# RL78 Family

## RSA Library: Introduction Guide

### Introduction

This document explains RSA Library for RL78 Family (hereafter referred to as "RSA Library") that depends on MCUs. The RSA Library is the software library incorporated in the RL78 Family and includes the data encryption/decryption functions that use the RSA encryption technology. Also it is designed in dedicated algorithm and fully-tuned up by assembly language.

Please refer to each User's Manual to know how to use RSA Library software library.

### Target Device

RL78/G14, RL78/G23

When using this application note with other Renesas MCUs, careful evaluation is recommended after making modifications to comply with the alternate MCU.

### Contents

# 1. Structure of product

This product includes the following data.

**Table 1 RSA Library product files(1)**

| Name | Description |
|---|---|
| sample program(r20an0326xx0201-rl78-rsa) | |
| workspace <DIR> | |
| Document (doc) <DIR> | |
| English (en) | |
| r20uw0115ej0200-rsa.pdf | User's manual |
| r20an0326ej0201-rl78-rsa.pdf | Introduction Guide (this document) |
| Japanese (ja) | |
| r20uw0115jj0200-rsa.pdf | User's manual |
| r20an0326jj0201-rl78-rsa.pdf | Introduction Guide |
| libsrc <DIR> | Driver storage folder |
| rsa <DIR> | RSA Library |
| src <DIR> | RSA Library source |
| 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 | Internal header file for RSA library |
| r_rsa_version.c | version file |
| include <DIR> | RSA library header |
| r_rsa.h | RSA library header file |
| r_mw_version.h | Version data header file |
| r_stdint.h | typedef header file |

**Table 2 RSA Library product files(2)**

| Name | Description |
|---|---|
| sample program (r20an0326xx0201-rl78-rsa) | |
| workspace <DIR> | |
| CS+ <DIR> | CS+ project folder |
| rsa_rl78_sim_sample <DIR> | G23 sample project folder |
| src <DIR> | program storage folder |
| main.c | sample main |
| main.h | sample main header |
| r_sample_key.c | sample RSA key |
| r_sample_key.h | sample RSA key header |
| r_sample_modexp.c | sample Modular exponentiation |
| r_sample_modexp.h | sample Modular exponentiation header |
| r_sample_rsa_if.c | sample User Definition |
| r_sample_rsa_if.h | sample User Definition header |
| r_sample_sig_gen_vrfy.c | sample RSASSA-PKCS1-V1_5 |
| r_sample_sig_gen_vrfy.h | sample RSASSA-PKCS1-V1_5 header |
| libsrc <DIR> | link to libsrc |
| smc_gen <DIR> | Smart configurator auto-generated folder |
| general | Common header file / source file storage folder |
| r_bsp | Initialization code register definition storage folder |
| r_config | Driver initialization config header storage folder |
| e$^2$ studio <DIR> | e$^2$ studio project folder |
| CCRL | sample project for CCRL |
| rsa_rl78_sim_sample <DIR> | sample project for G23 |
| LLVM | sample project for LLVM |
| rsa_rl78_sim_sample <DIR> | sample project for G23 |
| IAR | IAR project folder |
| rsa_rl78_sim_sample <DIR> | sample project for G23 |

# 2. Product Specifications

## 2.1 API Function

RSA Library supports the following functions.

**Table 3 Library Functions (API)**

| 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 |

# 3. CC-RL

## 3.1 Development environment

Please use the same or a later version of the toolchain listed below:

- Integrated Development Environment:
  CS+ for CC V8.05.00
  e$^2$ studio 2021-04 (21.4.0)
- C compiler:
  CC-RL V1.09.00

## 3.2 ROM / RAM / Stack size / Performance

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

Compiler options

-cpu=S3 -memory_model=medium –Odefault

Link options

-NOOPtimize

**Table 4 ROM, RAM size**

| library file name | ROM size [byte] (Notes 1) | RAM size [byte] (Notes 2) |
|---|---|---|
| rsa_api.c | 1,310 | 0 |
| mc_lib.c | 2,728 | |

Notes 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..
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 are below.

**Table 5 Memory for Structure Variable**

| Structure | Memory for one structure variable [byte] |
|---|---|
| R_RSA_WORK_t | 3680 |
| R_RSA_BYTEDATA_t | 4 |
| R_RSA_KEY_t | 8 |

**Table 6 Stack Size**

| API | stack size [byte] (Notes 1) |
|---|---|
| R_rsa_signature_generate_pkcs | 144 |
| R_rsa_signature_verify_pkcs | 144 |
| R_rsa_mod_exp | 124 |

Notes 1 This value is sample program stack size. If use changes the user definition function, stack size will be changed.

## 3.3 Performance

**Table 7 RSA Library Performance**

| Function | Key Type | Processing Time [second] RL78/G23@32MHz (Note1) |
|---|---|---|
| R_rsa_signature_generate_pkcs (Note2) | Private Key | About 184.82(Note3) |
| R_rsa_signature_verify_pkcs (Note2) | Public Key | About 1.07 |
| R_rsa_mod_exp | Public Key | About 1.07 |

Note1: This is the value when the sample program using the 2048-bit key is executed. The number of cycles changes when the user changes the key data or changes the implementation of the user-defined function.

2: User function R_rsa_if_hash() returns the fixed values in sample program. If add the hash calculate function, processing time is added to the above time.

3: If the watchdog timer is enabled, a reset may occur due to a timeout, so check the settings.

# 4. IAR Embedded Workbench

## 4.1 Development environment

Please use the same or a later version of the toolchain listed below:

- Integrated Development Environment:
  IAR Embedded Workbench for Renesas RL78 version 4.21.1

- C compiler:
  IAR C/C++ Compiler for Renesas RL78 : 4.20.1.2260 (4.20.1.2260)

## 4.2 ROM / RAM / Stack Size / Performance

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

Compiler options

--core=S3 --code_model=far --data_model=near --near_const_location=rom0 -e -Oh

--calling_convention=v2

**Table 8 ROM, RAM size**

| library file name | ROM size [byte] (Notes 1) | RAM size [byte] (Notes 2) |
|---|---|---|
| rsa_api.c | 1,352 | 0 |
| mc_lib.c | 2,629 | 0 |

Notes 1 RSA needs 276 bytes (max) for mirror area.
In case, user does not use version information or, user uses large model, the memory size for mirror area requires 144 bytes.
2 At least, one R_RSA_WORK_t and one R_RSA_KEY_t and two R_RSA_BYTEDATA_t variables are needed for work.

Each structures size are below.

**Table 9 Memory for Structure Variable**

| Structure | Memory for one structure variable [byte] |
|---|---|
| R_RSA_WORK_t | 920 |
| R_RSA_BYTEDATA_t | 4 |
| R_RSA_KEY_t | 8 |

**Table 10 Stack Size**

| API | stack size [byte] (Notes 1) (Notes 2) |
|---|---|
| R_rsa_signature_generate_pkcs | 152 |
| R_rsa_signature_verify_pkcs | 152 |
| R_rsa_mod_exp | 132 |

Notes 1 stack size is same in all libraries.
2 This value is sample program stack size. If use changes the user definition function, stack size will be changed.

## 4.3 Performance

**Table 11 RSA Library Performance**

| Function | Key Type | Processing Time [second] RL78/G23@32MHz (Note1) |
|---|---|---|
| R_rsa_signature_generate_pkcs | Private Key | About 336.828 (Note2) |
| R_rsa_signature_verify_pkcs | Public Key | About 1.98 |
| R_rsa_mod_exp | Public Key | About 1.98 |

Note1: This is the value when the sample program is executed. The number of cycles changes when the user changes the key data or changes the implementation of the user-defined function.

2: If the watchdog timer is enabled, a reset may occur due to a timeout, so check the settings.

# 5. LLVM

## 5.1 Development environment

Please use the same or a later version of the toolchain listed below:

- Integrated Development Environment:
  e$^2$ studio 2022-01 (22.1.0)

- C compiler:
  LLVM for Renesas RL78 10.0.0.202203

## 5.2 ROM / RAM / Stack size / Performance

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

Compiler options

CPU Type : S3-core

Optimization Level : Optimize size (-Os)

**Table 12 ROM, RAM size**

| library file name | ROM size [byte] (Notes 1) | RAM size [byte] (Notes 2) |
|---|---|---|
| rsa_api.c | 1,543 | 0 |
| mc_lib.c | 3,068 | |

Notes 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..
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 are below.

**Table 13 Memory for Structure Variable**

| Structure | Memory for one structure variable [byte] |
|---|---|
| R_RSA_WORK_t | 3680 |
| R_RSA_BYTEDATA_t | 4 |
| R_RSA_KEY_t | 8 |

**Table 14 Stack Size**

| API | stack size [byte] (Notes 1) |
|---|---|
| R_rsa_signature_generate_pkcs | 132 |
| R_rsa_signature_verify_pkcs | 132 |
| R_rsa_mod_exp | 112 |

Notes 1 This value is sample program stack size. If use changes the user definition function, stack size will be changed.

## 5.3 Performance

**Table 15 RSA Library Performance**

| Function | Key Type | Processing Time [second] RL78/G23@32MHz (Note1) |
|---|---|---|
| R_rsa_signature_generate_pkcs (Note2) | Private Key | About 418(Note3) |
| R_rsa_signature_verify_pkcs (Note2) | Public Key | About 2.4 |
| R_rsa_mod_exp | Public Key | About 2.4 |

Note1: This is the value when the sample program using the 2048-bit key is executed. The number of cycles changes when the user changes the key data or changes the implementation of the user-defined function.

2: User function R_rsa_if_hash() returns the fixed values in sample program. If add the hash calculate function, processing time is added to the above time.

3: If the watchdog timer is enabled, a reset may occur due to a timeout, so check the settings.

## Website and Support

Renesas Electronics Website

http://www.renesas.com/

Inquiries

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

## Revision History

| | | Description | |
|---|---|---|---|
| **Rev.** | **Date** | **Page** | **Summary** |
| 1.00 | Sep 01, 2016 | — | First edition issued |
| 1.01 | Sep 10, 2018 | — | Added chapter 4 CS+ for CC. |
| 1.02 | Nov 12, 2018 | — | Added chapter 5 IAR Embedded Workbench |
| 2.00 | Apr 21, 2021 | — | Changed the library provision form from Lib. Format to C source<br>Delete CS + for CA |
| 2.01 | Jun 30, 2022 | — | Supported LLVM. |

# 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/.