Renesas RA Family

Renesas Security Engine Operational Modes

Introduction

The Secure Crypto Engine (SCE) and Renesas Secure IP (RSIP) security engines that are integrated into RA Family MCUs are selected to provide optimum support for the cryptographic requirements of the MCU's target markets. Most of the security engines can operate in two different modes, Compatibility Mode and Protected Mode.

Compatibility Mode provides straight-forward integration with legacy systems and third-party software and solutions, while offering optimised performance and unlimited secure key storage. In Compatibility Mode, plaintext keys are allowed. Wrapped keys for secure key storage are supported but not required. Generation of wrapped keys is also supported. All security engines used in the RA Family MCUs support Compatibility Mode.

Protected Mode provides optimum protection against security attacks by providing enhanced SPA/DPA resistance and secure key injection and update, with a usage model that enforces secure best practices key handling. In Protected Mode, the security policy ensures that there is never any plaintext key exposure on any CPU or externally accessible bus. Plaintext keys cannot be used when the security engine is operating in Protected Mode. Select security engines used in the RA Family MCUs support Protected Mode.

This Application Note describes the two modes, highlights the advantages and disadvantages of each, and provides guidance for using the two modes. Reference links are provided to existing Renesas RA Family Application Projects demonstrating these two modes, so the user can refer to them for details on the corresponding FSP module usage.

Target Devices

- RA8P1 Group, RA8D2 Group, RA8M2 Group, RA8T2 Group with RSIP-E50D
- RA8D1 Group, RA8M1 Group, RA8T1 Group with RSIP-E51A
- RA4C1 Group with RSIP-E31A
- RA4L1 Group with RSIP-E11A
- RA4M2 Group, RA4M3 Group, RA6M4 Group, RA6M5 Group with SCE9
- RA6M1 Group, RA6M2 Group, RA6M3 Group, RA6T1 Group with SCE7 (Compatibility Mode only)
- RA4M1 Group, RA4W1 Group with SCE5 (Compatibility Mode only)
- RA6T2 Group with SCE5_B (Compatibility Mode only)

Prerequisites and Intended Audience

This application note assumes you have some knowledge about cryptography. The reader is recommended to read the Renesas Secure IP chapter or the Secure Cryptographic Engine chapter of the Hardware User's Manual to understand the basics of the hardware features of the security engine.

The intended audience are product developers, product manufacturers, product support, or end users who are involved with designing application systems involving usage of the Renesas RA Family MCU security engine.

Contents

1. Overview of RA Family MCU Security Engines

Both the RSIP and SCE security engines consist of an access management circuit, a dedicated volatile storage area, cryptographic accelerators, and a random number generation circuit.

There are several types of security engines that reside on the different MCU Groups. all variants of RSIP and only SCE9 support both Compatibility Mode and Protected Mode. The other SCE security engines support Compatibility Mode only.

- **RSIP-E51A**: RA8M1, RA8D1, RA8T1
- **RSIP-E50D**: RA8P1, RA8M2, RA8D2, RA8T2
- **RSIP-E31A**: RA4C1
- **RSIP-E11A**: RA4L1
- **SCE9**: RA4M2, RA4M3, RA6M4, RA6M5
- **SCE7**: RA6M1, RA6M2, RA6M3, RA6T1
- **SCE5**: RA4M1, RA4W1
- **SCE5_B**: RA6T2

1.1 General Structure of the Security Engines

RSIP and SCE have the same general structure. The security engines are an isolated subsystem within the MCU. The internal cryptographic operations are isolated from any CPU-accessible bus. Renesas's unique secure key handling capabilities enable the creation of solutions that have no plaintext key exposure outside the crypto engine.

Figure 1 is the RSIP structural feature representation. This representation is a super set of features of all the security engines on the RA Family MCUs. Different versions of the security engines offer different security feature sets, but the structural features are common. See section 1.2 for details on the differences.

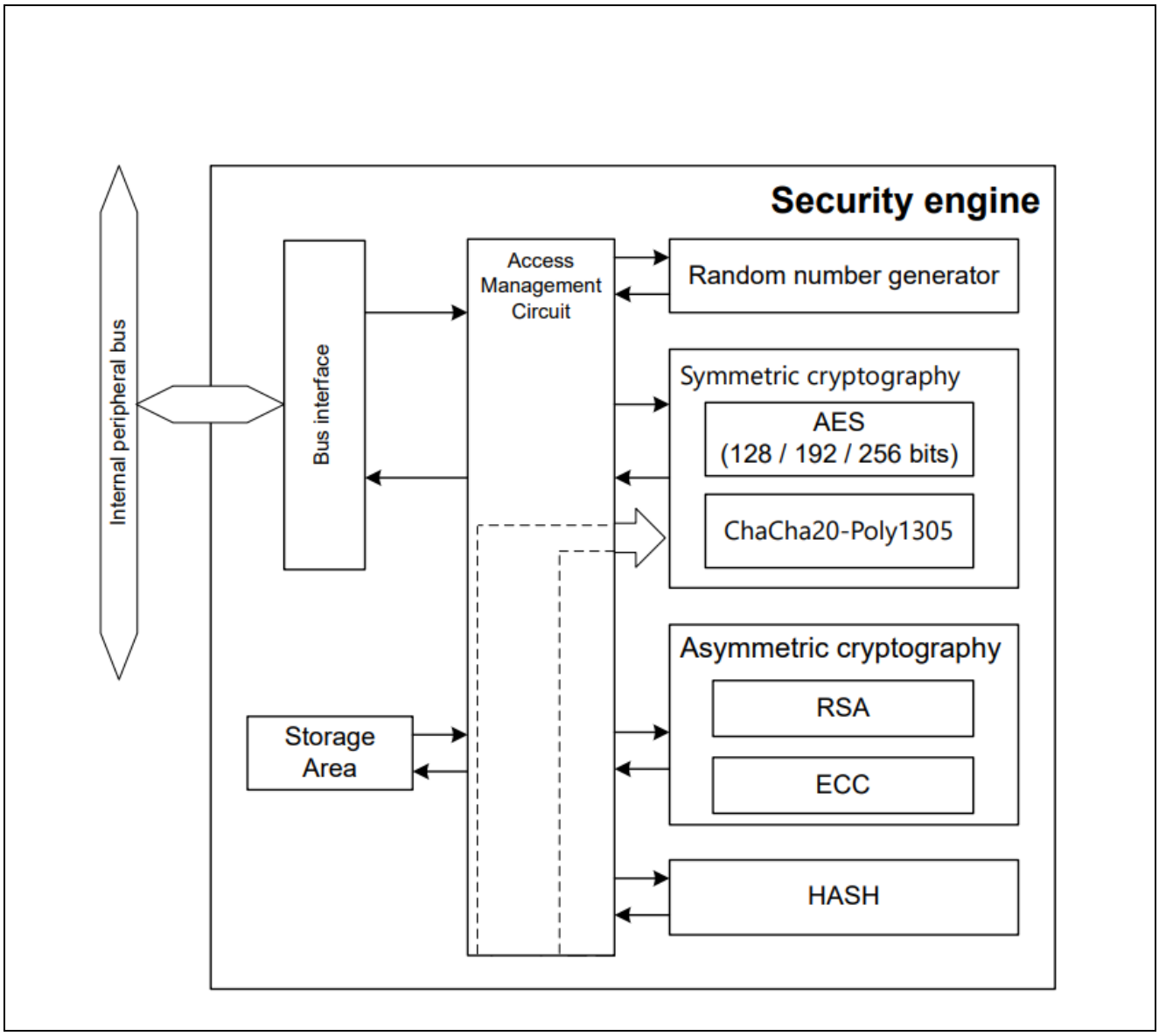

Figure 1. RSIP Structural Features

1.2 Cryptographic Capabilities of the Security Engines

The following table summarizes the capabilities of the security engines, as supported by the Flexible Software Package (FSP).

Table 1. Security Engine Cryptographic Capabilities

		RSIP-E51A	RSIP-E50D	RSIP-E31A	RSIP-E11A	SCE9	SCE7	SCE5_B	SCE5
Identity & Key Exchange (Asymmetric)									
RSA	Key Generation, Sign/Verify	Up to 4K	Up to 4K	-	-	Key gen, sign: Up to 2K Verify: Up to 4K	Up to 2K	-	-
ECC	Key Generation, ECDSA, ECDH	Up to 521 bits	Up to 521 bits	Up to 384 bits	Up to 256 bits	Up to 512 bits	Up to 384 bits	-	-
Ed25519	Key Generation, EdDSA	Y	Y	Y	-	-	-	-	-
Privacy (Symmetric)									
AES	ECB, CBC, CTR	128/192/256	128/192/256	128/256	128/256	128/192/256	128/192/256	128/256	128/256
	GCTR	128/192/256	128/192/256	128/256	128/256	128/192/256	128/192/256	128/256	128/256
	XTS	128/256	128/256	-	-	128/256	128/256	-	-
	CCM, GCM, CMAC	128/192/256	128/192/256	128/256	128/256	128/192/256	128/192/256	128/256	128/256
ChaCha20	Poly1305	-	Y	-	-	-	-	-	-
Data Integrity									
Hash	GHASH	Y	Y	Y	Y	Y	Y	Y	Y
	HMAC	Y	Y	Y	Y	Y	Y	-	-
	SHA-2 (224/256)	Y	Y	Y	Y	Y	Y	-	-
	SHA-2 (384/512)	Y	Y	Y	-	-	-	-	-
	SHA-3 (224/256/384/512)	-	Y	-	-	-	-	-	-
TRNG	HW Entropy, SP800-90B	Y	Y	Y	Y	Y	Y	Y	Y
Key Handling									
Wrapped	Secure key storage	256-bit HUK	256-bit HUK	256-bit HUK	256-bit HUK	256-bit HUK	128-bit DHUK	128-bit DHUK	128-bit DHUK
Plaintext	Legacy compatibility	Y	Y	Y	Y	Y	Y	Y	Y
Physical Protection									
Protected Mode available		Y	Y	Y	Y	Y	-	-	-
SPA/DPA resistance		PM[1] and CM[2]	PM and CM	PM and CM	PM only	PM only	-	-	-
Timing attack resistance		Y	Y	Y	Y	Y	Y	Y	Y
Certification									
NIST CAVP		Y	Y	Y	Y	Y	Y	-	-

The following are some highlights of each of the security engines:

- SCE5 and SCE5_B provide hardware-accelerated symmetric encryption for confidentiality.
- SCE7 adds hardware-accelerated asymmetric encryption and advanced hash functions for integrity and authentication. SCE7 AES, SHA, and random number generation DRBG are NIST CAVP certified.
- SCE9 extends asymmetric encryption support for RSA up to 4K and enhanced key storage capability with a Hardware Unique Key (HUK). The full complement of algorithms is NIST CAVP certified.
- RSIP-E31A builds on this by expanding ECC and SHA-2 support up to 384 bits, adding Ed25519 support, and providing SPA/DPA resistance for both Protected Mode and Compatibility Mode.
- RSIP-E51A offers a broader set of cryptographic features. It supports RSA, including signature and key generation, up to 4K bits, ECC up to 521 bits, and a wide range of symmetric AES modes with all three key lengths. Additionally, it provides SPA/DPA resistance for both Protected Mode and Compatibility Mode.
- RSIP-E50D offers the widest range of functions among all types, encompassing all functionalities of the earlier versions. It further enhances data integrity with SHA3 and extends symmetric cryptographic capabilities with support for ChaCha20-Poly1305.

[1] PM – Protected Mode, available for select security engines

[2] CM – Compatibility Mode, available for all security engines

1.3 Key Handling Capabilities of the Security Engines

1.3.1 Support for Wrapped Keys

Renesas RA Family MCUs have the unique ability to store and use cryptographic keys in wrapped format. Wrapping involves encrypting and signing the key with either the MCU's Hardware Unique Key (HUK) or a derived key based on the MCU's Unique ID. Since these Key Encryption Keys are unique for each individual MCU, even if an attacker were able to extract the wrapped key, another MCU will not be able to use it.

In Compatibility Mode, plaintext keys and wrapped keys can be used by application software. Plaintext keys can be wrapped by application software. Wrapped keys can also be generated by the security. The application software can then use the wrapped keys via the PSA Certified Crypto APIs.

In Protected Mode, only wrapped keys can be used by application software. Wrapped keys can be generated by the security engines (RSIP, SCE9), and known keys can be securely injected via a device programmer. Application software can update the application with new keys by using a previously injected Key-Update Key, which must be injected via a device programmer. Refer to the Renesas RA Family Injecting and Updating Secure User Keys (R11AN0496) Application Project for more information about this process.

1.3.2 Support for Plaintext Keys

Plaintext keys are often required to provide legacy system support or to integrate with various software stacks and libraries. The security engine's Compatibility Mode supports plaintext key usage.

The security engine (RSIP, SCE9) Protected Mode does not support plaintext keys. Having plaintext keys present in the application is inherently a security risk, because it is possible that malicious code could exploit system weaknesses and obtain the plaintext key data. This risk may be determined to be low enough to be acceptable, but the risk does exist. Protected Mode protects against this risk by not supporting plaintext key usage.

2. Compatibility Mode of the Security Engines

Compatibility Mode provides straight-forward integration with legacy systems and third-party software and solutions, while offering optimised performance and unlimited secure key storage.

2.1 Advantages of Compatibility Mode

The following are some advantages when using Compatibility Mode.

- Plaintext keys are allowed, including support for wrapping plaintext keys. This provides compatibility with legacy systems and simplifies software development. It can also be necessary to integrate with existing software and infrastructure. Many existing programming systems support plaintext key injection, often using application code to securely store the key on chip.
- Wrapped keys for secure key storage are supported but not required. Generation of wrapped keys is also supported.

2.2 Disadvantages of Compatibility Mode

The following are some disadvantages when using Compatibility Mode.

- Potential user key exposure if plaintext keys are used. The user must evaluate the potential threats and risk of this exposure and implement their design accordingly.
- Secure key injection is more complicated than for Protected Mode, as it involves application-level code.
- Secure key update is limited, as there will be plaintext exposure outside the security engine.
- Limited protection against SPA/DPA attacks.
- Countermeasures for timing attacks are implemented. The AES, ECC, and RSA implementations are constant-time when dealing with sensitive key material.
- The MCU's boot firmware does not support Compatibility Mode. Security features that leverage the boot firmware, such as secure key injection via the boot firmware serial interface and First-Stage Bootloader setup, will utilise Protected Mode.

2.3 Compatibility Mode Support with Renesas RA Family FSP

Compatibility Mode is supported by all RA security engines. This mode is supported by the PSA Certified Crypto APIs and can be accessed using the FSP's "Mbed TLS (Crypto Only)" module, included in FSP

v2.0.0 or later. There are several application projects that demonstrate the SCE and RSIP operating in Compatibility mode. Refer to the Reference section items **9** to **13**.

3. Protected Mode of the Security Engines

Protected Mode provides optimum protection against security attacks by providing SPA/DPA resistance and secure key injection and update, with a usage model that enforces secure best practices key handling.

3.1 Advantages of Protected Mode

Protected Mode has many security advantages listed as follows:

- No plaintext key exposure on any CPU or externally accessible bus.
- Secure key injection using the MCU boot interface simplifies secure key provisioning.
- Secure key update via user-installed Key-Update Keys enables secure key update in the field.
- Full SPA/DPA side-channel attack resistance is included. Side-channel attack using power analysis is one of the most frequent attacks used to extract sensitive information from a chip.
- Countermeasures for timing attacks are implemented. The AES, ECC, and RSA implementations are constant-time when dealing with sensitive key material.
- The MCU's boot firmware supports Protected Mode. Security features that leverage the boot firmware, such as secure key injection via the boot firmware serial interface and First-Stage Bootloader setup, will utilise Protected Mode.
- The API is designed to be compatible with the TSIP and RSIP libraries for RX Family MCUs and RZ Family MPUs.

3.2 Disadvantages of Protected Mode

The following are the potential disadvantages of using Protected Mode:

- Plaintext keys are not allowed, which can introduce difficulties integrating with legacy systems and software.
- For cryptographic protocols that need key calculation, for example ECDH and ECIES, key calculation must be done within the security engine. Depending on the specific protocol, this functionality may or may not be supported by the FSP and may be challenging to integrate with third party stacks.

3.3 Protected Mode Support with Renesas RA Family FSP

The SCE9 Protected Mode can be accessed using the FSP Crypto module (`r_sce_protected`).

The RSIP Protected Mode can be accessed using the FSP Crypto module (`r_rsip_protected`).

Additionally, support for other libraries (for example, TLS) will be integrated into later FSP releases.

Protected Mode supports wrapped user key generation via FSP Crypto API calls and key injection via the MCU boot firmware interface using the Renesas Flash Programmer (RFP) and select third-party tools.

Field update of user keys can be achieved by injecting one or more Key-Update Keys via the MCU boot firmware serial interface. New keys are then injected using one of the previously injected Key-Update Keys and the FSP Crypto APIs.

To get hands-on experience using the SCE9 and RSIP Protected Mode with FSP Crypto APIs, a user can reference the *Renesas RA Family Injecting and Updating Secure User Keys* Application Project. This Application Project includes an Application Note that provides step-by-step instructions on how to perform application key and Key-Update Key injection. In addition, a reference example software project is provided to demonstrate key update via the previously injected Key-Update Key and FSP Crypto APIs. See the Reference section for information on this Application Project.

4. Security Engines Operational Modes Summary

The PSA Certified Crypto API implementation uses RSIP and SCE Compatibility Mode. The FSP Crypto API implementation uses RSIP and SCE9 Protected Mode. The following table provides a side-by-side comparison of the two modes regarding key formats, key injection support from FSP, and inoperability between the two different operation modes. Note that RSIP and SCE9 keys injected via the MCU boot firmware interface cannot be used in Compatibility Mode. SCE5_B supports only Compatibility Mode;

therefore, SCE5_B key injection via the MCU boot firmware interface is performed in Compatibility Mode. MCUs with the SCE7 and SCE5 security engines do not support key injection via the MCU boot firmware interface.

Figure 2. Detailed Keys Capabilities support mode

5. Mode Selection based on Application Use Cases

This section introduces some of the common cryptographic application use cases. Information on the SCE and RSIP operational modes support status for these use cases is provided for user's reference.

5.1 Trusted Firmware-M (TF-M)

Trusted Firmware-M (TF-M) implements a Secure Processing Environment (SPE) for Armv8-M, Armv8.1-M architectures (for example, the Arm® Cortex®-M33 and Cortex-M85 cores). Renesas RA Family FSP has integrated TF-M support starting with FSP v2.0.0 for use on Arm TrustZone®-enabled MCUs.

The FSP port of TF-M supports the PSA Certified Crypto APIs with integrated support for RSIP and SCE Compatibility Mode for cryptographic operations. This support allows the customer to benefit from the Trusted Firmware ecosystem software.

5.2 Internet Connectivity

The FSP has integrated Amazon FreeRTOS and Trusted Firmware Mbed TLS support. Compatibility Mode is used when integrating with this software combination.

The FSP also integrates Azure RTOS and NetX Duo support. Compatibility Mode is used for this software combination.

Internet connectivity solutions using SCE9 Protected Mode are currently available from Renesas Partner wolfSSL Inc., providing optimum secure key storage.

5.3 Private Infrastructure Connectivity

For private infrastructure in industrial or networking applications, it is recommended, if possible, to use Protected Mode with FSP Crypto APIs for increased security considerations.

If plaintext private keys must be used, for example, to interface with existing infrastructure, then Compatibility Mode with PSA Certified Crypto APIs must be used.

5.4 Production Support and Supply Chain Considerations

Protected Mode provides the following benefits for customers who are concerned with protecting their supply chain:

- Secure key injection can be conveniently performed in production for all MCUs.
- With RA Family MCUs, OEMs can further lock down the secure key storage and IP region for enhanced security control prior to hardware delivery downstream.

Secure key injection solutions for both Protected Mode and Compatibility Mode are available from third-party Partners. Contact Renesas for more information.

6. References

1. Renesas RA Family MCU RA6T2 Group User's Manual: Hardware
2. Renesas RA Family MCU RA4M1 Group User's Manual: Hardware
3. Renesas RA Family MCU RA6M3 Group User's Manual: Hardware
4. Renesas RA Family MCU RA6M4 Group User's Manual: Hardware
5. Renesas RA Family MCU RA4L1 Group User's Manual: Hardware
6. Renesas RA Family MCU RA4C1 Group User's Manual: Hardware
7. Renesas RA Family MCU RA8M1 Group User's Manual: Hardware
8. Renesas RA Family MCU RA8P1 Group User's Manual: Hardware
9. Renesas RA Family Establishing and Protecting Device Identity using SCE7 and FAW (R11AN0449)
10. Renesas RA Family MCU Establishing and Protecting the Device Identity using SCE9 and Arm TrustZone (R11AN0475)
11. Renesas RA Family MCU Injecting Plaintext User Keys (R11AN0473)
12. Renesas RA Family Using Trusted Firmware M (TF-M) with FSP v2.0.3 (R11AN0493)
13. Renesas RA Family Injecting and Updating Secure User Keys (R11AN0496)

7. Website and Support

Visit the following URLs to learn about the RA family of microcontrollers, download tools and documentation, and get support.

RA Family Product Information	renesas.com/ra
Flexible Software Package (FSP)	renesas.com/ra/fsp
RA Family Product Support Forum	renesas.com/ra/forum
Renesas Support	renesas.com/support
Renesas Secure – IoT	renesas.com/iot-security

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	May.18.21	-	First release
1.10	Oct.03.22	Multiple	Minor updates
1.20	Nov.15.24	Multiple	Add the Renesas Secure IP of the RA8 MCUs series
1.30	Oct.09.25	Multiple	Update RSIP-E50D of the RA8 MCUs series. Correct the Security Engine Cryptographic Capabilities table. Remove out of scope information.

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/.