Renesas RA Family

Renesas Security Engine Operational Modes

Introduction

Renesas RA Family MCUs implements Security Engines of different configuration and capabilities. RA8 MCU series implements Renesas Secure IP (RSIP). Some RA6 and RA4 MCU families implement Secure Cryptographic Engine 9 (SCE9). Both RSIP and SCE9 can operate in two different modes, Compatibility Mode and Protected Mode. The other security engines support Compatibility Mode only.

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.

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. In Protected Mode, secure key provisioning is supported and there is no plaintext key exposure on any CPU or externally accessible bus. Plaintext keys cannot be used when the security engine is operating in 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

- RA4M2 Group, RA4M3 Group, RA6M4 Group, RA6M5 Group
- RA8D1 Group, RA8M1 Group, RA8T1 Group
- RA6M1, RA6M2, RA6M3, RA6T1 (Compatibility Mode only)
- RA4M1, RA4W1 (Compatibility Mode only)
- RA6T2 (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 and Secure Cryptographic Engine (SCE9) 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 SCE9 include a security engine which consists of an access management circuit, storage area, encryption/decryption circuit, and random number generation circuit.
At the time of release, there are five types of security engines that reside on the different MCU Groups. Only RSIP and SCE9 support both Compatibility Mode and Protected Mode. The other security engines support Compatibility Mode only.

- **RSIP-E51A**: RA8M1, RA8D1, RA8T1
- **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 SCE9 have similar general structures. The difference is that RSIP supports additional security components compared with SCE9. RSIP and SCE9 are an isolated subsystem within the MCU. The internal cryptographic operations are isolated from a 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.

Compared with SCE9, the RSIP supports two additional functionalities in addition to some added cryptographic algorithms (refer to the Hardware User Manual for the specific MCU Group to confirm support for these features):

- Generation of the key data for the decryption-on-the-fly IP (DOTF) through a dedicated bus. Both Protected Mode and Compatibility Mode are supported.
- Maintains the OEM BL Version that is used by the First Stage Bootloader (OEM BL Ver.). Only Protected Mode is supported.

Figure 1 is the RSIP structural feature representation. This representation is a super set of features of all the security engines on the RA 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.

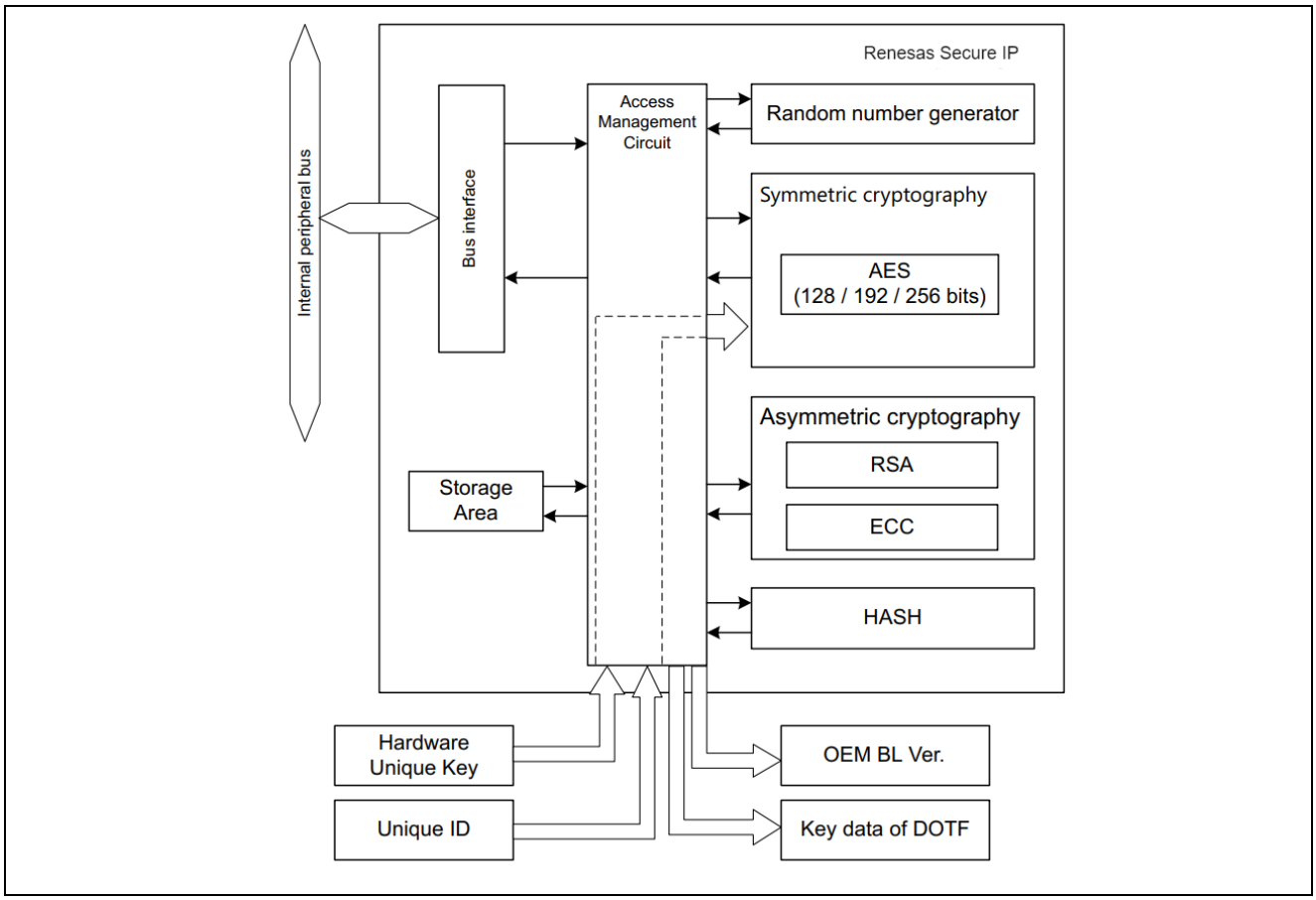

Figure 1. RSIP Structural Features

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

Functions		RSIP	SCE9	SCE7	SCE5, SCE5_B
RSA	Key Generation, Sign/Verify	Up to 4K	Up to 4K (RSA 3K/4K - Verify only)	Up to 2K	-
ECC	Key Generation, ECDSA, ECDH	Up to 521 bit	Up to 512 bit	Up to 384 bit	-
AES	ECB, CBC, CTR	128/192/256	128/192/256	128/192/256	128/256
	GCTR	128/192/256	128/192/256	128/192/256	-
	XTS	128/256	128/256	128/256	-
	CCM, GCM, CMAC	128/192/256	128/192/256	128/192/256	128/256
Hash	GHASH	Y	Y	Y	Y
	HMAC	SHA224/256/384/512	SHA224/256	SHA224/256	-
	SHA2 (224/256)	Y	Y	Y	-
	SHA2 (384/512)	Y	-	-	-
TRNG	HW Entropy, DRBG-AES-128	Y	Y	Y	Y
Wrapped	Key confidentiality, authenticity	Y	Y	Y	Y
Plaintext	Legacy compatibility	Y	Y	Y	Y
Modes	Operational Modes	Compatibility Mode, Protected Mode	Compatibility Mode, Protected Mode	Compatibility Mode	Compatibility Mode

The following are some highlights of the features of each of the Security Engine modules:

- 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 expands upon the SCE9 by adding advanced cryptographic algorithms like EdDSA, ECC secp521r1, SHA384, and SHA512.

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 Hardware Root Key and MCU's Unique ID. Since these 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 Engine (RSIP, SCE9, SCE7, SCE5 or SCE5_B). 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 Installing and Updating Secure Keys* 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. 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 installation, 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.

- No Simple Power Analysis (SPA) and Differential Power Analysis (DPA) protections.
- 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 SCE and RSIP.

2.3 Compatibility Mode Support with Renesas RA Family FSP

The Compatibility Mode is supported by all RA security engines. This mode can be accessed using FSP Mbed Crypto module, the PSA Certified Crypto APIs, or the Network connection stacks 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 3 to 0.

3. The 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 Key enables secure key update in the field.
- 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. Renesas RA Family SCE9 and RSIP Protected Mode implement countermeasures against such attacks.
- Countermeasures for timing attacks are implemented. The ECC and RSA implementation on SCE9 and RSIP are constant time when dealing with sensitive key material.
- The implemented API is designed to be compatible with the RX Family TSIP Library, facilitating the porting of software between Renesas MCU families.

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 needs key calculation, for example ECDH and ECIES, key calculation must be done within the SCE9 and RSIP. Depending on the specific protocol, this functionality may or may not be supported by the FSP.

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 interface using RFP.

Field update of user keys can be achieved by injecting one or more Key-Update Keys via the MCU boot 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 Installing and Updating Secure 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 keys injected via the MCU boot interface (that is, the factory boot firmware) cannot be used in Compatibility Mode with RSIP and SCE9. SCE5_B key injection via the MCU boot mode is performed in Compatibility Mode.

Detailed Keys Capabilities	Compatibility Mode PSA Crypto API	Protected Mode FSP Crypto API
Plaintext Symmetric and Private Keys		
Injection via factory bootloader	No	No
Injection via FSP	Yes	
Creation via key generation	No	
Usage within FSP	Yes	
Standard Format Public Keys		
Injection via factory bootloader	No	No
Injection via FSP	Yes	
Creation via key generation	Yes	
Usage within FSP	Yes	
MCU-wrapped Symmetric and Private Keys		
Secure injection via factory bootloader	No	Yes
Secure injection via FSP	Yes	No
Secure update via FSP	Yes*	Yes
Creation via key generation	Yes	Yes
Usage within FSP	Yes	Yes
Cross-mode compatibility	**No**	**No**
MAC-tagged Public Keys		
Secure injection via factory bootloader	No	Yes
Secure injection via FSP		No
Secure update via FSP		Yes
Creation via key generation		Yes
Usage within FSP		Yes
Cross-mode compatibility	**No**	**No**

Ensures optimal key storage protection

Enables legacy system and software support

Simplifies secure provisioning

Removes Renesas DLM server dependency. Protects against malicious key injection.

Provides authenticity and integrity check of public key.

Note on *: There is no KUK in Compatibility Mode. Key update is done manually, with key exposure outside the MCU.

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 are provided for user's reference.

5.1 Trusted Firmware M (TF-M)

Trusted Firmware-M (TF-M) implements the Secure Processing Environment (SPE) for Armv8-M, Armv8.1-M architectures (for example, the Arm® Cortex®-M33, Cortex-M23, Cortex-M85 processors) or dual-core platforms. Renesas RA Family FSP integrated TF-M support starting with FSP v2.0.0 for use on TrustZone-enabled MCUs.

TF-M uses PSA Certified Crypto APIs, RSIP and SCE Compatibility Mode for cryptographic operations. This support allows the customer to benefit from the Arm PSA Ecosystem software.

5.2 Internet Connectivity

The FSP has integrated Amazon FreeRTOS and MbedTLS 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 Protected Mode are currently available from Renesas Partner wolfSSL Inc., providing optimum secure key storage.

5.3 Private Infrastructure Connectivity

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

If plaintext 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.

6. References

1. Renesas RA Family MCU RA6M4 Group User's Manual: Hardware
2. Renesas RA Family MCU RA6M3 Group User's Manual: Hardware
3. Renesas RA Family MCU RA8M1 Group User's Manual: Hardware
4. Renesas RA Family MCU Establishing and Protecting the Device Identity using SCE7 and FAW (R11AN0449)
5. Renesas RA Family MCU Establishing and Protecting the Device Identity using SCE9 and Arm TrustZone (R11AN0475)
6. Renesas RA Family MCU Injecting Plaintext User Keys (R11AN0473)
7. Using Trusted Firmware M (TF-M) with FSP v2.03 (R11AN0493)
8. 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

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/.