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	V1.0.1

RZ/G Series Security Solution V1.0.1 runs on Verified Linux Package (VLP) or equivalent one*. Target Version of VLP are below.

No.	Name	Version
1	RZ/G Verified Linux Package	V2.0.3

note* : 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. Also, it is available on RZ/G Cloud Development Environment Service.

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. User products are also protected by the detection of tampering or the illegal copying of software at the time of booting up.
Encrypted communications	Mutual authentication between the product and server proceeds and support for SSL/TLS enables secure communications.
Secure storage	Data are encrypted and decrypted by using keys that are specific to products. Individual keys are generated for each product, so only the product in which the encryption was applied is capable of decrypting the data.
Secure software updates	This function safely updates the key data and Linux kernel data used in booting of the encrypted kernel.
Basic cryptographic functions	The basic cryptographic functionality is provided as an API. The cryptographic functionality provided within the security solution is shown in Table 1-2 below.

Table 1-2 Cryptographic Functionality Provided within the Security Solution

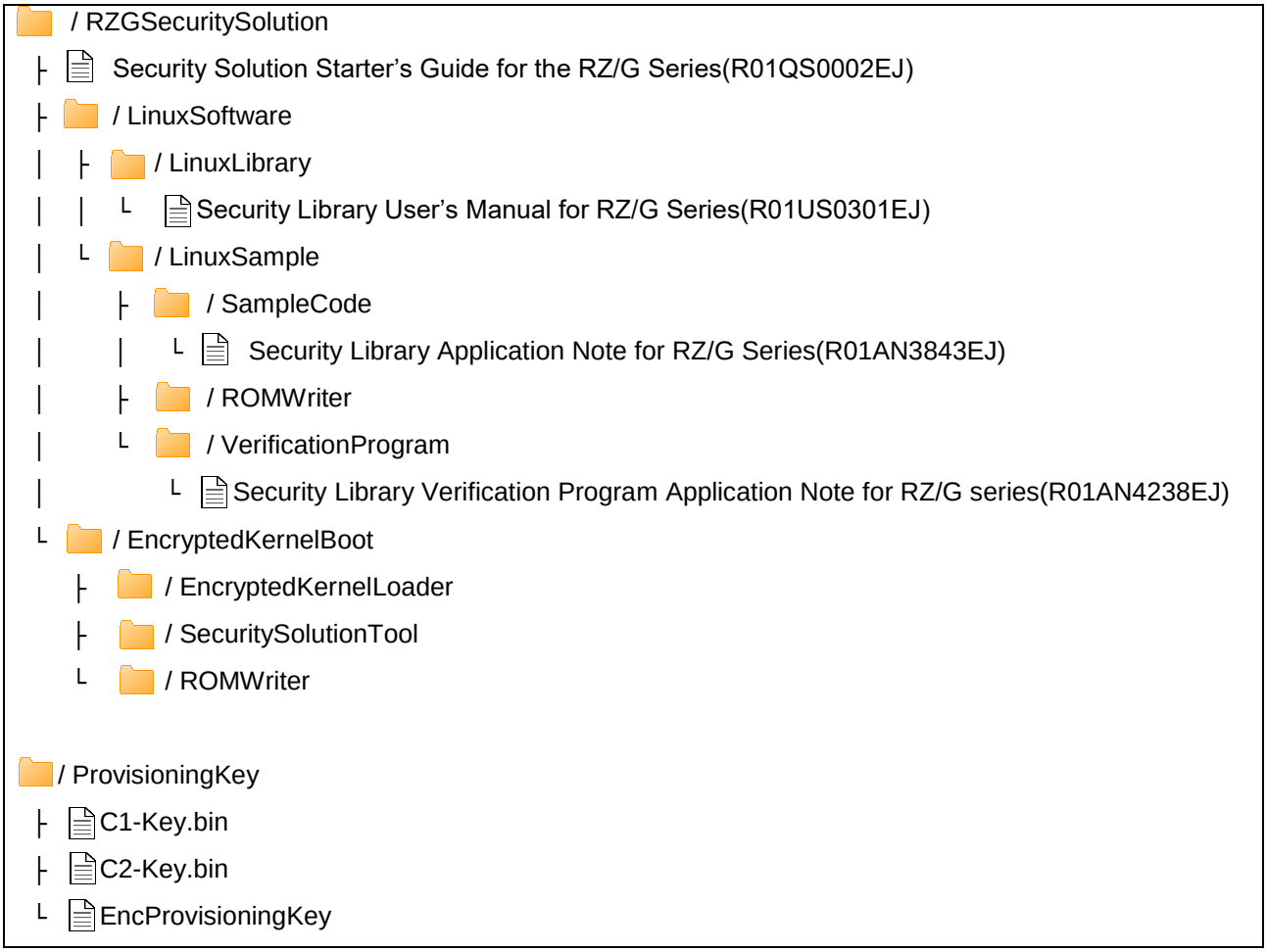
Encryption	**Algorithm**
Symmetric cryptography	AES algorithm in CBC mode (128 or 256 bits)
Asymmetric cryptography	RSA (1024 or 2048 bits)
Hashing algorithm	SHA-1 or SHA-256
MAC	HMAC (SHA-1 or SHA-256) CMAC (AES-128 or AES-256)

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)	1.02	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)	1.02	The manual describes the user interface for RZ/G security.
sec_library	1.0.0	Security library files which provide interface with application are stored in this folder.
sec_daemon	1.0.0	Security daemon file which handles requests from application is stored in this folder.
LinuxSample	-	This folder contains Linux samples that are helpful for using RZ/G security.
SampleCode	1.0.2	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)	1.0.2	The application note describes the procedure for executing the sample code.
ROMWriter	1.02	ROM Writer (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's RZ/G development board.
VerificationProgram	1.00	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)	1.00	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.
EncryptedKernelLoader	1.01	Boot loader used in booting the encrypted kernel
SecuritySolutionTool	1.41	This tool is for use in the RZ/G Security Solution. 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.
ROMWriter	1.02	ROM Writer (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 (C1-Key.bin, C2-Key.bin)	-	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.

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.

- Adds the support of RZ/G1E-PF (R8A77450HA02BG)

- Security Library
  Adds the support of SHA-1 with RSA-PKCS1-v1.5 in signature verification algorithm for TLS
  Adds the support of up to 3 tiers in server and client certificate hierarchy
  Changes size of buffer where version number is stored by SEC_GetPackageVersion()

- Sample Code
  Adds encrypted communication sample program
  Adds secure software update sample program

- ROM Writer
  Adds ROM Writer (Tool for writing to the non-volatile memory device) sample code

- Verification Program
  Adds verification program sample code.

5. Restrictions

None.

6. Note

None.