RZ/G Series Security Solution V1.1.1

Release Notes

R01TU0258EJ0101
Rev.1.01
2019.4.25

Table of Contents

1. Overview

This release note describes the contents, how to apply and important point of the RZ/G Series Security Solution to customers.

The Version of RZ/G Series Security Solution covered by this release note is shown below.

No.	Name	Version
1	RZ/G Series Security Solution	V1.1.1

This RZ/G Series Security Solution runs on Verified Linux Package (VLP) or equivalent one*. Target Version of VLP are below.

Target Device	Name	Version
RZ/G1M-PF	RZ/G Verified Linux Package	V2.1.0, V2.1.1
RZ/G1E-PF	RZ/G Verified Linux Package	V2.1.0, V2.1.1
RZ/G1C-PF	RZ/G Verified Linux Package	V2.1.0, V2.1.1
RZ/G1N-PF	RZ/G Verified Linux Package	V2.1.0, V2.1.1

note* : About VLP equivalent Linux, please refer to RZ/G Yocto recipe Start-Up Guide which is obtained from Renesas Market Place site.

VLP is obtained from Renesas Market Place site.

1.1 Outline of RZ/G Security Solution

Renesas provides a security solution for RZ/G series products. This security solution provides the following functions to protect user products connected with the network in the age of the Internet of things (IoT).

Table 1-1 Functions of the Security Solution

Function	**Description**
Encrypted kernel booting	The kernel in the non-volatile memory is encrypted to prevent illegal copying of software. Detection of tampering or the illegal copying is enable at the booting up.
Encrypted communications	Secure communications are enable by mutual authentication between the product and server (SSL/TLS).
Secure storage	Data are encrypted and decrypted by device-specific key. By device-specific key, only the product in which encrypted the data can decrypt the data.
Secure software updates	The key and Linux kernel used in encrypted kernel booting are updated safely.
Basic cryptographic functions	The basic functions of encryption/decryption provided. (See Table 1-2.)

Table 1-2 Cryptographic Functionality Provided within the Security Solution

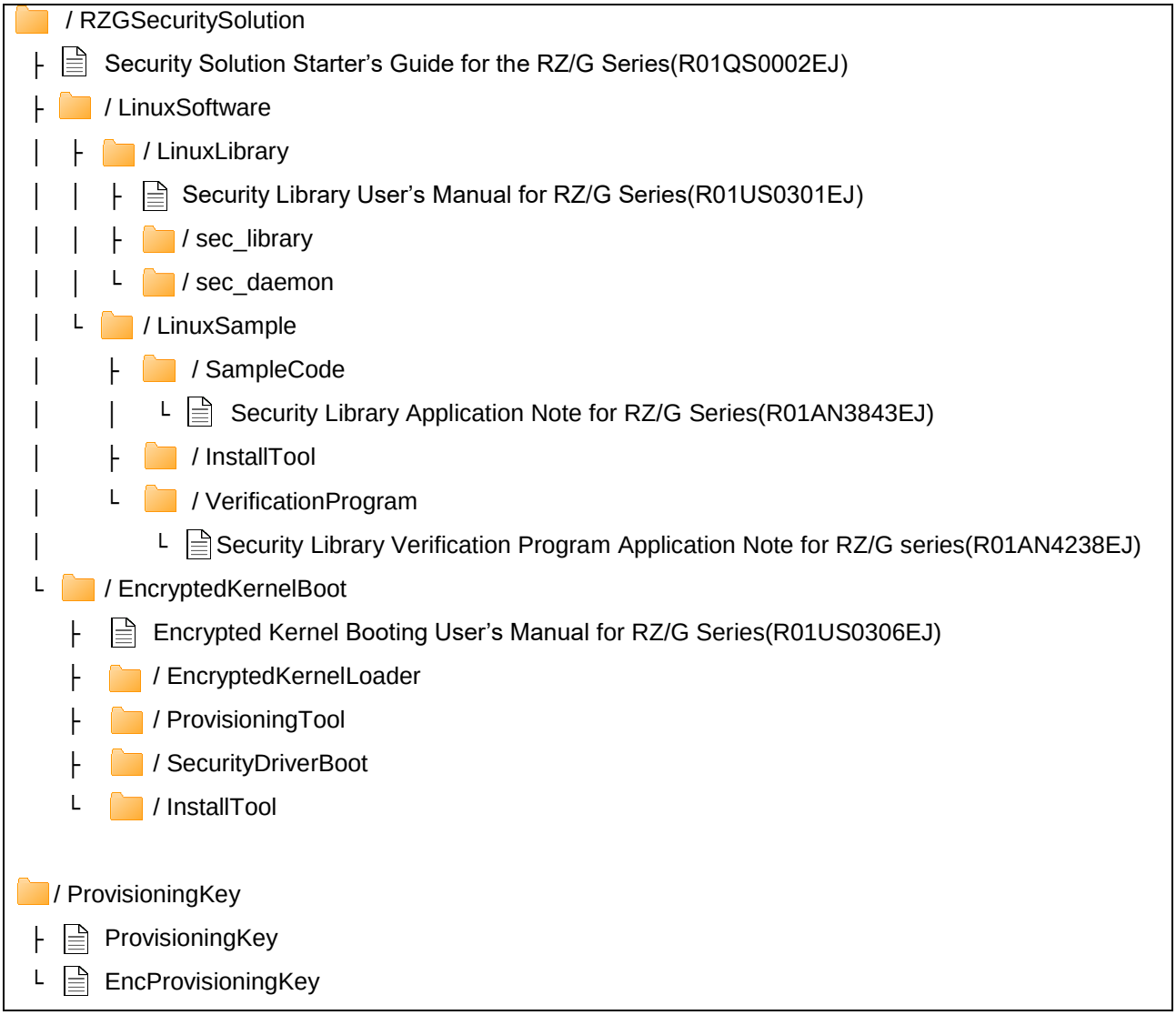
Encryption	**Algorithm**
Symmetric cryptography	AES algorithm in CBC mode (128 or 256 bits)
Asymmetric cryptography	RSA (1024 or 2048 bits)
Hashing algorithm	SHA-1 or SHA-256
MAC	HMAC (SHA-1 or SHA-256) CMAC (AES-128 or AES-256)

2. Release Items

This section describes the items provided by Renesas as the RZ/G security solution.

2.1 Configuration of Files for Items Provided by Renesas

The configuration of files for items provided by Renesas is given below. Key data (ProvisioningKey) for the provisioning Process (initialize RZ/G security solution) are provided as other package by Renesas.



2.2 Detailed Descriptions of Items Provided by Renesas

This section describes the details of the items provided by Renesas.

Table 2-1 Details of Items Provided by Renesas (1 of 2)

Item	Ver	Description
Security solution starter's guide for the RZ/G series (R01QS0002EJ)	1.10	This is the guide to starting to use the RZ/G security solution.
LinuxSoftware	-	A set of software required to run the RZ/G security functions in a Linux environment and related documents.
LinuxLibrary	-	Linux library for RZ/G security.
Security library user's manual for the RZ/G series (R01US0301EJ)	1.11	The manual describes the user interface for RZ/G security.
sec_library	1.1.1	Security library files which provide interface with application are stored in this folder.
sec_daemon	1.1.1	Security daemon*2 file which handles requests from application is stored in this folder. Security daemon includes Security Driver *1.
LinuxSample	-	This folder contains Linux samples that are helpful for using RZ/G security.
SampleCode	1.10	The sample code is used to confirm the operation of each function of the RZ/G security.
Security library application note for the RZ/G series (R01AN3843EJ)	1.10	The application note describes the procedure for executing the sample code.
InstallTool	1.10	Install Tool (source code) This folder contains sample code of tool that is used to write the keyring data and Linux kernel required in booting of the encrypted kernel to the non-volatile memory on an RZ/G development board. It is provided as an application program which runs in a Linux environment on iWave RZ/G development kit.
VerificationProgram	1.11	Verification Program This folder contains sample source code of verification program and binary for verification tool. It is used to verify user program using RZ/G security library.
Security library verification program application note for the RZ/G series(R01AN4238EJ)	1.10	This application note describes the procedure for applying the verification program to software that uses security library.

Table 2-2 Details of Items Provided by Renesas (2 of 2)

Item	Ver	Description
EncryptedKernelBoot	-	This folder contains software and documents used in booting of the encrypted kernel, which enables the RZ/G security functions.
Encrypted Kernel Booting User's Manual for RZ/G Series(R01US0306EJ)	1.10	The manual describes outline of the encrypted kernel booting and processing of encrypted kernel loader. It also includes a description of the driver for boot used by encrypted kernel loader.
EncryptedKernelLoader	1.10	Encrypted Kernel Loader Boot loader used in booting the encrypted kernel
ProvisioningTool	1.60	Provisioning Tool This tool is for use in the Provisioning Process. This tool is for generating various key data, keyring data, and Linux kernel for encrypted kernel booting. This tool is provided as application programs that run under Windows.
SecurityDriverBoot	*1	Security Driver for Boot (Binary) This folder contains binary of Security Driver for Boot that is used in encrypted kernel loader and ROM Writer.
InstallTool	1.10	Install Tool (Binary) This folder contains binary of ROM Writer that is used to write the keyring data and Linux Kernel required in booting of the encrypted kernel to the non-volatile memory on an RZ/G development board.
ProvisioningKey	-	Key data The key is for use in provisioning. Renesas provides a specific key for each customer.
Provisioning Key	-	Provisioning Key The key for protecting the keyring for use in provisioning.
EncProvisioning Key	-	Provisioning key data used to write to a product This is the converted provisioning key data to write to the ROM of a product.

note*1: Security Driver Version is shown below.

Target Device	Security Driver Version
RZ/G1M-PF	1.2.00
RZ/G1E-PF	1.2.00
RZ/G1C-PF	1.2.00
RZ/G1N-PF	1.2.00

note*2: Security Daemon uses LibreSSL 2.5.4.

3. How to Apply

Please refer to RZ/G series Security Solution Starter's Guide(R01QS0002EJ) on how to apply this package.

4. Additional Functions and change functions from previous edition

The main additions and changes in this edition are listed below.

- Security Library/Security Daemon
  SEC_ContentsDataMakeVerifyCode, SEC_ContentsDataVerify,
  Changes hash and MAC calculation method.

- Provisioning Tool
  Changes calculation method of injection for HMAC-SHA1-Key.

- Verification Program
  Changes temporarily encrypted keys included in samples.

5. Restrictions

None.

6. Note

None.

7. Open Source Licenses

Security Solution for RZ/G Series uses LibreSSL.

```
   LibReSSL files are retained under the copyright of the authors. New
   additions are ISC licensed as per OpenBSD's normal licensing policy,
   or are placed in the public domain.

   The OpenSSL code is distributed under the terms of the original OpenSSL
   licenses which follow:

   LICENSE ISSUES
   ==============

   The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
   the OpenSSL License and the original SSLeay license apply to the toolkit.
   See below for the actual license texts.  In case of any license issues
   related to OpenSSL please contact openssl-core@openssl.org.

   OpenSSL License
   ---------------

 /* ====================================================================
  * Copyright (c) 1998-2011 The OpenSSL Project.  All rights reserved.
  *
  * Redistribution and use in source and binary forms, with or without
  * modification, are permitted provided that the following conditions
  * are met:
  *
  * 1. Redistributions of source code must retain the above copyright
  *    notice, this list of conditions and the following disclaimer.
  *
  * 2. Redistributions in binary form must reproduce the above copyright
  *    notice, this list of conditions and the following disclaimer in
  *    the documentation and/or other materials provided with the
  *    distribution.
  *
  * 3. All advertising materials mentioning features or use of this
  *    software must display the following acknowledgment:
  *    "This product includes software developed by the OpenSSL Project
  *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
  *
  * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
  *    endorse or promote products derived from this software without
  *    prior written permission. For written permission, please contact
  *    openssl-core@openssl.org.
  *
  * 5. Products derived from this software may not be called "OpenSSL"
  *    nor may "OpenSSL" appear in their names without prior written
  *    permission of the OpenSSL Project.
  *
  * 6. Redistributions of any form whatsoever must retain the following
  *    acknowledgment:
  *    "This product includes software developed by the OpenSSL Project
  *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
  *
  * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
  * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
  * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
  * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
  * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
  * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
  * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
  * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
  * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
  * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
  * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
  * OF THE POSSIBILITY OF SUCH DAMAGE.
  * ====================================================================
  *
```

```
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

 Original SSLeay License
 -----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	2018.12.12	-	(new issued)
1.01	2019.4.25	2	Add support for VLP V2.1.1

Website and Support

Renesas Electronics Website

http://www.renesas.com/

Inquiries

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