overview of this process.

Since plaintext key exposure occurs outside the security engine, it is recommended to perform the entire key update operation in the Secure region.

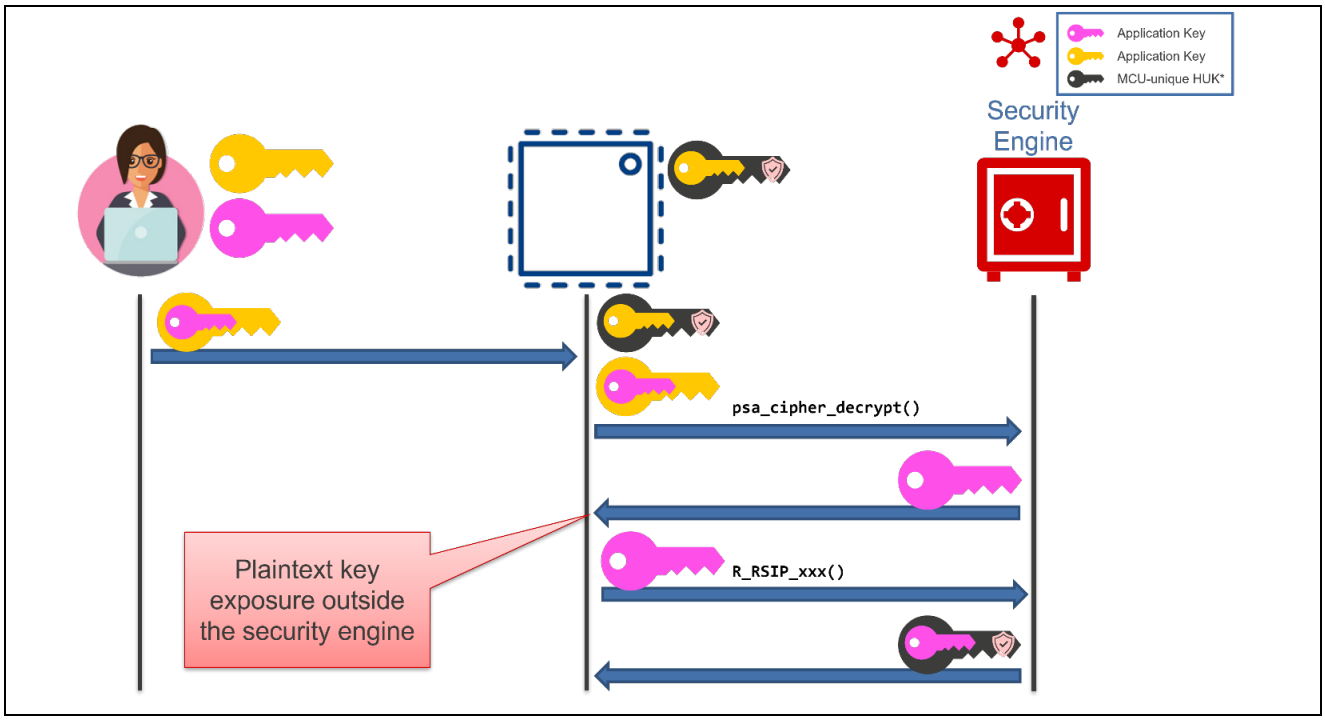

Figure 6. Compatibility Mode Key Update

5. SCE5 Cryptographic Functions and Key Generation

The SCE5 security engine provides hardware acceleration for basic cryptographic functions. The FSP Crypto APIs (Protected Mode) and PSA Certified Crypto APIs (Compatibility Mode) provide any needed software support.

Table 1 SCE5 Cryptographic Operations lists the cryptographic algorithms supported by the security engine. Table 2 SCE5 Key Generation lists the cryptographic key generation supported by the security engine.

The application code should utilize cryptographic algorithms with sufficient strength, as appropriate to the application's threat model.

Table 1 SCE5 Cryptographic Operations

Algorithm	Operations	Specification	Key lengths	Modes
AES	Encryption, decryption, and MAC	NIST FIPS PUB 197 NIST SP800-38A (ECB, CBC, CTR) NIST SP800-38B (CMAC) NIST SP800-38C (CCM) NIST SP800-38D (GCM, GMAC)	128 and 256 bits	ECB, CBC, CTR, CCM, GCM, CMAC, GMAC

Table 2 SCE5 Key Generation

Algorithm	Specification	Key lengths
AES	NIST FIPS PUB 197	128 and 256 bits

For more details, refer to the following document:

- [RA4M1 User Manual]

6. SCE5 Random Number Generation

The RA4M1 MCU Group implements random number generation by utilizing the True Random Number generation capability of the SCE5 security engine. The TRNG implementation consists of an SP800-90A compliant DRBG that is fed by an SP800-90B compliant seed, which is generated from an entropy source. Each TRNG request generates a 128-bit random number.

This feature has passed internal testing for both SP800-22 and SP800-90B compliance (see [SP800-22 Test Report] and [SP800-90B Test Report]).

The TRNG is initially seeded by calling the APIs to initialize the security engine:

- Compatibility Mode: `mbedtls_platform_setup()`

Periodic reseeding of the TRNG is typically recommended for most applications that utilize a TRNG. Reseeding the TRNG can be performed as follows:

The reseeding interval for Compatibility Mode is configured by defining the macro `MBEDTLS_CTR_DRBG_RESEED_INTERVAL` and setting it to the number of calls to psa_generate_random() that can be made before reseeding is required. The macro can be defined and set using either the e^2 studio IDE or the RA Smart Configurator (*MbedTLS (Crypto Only) module* > *RNG*). Reseeding will occur automatically if needed when `psa_generate_random()` is called.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [SP800-22 Test Report]
- [SP800-90B Test Report]

7. Immutable Memory

A portion of the code flash of the MCU can be configured to be immutable. This property is commonly used to protect critical assets that define the identity of the device and control access to the device through a secure firmware update mechanism.

The RA4M1 supports a Flash Access Window (FAW), whereby all the code flash is configured as immutable except the code flash within a specified address range. The FSP provides APIs for configuring the FAW.

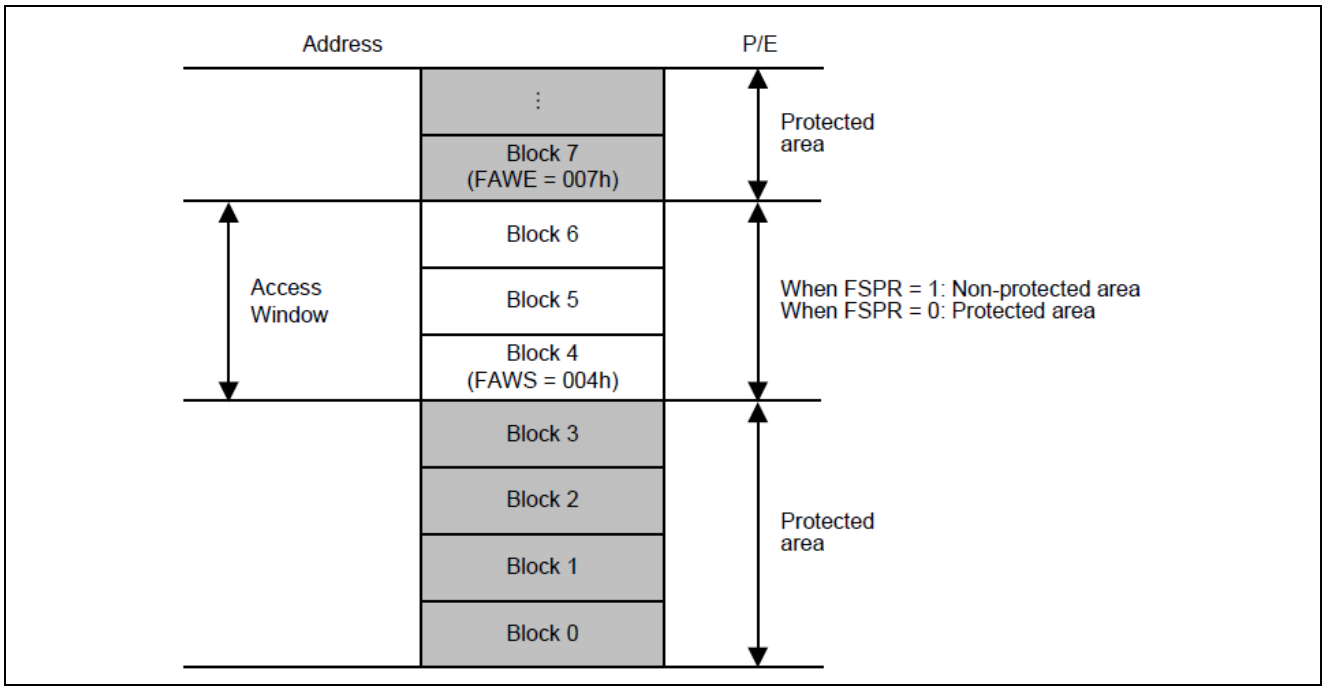

Figure 7. Flash Access Window Example

An application that intends to be configured with immutable flash blocks can be prototyped by leaving the FAW protection bit (FSPR) set to 1. This will allow the FAWS and FAWE registers to be modified.

Production programming of the end-product should configure the FAWS and FAWE registers appropriately and program the FSPR bit to 0. After the FSPR bit is programmed to 0:

- The FAWS and FAWE cannot be changed.
- The Startup Area Select Flag (BTFLG) bit cannot be changed
- The FSPR bit itself cannot be changed.
- The boot firmware “ALeRASE” command cannot be executed.

The code flash blocks that contain the Root of Trust should be made immutable. The immutable Root of Trust contains items such as a secure boot solution, root keys, and certificates.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]
- [Secure Data at Rest]

8. Tamper Protection

8.1 Passive Tamper Detection

Passive tamper detection is provided by the Realtime Clock (RTC) peripheral of the MCU. The RTC can be configured such that a change on one of the input capture pins, RTCICn, triggers a capture of the current RTC value (i.e., the current time) and an optional interrupt. The captured value is retained after reset.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA4M1 User Manual] for the requirements and limitations of this hardware feature.

Figure 8. Passive Tamper Detect shows the passive tamper components included in the RTC.

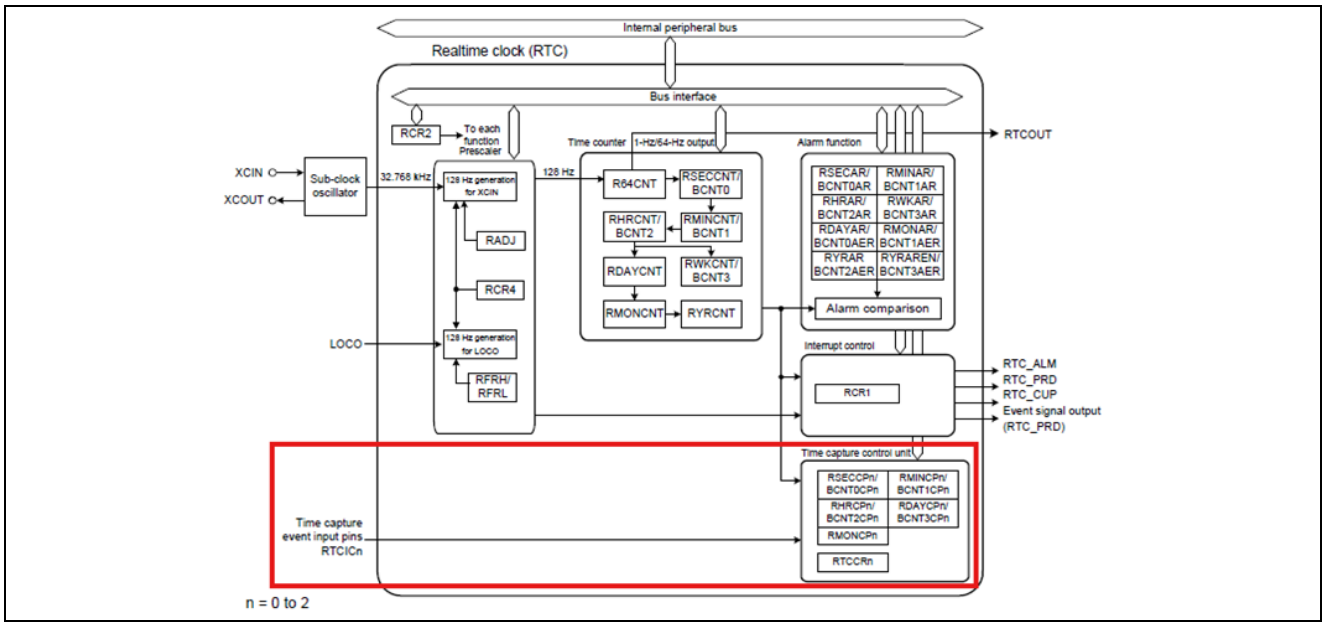

Figure 8. Passive Tamper Detect

Use of the passive tamper detection feature is application-specific and dependent on the end product's threat model. A typical use of passive tamper detection is to detect breaches in the enclosure that would grant an attacker physical access to a sensitive area of the end-product.

It is recommended to place the code that interacts with this peripheral in the Secure region if the application utilizes an isolation mechanism.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]

8.2 SCE5 Protection Features

SCE5 includes protection features designed to safeguard key material against physical and logical attacks.

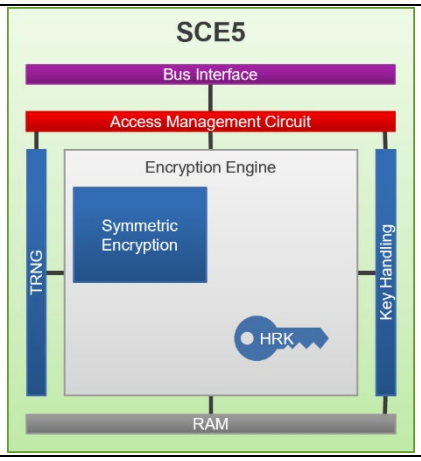

Figure 9. SCE5 Block Diagram

As shown in Figure 9. SCE5 Block Diagram, access to the internal components of the security engine is protected by the Access Management Circuit. The software driver provided in the FSP must be used to perform the various cryptographic functions supported by SCE5. This driver performs the proper authenticated access sequence to interface with the SCE5's Access Management Circuit. Improper access attempts via the CPU or the debugger will result in the Access Management Circuit generating an interrupt (SCE_TADI) and locking the security engine, preventing it from performing cryptographic functions. A device reset is required to clear the error.

The application should use the e^2 studio IDE or the RA Smart Configurator to enable the SCE_TADI interrupt event and call an application-defined ISR. The SCE signal will be armed during the SCE initialization process. The interrupt should be enabled immediately after SCE initialization and disabled before SCE shutdown. It is essential to note that repeating the initialization process will trigger the interrupt, even if the shutdown process has been performed. To prevent any issues, clear the interrupt status before enabling the interrupt; otherwise, the interrupt will trigger when SCE is initialized for a second time.

It is recommended to place the code that interacts with this peripheral in the Secure region if the application utilizes an isolation mechanism.

The following sections provide more details about the additional hardware protection features that are available for each operational mode of the security engine. For more details, refer to the following documents:

- [RA4M1 User Manual]
- [SCE_TADI TU]
- [FSP User Manual]
- [SCE Modes]
- Section 3.3 SCE5
- Section 4 SCE5 Secure Key Injection, Storage, and Usage
- Section 5 SCE5 Cryptographic Functions

8.2.1 SCE5 Compatibility Mode Protection Features

Compatibility Mode offers protection against timing attacks for symmetric cryptographic algorithms.

SPA/DPA protections are not provided for AES operations. This security risk must be analyzed and accepted when considering the use of Compatibility Mode.

8.3 Operational Temperature Monitoring

Some attacks involve operating the MCU outside its specified temperature range to induce erroneous behaviour. The on-chip Temperature Sensor (TSN) peripheral can be used to monitor the die temperature.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA4M1 User Manual] for the requirements and limitations of this hardware feature.

The application code must periodically check the die temperature, compare it to the device's operating range, and trigger a fault if the temperature is outside the range.

If temperature attacks are in scope for the application's threat model, this check should be performed at a rate consistent with the application's threat model.

It is recommended to place the code that interacts with this peripheral in the Secure region if the application utilizes an isolation mechanism.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]

8.4 Operational Voltage Monitoring

Some attacks involve operating the MCU outside its specified voltage range to induce erroneous behavior. The Low Voltage Detection (LVD) peripheral can be used to monitor the voltage level input to the VCC and EXLVD pins and alert if a selectable voltage threshold is crossed.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA4M1 User Manual] for the requirements and limitations of this hardware feature.

The MCU features three programmable voltage monitors.

Voltage Monitor 0 can be configured to be active immediately upon reset, using the voltage level selected in the Option-Setting Memory, which resets the MCU if the voltage drops below the selected value.

It is recommended to configure Voltage Monitor 0 to be active immediately upon reset at a level that is appropriate for the application to mitigate against voltage fault injection attacks.

Voltage Monitor 1 and Voltage Monitor 2 can be configured for more advanced voltage detection scenarios.

It is recommended to place the code that interacts with the LVDs in the Secure region if the application utilizes an isolation mechanism.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]

8.5 Clock Protection

Some attacks involve varying the frequency of the MCU clock to try to induce erroneous behaviour. The Clock Frequency Accuracy Measurement Circuit (CAC) peripheral counts pulses of the measurement target

clock using a measurement reference clock. If the number of pulses falls outside an allowable range, an interrupt is generated.

Refer to the detailed description of this peripheral and its associated electrical characteristics as stated in the [RA4M1 User Manual] for the requirements and limitations of this hardware feature.

If the application uses an external clock and clock attacks are within the scope of the application's threat model, the application should utilize the CAC.

It is recommended to place the code that interacts with this peripheral in the Secure region if the application utilizes an isolation mechanism.

For more details, refer to the following documents:

- [RA4M1 User Manual]
- [FSP User Manual]

9. Internet Connectivity

The RA4M1 MCU Group does not include any hardware to facilitate internet connectivity. If the end-product includes additional hardware that provides internet connectivity, security best practices to support that connectivity in conjunction with the additional hardware should be implemented.

10. Secure Boot

To ensure the secure initialization of the application, it is recommended to utilize and potentially customize the secure bootloader solution provided in the FSP.

10.1 Second Stage Bootloader

The RA4M1 does not have a built-in (i.e., First Stage) secure bootloader; however, it is possible to implement an immutable bootloader using the secure bootloader solution provided in the FSP.

The FSP includes a port of the TrustedFirmware MCUboot project, an open-source secure boot and firmware update solution for 32-bit microcontrollers. Secure boot is usually very application-specific; therefore, Renesas provides multiple examples of how the secure boot solution can be used. Note that secure boot and secure firmware updates are provided as a unified solution.

Review the threat model and start-up time requirements of the application when implementing secure boot. Since all code flash on the RA4M1 is stored inside the chip, and the programmer and debugger interface should be locked upon deployment, it may be sufficient to implement only the secure firmware update portion of the secure bootloader solution.

It is recommended to make the code flash blocks that contain MCUboot immutable to form the application's immutable Root of Trust.

For more details, refer to the following documents:

- [Bootloader Basic]
- [Bootloader Encrypted]
- Section 7 Immutable Memory

11. Secure Firmware Update

The ability to update firmware in an end product is becoming a standard requirement, especially if the product is connected to public infrastructure such as the internet. Any firmware update, whether through public infrastructure or a private connection, should be performed securely.

The FSP includes a port of the TrustedFirmware MCUboot project, an open-source secure boot and firmware update solution for 32-bit microcontrollers. Secure firmware updates are usually very application-specific; therefore, Renesas provides multiple examples of how the secure firmware update solution can be utilized. Note that secure boot and secure firmware updates are provided as a unified solution.

There are many items to consider when devising a secure firmware update strategy, including:

How will the new image be received? Is it received over a secure channel, or does the image need to be encrypted for transfer to the product? A TLS connection can usually be considered a secure channel.

The authenticity of the image needs to be verified before it is programmed for execution. Therefore, the entire image must be received and stored locally. Will the new image be stored on-chip or in an external memory?

If the new image is stored externally before installation, does it need to be encrypted so that an attacker cannot physically extract the plaintext binary?

Be sure to consider the threat model for the end product when architecting a firmware update strategy.

It is recommended that the firmware update strategy include an anti-rollback mechanism to prevent an attacker from regressing the end-product firmware to an older version with exploitable vulnerabilities.

It is recommended to make the code flash blocks that contain MCUboot immutable to form the application's immutable Root of Trust.

For more details, refer to the following documents:

- [Bootloader Basic]
- [Bootloader Encrypted]
- Section 7 Immutable Memory

12. Provisioning

12.1 ID Code Protection

When the MCU is programmed for incorporation into an end product, there are several available options. The most common ones are:

- If there is no desire to re-enable the debugging capability of the MCU or completely erase the flash contents, ID Code bit 127 should be programmed to 0, and either the FSPR bit should be programmed to 0, or the Security MPU should be enabled.
- To maintain the ability to re-enable debugging or completely erase the flash contents via the serial programmer interface, set the ID Code such that bits [127:126] are 0x03 and the remaining bits are a known value (not all 0xFF and not the value for the ALeRASE ("All Erase") command).

- To maintain the ability to re-enable debugging but remove the ability to completely erase the flash contents via the serial programmer interface, set the ID Code such that bits [127:126] are 0x02 and the remaining bits are a known value.

For all cases where serial programmer access is enabled, the following limitations exist:

- If the Flash Access Window has been defined, then a block outside the FAW cannot be erased or programmed.
- If the FSPR bit is 0, then FAWS, FAWE, and BTFLG cannot be programmed, and the FSPR bit cannot be set to 1.

The available configurations are summarised in the following table.

Table 3. ID Code Protection Options

ID Code	ID Code Sent	FSPR=0 or SMPU Enabled	Debugger Access	Serial Programmer Access
All 0xFF	N/A	No	Yes	Yes
	N/A	Yes	Yes	Block erase/program (1)
[127:126]=0x3, [125:0]=ID Code (not all 0xFF)	Match	No	Yes	Yes
	Match	Yes	Yes	Block erase/program (1)
	ALeRASE	No	No	All flash erased
	ALeRASE	Yes	No	No
[127:126]=0x2, [125:0]=ID Code	Match	No	Yes	Yes
	Match	Yes	Yes	Block erase/program (1)
[127]=0, [126:0]=X	Not ALeRASE	N/A	No	No
	ALeRASE	No	No	All flash erased
	ALeRASE	Yes	No	No

Note 1. Limitations:

- If the FAW is enabled and the target area is not entirely within the FAW, Erase and Write commands will fail.
- If FSPR=0, Option-setting memory (Config area) cannot be erased with the Erase command.
- If FSPR=0 and the target area contains FAWS, FAWE, FSPR, or BTFLG, a Write command will fail.

Do not use the value of the ALeRASE command (0x414C_6552_4153_45FF_FFFF_FFFF_FFFF_FFFF) as the ID code.

The most secure configuration is with the ID Code configured with bit 127 programmed to 0 and either the FSPR bit programmed to 0 or the Security MPU enabled; however, the application use case may require the ability to re-enable programming and/or debugging of the end-product. It is recommended to avoid using duplicate ID codes and, optimally, to use a unique ID Code for each chip.

For more details, refer to the following documents and sections of this document:

- [RA4M1 User Manual]
- [Boot Firmware]

13. Website and Support

Visit the following URLs to learn about key elements of the RA family, download components and related documentation, and get support:

RA Product Information	renesas.com/ra
RA4M1 Product Information	renesas.com/RA4M1
RA Product Support Forum	renesas.com/ra/forum
RA Flexible Software Package	renesas.com/FSP
Renesas Support	renesas.com/support
Renesas PSIRT	renesas.com/psirt

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	May.07.26	—	Initial release

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.

(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.