RX Family

RSA Library Firmware Integration Technology

R20AN0292EJ0104
Rev.1.04
Oct.31.2022

Introduction

This application note explains information for implementing the RX Family RSA library (hereafter referred to as the RSA FIT library) using Firmware Integration Technology (FIT). The RSA library is a software library for implementing RSA signatures on RX microcontrollers.

And RSA FIT library package also includes RSA driver function.

Please refer to the User's Manual (R20UW0115JJ0200) to know how to use this software library.

Target Device

RX Family

When applying this application note to other microcontrollers, please modify it according to the specifications of the microcontroller and evaluate it thoroughly.

Target Compiler

Renesas Electronics C/C++ Compiler Package for RX Family

GCC for Renesas RX

IAR Embedded Workbench for Renesas RX

For detailed information on the compiler's system requirements, please refer to Section "4.1 Confirmed Operation Environment".

Related Documents

Firmware Integration Technology User’s Manual (R01AN1833)

Board Support Package Module Using Firmware Integration Technology (R01AN1685)

Adding Firmware Integration Technology Modules to Projects (R01AN1723)

Adding Firmware Integration Technology Modules to CS+ Projects (R01AN1826)

Renesas e2studio Smart Configurator User's Guide (R20AN0451)

Contents

1. Overview

1.1 RSA FIT Library

This library is used as an API to be embedded in a project. See "2.8 Adding the FIT Module to Your Project " for details on how to incorporate this library.

1.2 RSA FIT Library Overview

RSA library signature generation and signature verification supports SHA-1, SHA-256, and SHA-384 when using the SHA FIT library (R20AN0157JJ0104).

Please refer to the user's manual (R20UW0115JJ0200) stored in the package.

1.3 API Function

RSA Library for the RX supports the following functions.

For details on each API function, please refer to the user's manual (R20UW0115JJ0200).

Table 1-1 RSA Library API Function

API	Outline
R_rsa_signature_generate_pkcs	RSA Signature Generation (RSASSA-PKCS1-V1_5)
R_rsa_signature_verify_pkcs	RSA Signature Verification (RSASSA-PKCS1-V1_5)
R_rsa_mod_exp	Modular Exponentiation

1.4 Version Information

In the RSA Library, the version information is stored as a character string in the R_rsa_version variable. This variable can be accessed by the following extern declaration. In addition, the data stored in the product's library is as follows.

extern const char R_rsa_version[];

1.5 The Structure of RSA FIT Library

1.5.1 Application Note Structure

This product includes the files listed in Table 1-2 Structure of Product Files below.

Table 1-2 Structure of Product Files

File / Directory(bold) Names	Description
r20an0292jj0104-rx-rsa.pdf	RSA FIT Library Application Note (Japanese)
r20an0292ej0104-rx-rsa.pdf	RSA FIT Library Application Note (English)
r20uw0115jj0200-rsa.pdf	RSA FIT Library User's manual (Japanese)
r20uw0115ej0200-rsa.pdf	RSA FIT Library User's manual (English)
FITDemos	FIT Module Demo Program
rsa_demo_65n_2m.zip	RSA FIT Module Demo Program
FITModules	FIT Module folder
r_rsa_rx_v1.04.zip	RSA FIT Module
r_rsa_rx_v1.04.xml	RSA FIT Module XML file
r_rsa_rx_v1.04_extend.mdf	RSA FIT Module MDF file

1.5.2 File Structure

The folder to which the content of r_rsa_rx_v1.04.zip is extracted will contain the files listed in Table 1-3 File Structurebelow.

Table 1-3 File Structure

File / Directory(bold) Names	Description
r_rsa_rx	FIT Module folder
doc	Document folder
en	Document folder (English)
r20an0292ej0104-rx-rsa.pdf	RSA FIT Library Application Note (English)
r20uw0115ej0200-rsa.pdf	RSA FIT Library User's manual (English)
ja	Document folder (Japanese)
r20an0292jj0104-rx-rsa.pdf	RSA FIT Library Application Note (Japanese)
r20uw0115jj0200-rsa.pdf	RSA FIT Library User's manual (Japanese)
ref	Reference folder
r_rsa_config_reference.h	Configure reference file
src	Source code folder
rsa_api.c	RSA API function
mc_lib.c	Multi-byte length arithmetic function
mc_lib.h	Multibyte length arithmetic function header file
rsa_internal_header.h	RSA FIT Library Internal header file for RSA library
r_rsa_version.c	RSA FIT Library version file
r_sample_rsa_if.c	User definition functions(Signature/Authentication)
r_mw_version.h	Version data header file
r_stdint.h	typedef header file
r_rsa_rx_if.h	RSA library header file
readme.txt	Readme file
r_config	Config file folder
r_rsa_config.h	Config file (default)

2. API Information

2.1 Hardware Requirements

There are no hardware requirements.

2.2 Software Requirements

There are no software requirements.

2.3 Limitations

This library can be used only with the microcomputer option fint_register = 0 (high-speed interrupt dedicated register [none]). The default interpretation for this option is fint_register = 0.

2.4 Supported Toolchain

This driver has been confirmed to work with the toolchain listed in “4.1 Confirmed Operation Environment”.

2.5 Header Files

All API calls and their supporting interface definitions are in r_rsa_rx_if.h.

2.6 Integer Types

This project uses ANSI C99. These types are defined in stdint.h.

2.7 RSA Library ROM / RAM / Stack Size / Performance

The various sizes and processing cycles when building with the following optimization options are described for reference.

CCRX : Level2 performs whole module optimization

GCC : -O2

IAR : High (size)

2.7.1 ROM/RAM Size

library name	Little/Big Endian	ROM size [byte]			RAM size [byte] [Note]		
		CCRX	GCC	IAR	CCRX	GCC	IAR
RSA library	Little	2913	3634	2133	0	0	0

Note 1: At least, one R_RSA_WORK_t and one R_RSA_KEY_t and two R_RSA_BYTEDATA_t variables are needed for work.

Note 2: Since the API functions use the functions defined in mc_lib.c, the sum of the ROM sizes of the two files is required.

Each structures size is below.

Structure	Little/Big Endian	Memory for one structure variable [byte]		
		CCRX	GCC	IAR
R_RSA_WORK_t	Little/Big	3680	3680	3680
R_RSA_BYTEDATA_t	Little/Big	8	8	8
R_RSA_KEY_t	Little/Big	16	16	16

2.7.2 Stack Size

API	Little/Big Endian	stack size [byte] [Note]		
		CCRX	GCC	IAR
R_rsa_signature_generate_pkcs	Little/Big	40	44	28
R_rsa_signature_verify_pkcs	Little/Big	44	44	28
R_rsa_mod_exp	Little/Big	52	52	48

Note: This value is sample program stack size. If use changes the user definition function, stack size will be changed.

2.7.3 Performance

The performance of RSA library.

The measurement condition is CC-RX and optimization level 2.

API	Little/Big Endian	Performance (Cycle)		
		SHA-1	SHA-256	SHA-384
R_rsa_signature_generate_pkcs	Little	492527004	492517210	492536410
	Big	503468244	503475786	503472902
R_rsa_signature_verify_pkcs	Little	2926278	2925734	2934712
	Big	3005624	3005454	3016348
R_rsa_mod_exp	Little	2915646		
	Big	2996680		

Note: This value is sample program stack size. If use changes the user definition function, stack size will be changed.

2.8 Adding the FIT Module to Your Project

This module must be added to each project in which it is used. Renesas recommends the method using the Smart Configurator described in (1) or (3) below. However, the Smart Configurator only supports some RX devices. Please use the methods of (2) or (4) for RX devices that are not supported by the Smart Configurator.

(1) Adding the FIT module to your project using the Smart Configurator in e2 studio

By using the Smart Configurator in e2 studio, the FIT module is automatically added to your project. Refer to “Renesas e2 studio Smart Configurator User Guide (R20AN0451)” for details.

(2) Adding the FIT module to your project using the FIT Configurator in e2 studio

By using the FIT Configurator in e2 studio, the FIT module is automatically added to your project. Refer to “Adding Firmware Integration Technology Modules to Projects (R01AN1723)” for details.

(3) Adding the FIT module to your project using the Smart Configurator in CS+

By using the Smart Configurator Standalone version in CS+, the FIT module is automatically added to your project. Refer to “Renesas e2 studio Smart Configurator User Guide (R20AN0451)” for details.

(4) Adding the FIT module to your project in CS+

In CS+, please manually add the FIT module to your project. Refer to “Adding Firmware Integration Technology Modules to CS+ Projects (R01AN1826)” for details.

3. Demo project

The demo project is a stand-alone program. The demo projects include function main() that utilizes the FIT module and its dependent modules (e.g. r_bsp). This FIT module includes the following demo projects.

3.1 rsa_demo_65n_2m

rsa_demo_65n_2m shows how to use the RSA library API. This demo project will perform exponentiation, RSA signature generation and signature verification (RSASSA-PKCS1v1_5).

3.2 Add the Demo to Workspace

The demo projects are found in the FITDemos subdirectory of the distribution file for this application note. To add a demo project to a workspace,

- Select "File" -> "Import".
- In the "Import" dialog, select "Existing Project to Workspace" under "General" and click the "Next" button.
- In the "Import" dialog, select the "Select archive file" radio button.
- Click the "Browse" button to open the FITDemos subdirectory.
- Select the desired demo zip file, then click “Finish”.

The above process will add the demo project to the workspace.

4. Appendix

4.1 Confirmed Operation Environment

This section describes confirmed operation environment for the RSA FIT Library.

Table 4-1 Confirmed Operation Environment (Rev. 1.04)

Item	Contents
Integrated Development Environment	Renesas Electronics e2 studio Version 2022-01 IAR Embedded Workbench for Renesas RX 4.20.3
C compiler	Renesas Electronics C/C++ Compiler Package for RX Family V3.04.00 Compiler option: The following option is added to the default settings of the integrated development environment. -lang = c99
	GCC for Renesas RX 8.3.0.202104 Compiler option: The following option is added to the default settings of the integrated development environment. -std=gnu99 Linker option: The following user defined option should be added to the default settings of the integrated development environment, if “Optimize size (-Os)” is used: -Wl,--no-gc-sections This is to work around a GCC linker issue whereby the linker erroneously discards interrupt functions declared in FIT peripheral module
	IAR C/C++ Compiler for Renesas RX version 4.20.3 Compiler option: The default settings of the integrated development environment
Endian	Big endian/little endian
Revision of the module	Rev.1.04
Board used	Target Board for RX65N Target Board for RX130 Renesas Envision Kit for RX72N

5. Reference documents

Related Technical Updates

This module reflects the content of the following technical updates.

None

Website and Support

Renesas Electronics Website
http://www.renesas.com/

Inquiries
http://www.renesas.com/contact/

Revision History

Rev.	Date	Description	
		Page	Summary
1.04	2022.10.31	-	Updated the confirmed operation environment
1.03	2022.08.10	-	With the fixed of FIT, the title was corrected, and FIT-related information was added. The library format has been changed from Lib. format to C source. RSAES-PKCS1-V1_5 is no longer supported. Accordingly, R_rsa_encrypt_pkcs and R_rsa_decrypt_pkcs APIs have been removed.
1.00	2014.03.31	-	First edition issued

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/.

© 2022 Renesas Electronics Corporation. All rights reserved.