RX Family

Security Guide for MCUs with Encryption Functions

Introduction

This document provides guidance on the safe and secure use of RX Family MCUs with encryption functions.

Target Devices

Products with Trusted Secure IP or Trusted Secure IP Lite: RX671 Group

Products without Trusted Secure IP or Trusted Secure IP Lite: RX140 Group

Contents

1. Introduction 2

2. General Security Requirements 3

2.1 Protection of Confidential Technical Information and Development Tools 3

2.2 Handling of Discarded Items 3

3. Guidance on Programming and Usage 4

3.1 General Requirements Related to Development of Internal Software 4

3.2 Use of On-Chip Memory 5

3.2.1 Use of Flash Memory 5

3.2.2 Transport Keys 5

3.2.3 Use of RAM 5

3.3 Encryption 6

3.4 Data Transfer 6

3.5 Random Numbers 6

3.5.1 Use of TRNG 6

3.5.1.1 Checking TRNG Hardware 6

4. Conclusion 7

Revision History 8

1. Introduction

This security guide has been prepared to enable the safe and secure use of RX Family MCUs with encryption functions.

In addition to the implementation of security functions, Renesas undertakes special security management during the design process. As part of this effort, Renesas recommends that customers endeavor to meet the environmental security requirements described in this document. Unless otherwise specified, the description in this guide applies to all the target devices.

This document provides guidance on developing software based on an awareness of the protection and security of MCU security information. This guidance document takes as its basis general secure programming techniques, knowledge of how MCUs operate, and vulnerability analysis including the use of rating agencies. All of these are intended as guidelines rather than indispensable conditions. It is up to the customer (or the rating agency) to decide whether or not these guidelines are appropriate to particular use cases, as well as whether or not the implementation methods in the guidelines (or other methods) are required in particular use cases.

This document contains guidance on using RX Family MCUs more effectively, but since each application and its associated requirements are different, there is no guarantee that a given set of measures will be appropriate, or even adequate, for a specific application. Generally speaking, in order to confirm these points for the finished product, it is necessary to perform a final evaluation of the product in which the hardware and internal software are combined.

This document is not part of a binding agreement with Renesas. Should any inconsistencies arise, the specifications and performance stipulated in the related delivery specifications (when applicable) or the current version of the User’s Manual: Hardware shall apply.

2. General Security Requirements

To protect the internal information on the MCU, we recommend investigating the threats that may exist for the MCU's internal information when the final product is placed in a situation other than the environment in which it is normally used.

2.1 Protection of Confidential Technical Information and Development Tools

A variety of tools and information are provided to assist in the development of applications based on RX Family MCUs, such as the User's Manual: Hardware, application notes, and sample software. Some of these are subject to non-disclosure agreements, and the terms of such agreements must be strictly observed. Unauthorized disclosure of such information or tools could reduce the effectiveness of the security functions built into RX Family MCUs.

In like manner, if maintaining the confidentiality and integrity of the information in the code flash memory and data flash memory over the product life cycle is among the customer's requirements for the product, this requirement must also be satisfied. This also applies to the creation, distribution, management, and discarding of data.

Always ensure that the keys used by encryption software are generated, stored, and used in a secure manner over the life cycle of the product.

2.2 Handling of Discarded Items

When investigating possible methods of attacking an MCU or application, it is important to ensure that all discarded items are disposed of securely so that they can no longer be used. If important security-related information is stored in the MCU's memory, we recommended that this information be deleted before discarding the MCU. One means of disposing of MCUs is to pulverize them into tiny fragments using a grinder.

3. Guidance on Programming and Usage

Many security-related requirements for MCUs have to do with interaction between the functions of the internal software and the hardware. Relevant recommendations for RX Family MCUs are presented in this chapter.

3.1 General Requirements Related to Development of Internal Software

When developing software that utilizes encryption functions, it is necessary to follow the usage procedures described in the User's Manual: Hardware and to consider the guidance contained in this document.

In encryption processing utilizing encryption functions, make sure to implement and make use of a key handling routine in order to minimize the danger of losing encryption keys when the software is run.

For example, the following practices can be mentioned.

- The necessity of ensuring the integrity of keys (and key pairs)
- The necessity of ensuring that keys are unique and strongly encrypted to guarantee sufficient reliability
- In the case of asymmetric algorithms, the necessity of ensuring that in practical terms the private key cannot be extracted from the public key
- When importing keys from an external source, the necessity of having a system in place that ensures that the keys are of sufficient quality and confidentiality to meet the requirements of the application

With regard to key management on products with TSIP or TSIP-Lite, Renesas offers a Key Wrap service with a dedicated webpage that customers can use to encrypt keys securely, and we recommend its use alongside the key index generation API provided with the TSIP driver. Please contact your Renesas sales representative for details.

3.2 Use of On-Chip Memory

RX Family MCUs are provided with three types of memory: code flash memory, data flash memory, and RAM. The degree of security and the applications differ among the different types of memory. The following guidance is provided in order to maximize the security of each type of memory.

It is also necessary to consider requirements other than those presented below when reading important data from memory and when writing it to memory.

3.2.1 Use of Flash Memory

RX Family MCUs are provided with protection functions for user programs. Refer to the User's Manual: Hardware for details.

- Code flash memory and startup program protection functions
  These functions protect the program that runs after a reset (the startup program). They provide a secure update procedure in case the programming operation is interrupted by a reset, or the like, while the startup program is being updated. In addition, by making settings for the area protection function it is possible to protect the startup program and to fix the selection status of the startup area specified in the option setting memory. These functions enable users to boot their RX Family MCUs with a startup program that is highly secure.
  It is recommended that the startup program first verify the data in the code flash memory and confirm that it has not been tampered with before running the customer's program. On products with TSIP or TSIP-Lite, we recommend using the secure boot API provided with the TSIP driver.

- On-chip debugger and serial programmer connection protection function
  Settings in option setting memory can be used to enable or disable on-chip debugger connection and to enable or disable connection to the code flash memory or data flash memory using a serial programmer. To prevent leaks of confidential data, we recommend that both on-chip debugger and serial programmer connections be disabled when the product is shipped to the customer.

- Parallel programmer connection protection function
  This function can be used to control read, program, and erase access to the code flash memory when a parallel programmer is connected by setting the ROM code bits in the ROM code protect register. To prevent leaks of confidential data and unintended overwriting of data, we recommend making protection function settings when the product is shipped to the customer.

3.2.2 Transport Keys

We recommend that the internal software implement some sort of transport key system to reduce the danger of unauthorized use of customers' products. This makes it possible to specify that confidential data (a password, etc.) is required to access an RX Family MCU and to limit access to RX Family MCUs during the period up to when the product is shipped to the final user.

Using values consisting of all ones or all zeros as transport keys should be avoided. The danger of code being altered, either accidentally or intentionally, is reduced substantially when values consisting of a mixture of ones and zeros are used.

3.2.3 Use of RAM

We recommend erasing any unneeded data from the RAM after security processing is finished so that no such data remains.

3.3 Encryption

Encryption is one of the principal security systems used in applications. Encryption technology protects data stored on the MCU and also makes possible protection of various processes such as data transfer, authentication, and verification with external devices and systems.

3.4 Data Transfer

As far as possible, configuration and transfer of important data should not be performed on products without TSIP or TSIP-Lite without first instituting data protection measures such as authentication of users or external devices. We also recommend incorporating a secure counter into the authentication system to limit the number of verification attempts.

3.5 Random Numbers

Using good quality random numbers enhances the security environment.

The true random number generator (TRNG) on products with TSIP or TSIP-Lite is designed and verified to ensure generation of good quality random numbers in a normal operating environment.

The output of the random number generator on products without TSIP or TSIP-Lite should not be used unmodified as key information but should first undergo conditioning.

3.5.1 Use of TRNG

The TRNG plays an important role in many applications. In particular, make sure to follow the guidance in this document when using the output of the TRNG for important applications such as key generation. For other applications, decide on an appropriate verification method, taking into account factors such as the purpose for which the random numbers will be used and post-processing by software.

3.5.1.1 Checking TRNG Hardware

To detect possible faults in the operation of the TRNG, make sure to verify with internal software that the TRNG is functioning properly before actually making use of random numbers generated by the TRNG.

We recommend that appropriate statistical testing be performed on the output of the TRNG in order to detect the most commonly occurring fault mechanisms.

4. Conclusion

This guidance consists of recommendations intended to enable users to make effective use of the security functions of RX Family MCUs. Further protective measures to prevent loss of the functionality of the internal software exist in addition to the those referred to in this document, and we encourage you to implement them as necessary.

In order to protect information systems from unauthorized external access when building systems for customers, we encourage you to make effective use of the security functions of the TSIP driver on products with TSIP or TSIP-Lite. Also investigate the implementation of multilayered defenses appropriate to the customer's usage environment (multiple security measures such as software updates, data access restrictions, and network decentralization).

Renesas has put in place a Product Security Incident Response Team (PSIRT). Feel free to contact the Renesas PSIRT with any concerns you may have regarding vulnerabilities affecting Renesas products.

Renesas PSIRT webpage: https://www.renesas.com/psirt

Please contact your Renesas sales representative should you require any further information.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Sep. 3, 2021	—	First edition issued
1.01	May 11, 2022	All	Support for RX140 added

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/.