RZ/G2 Trusted Execution Environment

Start-Up Guide

Introduction

This document explains the outline RZ/G2 Trusted Execution Environment (hereinafter referred to as “TEE for RZ/G2”) and how to build TEE for RZ/G2 on the evaluation board with RZ/G2 Linux BSP.

The build instructions in this document assume that the build of RZ/G2 Linux BSP has been executed using Yocto build environment in advance. Please refer to "Linux Interface Specification Yocto recipe Start-Up Guide" for the build procedure using Yocto build environment for RZ/G2 Group.

Target Device

RZ/G2E

RZ/G2M

RZ/G2N

RZ/G2H

Table of Contents

1. Overview

TEE for RZ/G2 consists of ARM TrustZone and OP-TEE (Open Portable Trusted Execution Environment).

- TrustZone is a security function provided by ARM processor. It provides system-wide hardware isolation for trusted software by creating an isolated secure world.
- OP-TEE is open source to provide an independent environment isolated from the underlying hardware. It is implemented using TrustZone to protect the environment for executing trusted applications. OP-TEE consists of multiple components such as OP-TEE OS, OP-TEE Driver and OP-TEE Client.

1.1 Components

Figure 2-1 shows the software components of TEE for RZ/G2.

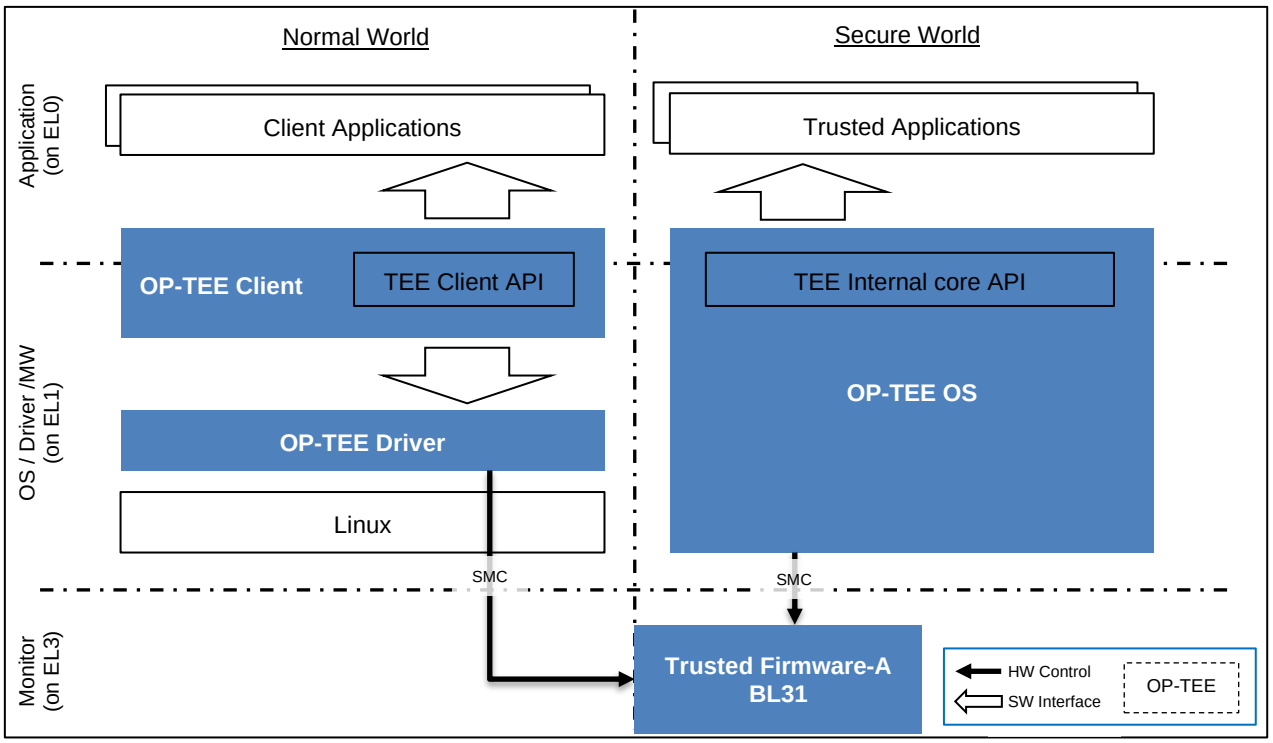

Figure 2-1 Software Components

(a) Trusted Firmware-A (BL31)

This software is ported to the RZ/G2 platform.
Trusted Firmware-A is provided by ARM and is a reference implementation of ARM interface standards such as Secure Monitor and PSCI (Power State Coordination Interface).

(b) OP-TEE OS

This software is ported to the RZ/G2 platform.
OP-TEE OS is a trusted OS that uses ARM TrustZone technology and provides the TEE internal core API defined in the global platform API for the development of trusted applications.

(c) OP-TEE Client

This software includes TEE Client Library and TEE supplicant. It contains TEE Client API defined by the GlobalPlatform TEE standard for communication with the Trusted OS.

(d) OP-TEE Driver

This software is a Linux driver. It implements a TEE driver that allows communication between Linux and OP-TEE OS.

(e) OP-TEE Test

This software is the test suite for OP-TEE. It consists of Trusted Application and Client Application. It performs basic operation checking the installed OP-TEE.

1.2 References

1.2.1 Standard Documents

The following table shows the standard documents related to TEE for RZ/G2.

Table 2-1 Standard Documents

No	Issue	Title	Edition
1	GlobalPlatform	TEE Client API Specification	1.0
2	GlobalPlatform	TEE Internal Core API Specification	1.1

1.2.2 Related Document

The following table shows the documents related to TEE for RZ/G2.

Table 2-2 Related Documents

No	Issue	Title	Edition
1	Renesas Electronics	Linux Interface Specification Yocto recipe Start-Up Guide	1.08
2	Renesas Electronics	RZ/G2 Reference Boards Start-up Guide	1.07
3	Renesas Electronics	RZ/G Series, 2nd Generation User's Manual: Hardware LSIs for Rich Graphics Applications	1.01
4	Renesas Electronics	RZ/G Series, 2nd Generation User's Manual: Hardware Additional Document for Security	1.00
5	Renesas Electronics	RZ/G2 Trusted Execution Environment Porting Guide	1.00

1.2.3 Related Original Software

The following table shows the original software related to TEE for RZ/G2.

Table 2-3 Related Original Software

No	Software	Title and URL	Edition
1	Trusted Firmware-A	Secure Monitor https://github.com/ARM-software/arm-trusted-firmware	2.4
2	OP-TEE OS	Trusted side of the TEE https://github.com/OP-TEE/optee_os	3.12.0
3	OP-TEE Driver	Normal World driver https://git.kernel.org/pub/scm/linux/kernel/git/cip/linux-cip.git Branch: linux-4.19.y-cip Source Directory: drivers/tee	-
4	OP-TEE Client	Normal World Client side of the TEE https://github.com/OP-TEE/optee_client	3.12.0
5	OP-TEE Test	OP-TEE Test suite https://github.com/OP-TEE/optee_test	3.12.0
6	Security Module	RZ/G Security Module https://github.com/renesas-rz/rzg_security-module	1.00
7	Flash Writer	RZ/G2 Flash Writer https://github.com/renesas-rz/rzg2_flash_writer	1.04

1.3 Related Package

The following table shows the package related to TEE for RZ/G2.

Table 2-4 Related Package

No	Package	Explanation	Edition
1	RZ/G2 Secure IP Package	This is a package provided by Renesas and is required to implement Secure Boot. For more information, refer to "Build Instructions (Enable Secure Boot)".	1.00

1.4 Licenses

The following table shows the licenses of software related to TEE for RZ/G2.

Table 2-5 Software Licenses

No	Software		Licenses
1	Trusted Firmware-A		BSD-3-Clause
2	OP-TEE OS		BSD-2-Clause or BSD-3-Clause
3	OP-TEE Driver		GPLv2
4	OP-TEE Client		BSD-2-Clause
5	OP-TEE Test	Client Application	GPLv2
		Trusted Application	BSD-2-Clause
6	Security Module		BSD-3-Clause
7	Flash Writer		BSD-3-Clause

1.5 Terminology

The following table shows the terminology related to this guidance.

Table 1-4 Terminology

No	Term	Explanation
1	PSCI	Power State Coordination Interface. It defines a Standard Interface for power management that can be used by OS vendors for supervisory software working at different levels of privilege on an ARM device.
2	Secure World	It is one of the security states that defined ARMv8-A architecture. When in this state, the CPU can access both the Secure and Non-Secure space.
3	Normal World	It is one of the security states that defined ARMv8-A architecture. When in this state, the CPU can access only Non-Secure space.
4	SMC	Secure Monitor Call. An ARM assembler instruction that causes an exception that is taken synchronously into EL3.
5	RPMB	Replay Protected Memory Block
6	Exception Levels (EL0/EL1/EL3)	The ARMv8-A architecture defines a set of Exception levels EL0 to EL3 where: If ELn is the Exception level, increased values of n indicate increased software execution privilege. Execution at EL0 is called unprivileged execution. EL1 provides support for virtualization of Non-Secure operation. EL3 provides support for switching between to Security states, Secure state and Non-Secure state.

2. Build Environment

The recommended environment for build is the same as the RZ/G2 Linux BSP. For details, refer to “Related Document No.1”.

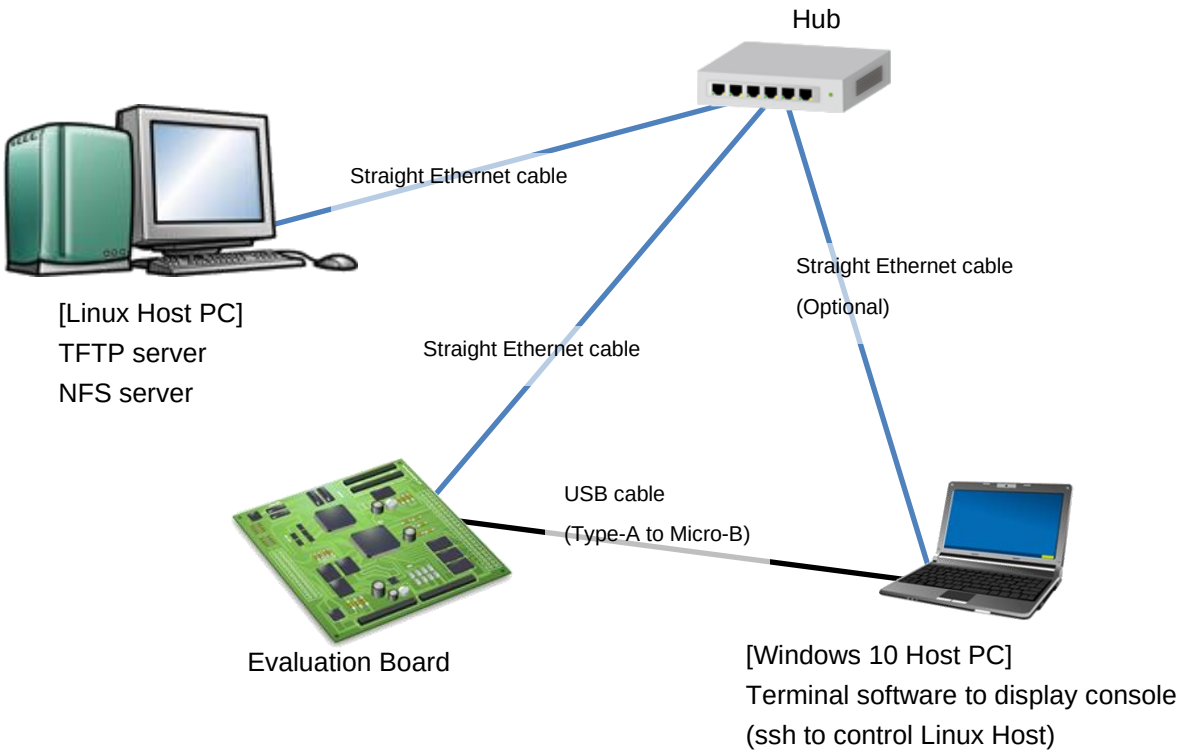

Figure 2-1 Recommended Environment

3. Build Instructions

This section explains how to build RZ/G2 Linux BSP with OP-TEE enabled.

3.1 Build Images

Step 1 Set the shell variable
Set the environment variable WORK to the directory specified in the build procedure for RZ/G2 Linux BSP.

```
$ export WORK=</home/user/user_work>
```

Note: Please replace </home/user/user_work> to the path to your Yocto Project work directory.

To perform the following steps, the Linux host PC needs access to the network. Set the "${WORK}/build/conf /local.conf" line as shown below.

```
BB_NO_NETWORK = "0"
```

Step 2 Prepare recipe files and checkout version
Please refer document “Linux Interface Specification Yocto recipe Start-Up Guide” for prepare and checkout right revision of each recipes.

Please chose right version of “meta-rzg2” as below:

```
$ cd ${WORK}/meta-rzg2
$ git checkout -b tmp2 <tag>
<tag>: please check and choose the following tag by ‘git tag’
      $ git tag
            BSP-1.0.8
```

Step 3 Add OP-TEE to environment
Please follow below instruction:

```
$ cd ${WORK}/meta-rzg2
$ vi recipes-bsp/arm-trusted-firmware/arm-trusted-firmware_git.bb
```

Add 1 more “ATFW_OPT_append” below all existed option “ATFW_OPT_append*”:

```
 …
ATFW_OPT_append += " RZG_RPC_HYPERFLASH_LOCKED=0 MBEDTLS_DIR=../mbedtls "
ATFW_OPT_append += " SPD="opteed" "
```

To add the OP-TEE only to one of the platforms, please refer to the following option.

```
ATFW_OPT_append_${soc_name} += " SPD="opteed" "
```

With ${soc_name}:

r8a774c0: EK874

r8a774a1: HiHope RZ/G2M (v1.3 and v3.0)

r8a774b1: HiHope RZ/G2N

r8a774e1: HiHope RZ/G2H

Step 4 Setup the build environment
Set environment variables for building with the “source” command.

```
$ cd $WORK
$ source poky/oe-init-build-env
```

Step 5 Build
Please build as follows.

```
$ bitbake core-image-weston
```

Note: Please refer to “Related Document No.1” for the image types supported by RZ/G2 Linux BSP.

The data file is stored in the ${WORK}/build/tmp/deploy/images/<board> directory.

3.2 Board Settings

Write RZ/G2 Linux BSP image file with TEE for RZ/G2 into flash memory on the evaluation board. Refer to “Related Document No.1” for the procedure for writing to the flash memory and setting the evaluation board.

Table 3-1 Addresses for each file

File Name	Address to load to RAM	Address to save to ROM	Description
bootparam_sa0.srec	E6320000	00000	Loader(Boot Parameter)
bl2-<board>.srec	E6304000	40000	Loader
cert_header_sa6.srec	E6320000	180000	Loader(Certification)
bl31-<board>.srec	44000000	1C0000	Trusted Firmware-A
tee-<board>.srec	44100000	200000	OP-TEE OS
u-boot-elf-<board>.srec	50000000	300000	U-Boot

Note: <board>: ek874, hihope-rzg2m, hihope-rzg2n, hihope-rzg2h.

4. Build Instructions (Enable Secure Boot)

This section explains how to build RZ/G2 Linux BSP with the Secure Boot provided by TEE for RZ/G2 enabled. For more information, please refer to "Related Document No.5".

The build procedure described in this section requires RZ/G2 Secure IP Package that includes Secure IP Libraries, etc. For inquiries regarding the provision of RZ/G2 Secure IP Package, please contact Renesas Electronics distributor or contact us.

4.1 Functions

TEE for RZ/G2 supports Secure Boot using the on chip Trusted Secure IP included with RZ/G2 Group processor. The signed and encrypted data stored in the non-volatile memory is decrypted and verified using TSIP to check for tampering.

4.1.1 Secure Boot

Secure Boot sequence is shown below.

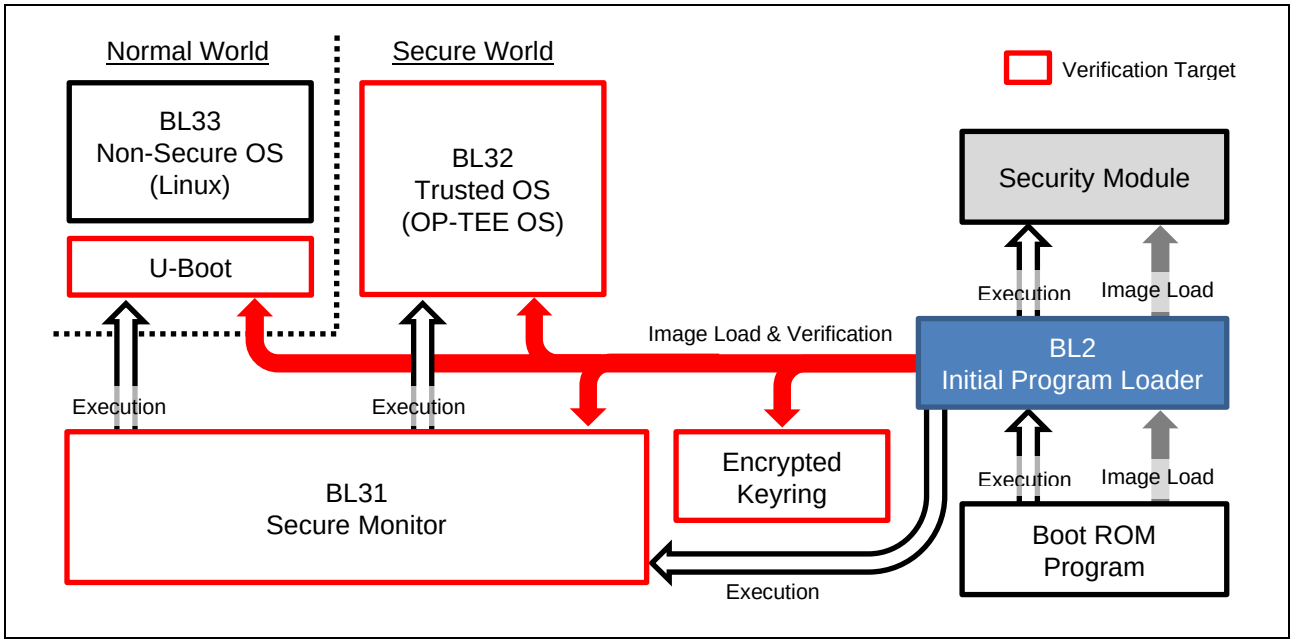

Figure 4-1 Secure Boot Sequence

BL31, BL32, U-Boot, and Keyring are verified by Secure Boot. These data are signed and encrypted before being stored in non-volatile memory. During Secure Boot, BL31, BL32 and U-Boot are decrypted and validated, and placed in RAM. The Keyring is verified and placed in RAM.

Verification and decryption of firmware images by Secure Boot is done in the Security Module. If Security Module failed validation, BL2 aborts the boot sequence.

(a) Security Module

Security Module is software for using TSIP included with RZ/G2 Group processor. Security Module includes Secure IP library for decryption and verification using TSIP. Secure IP library is a library for accessing TSIP.

(b) Encrypted Keyring

Keyring is a bunch of Session Keys used to bring data prepared in the external environment to the user product environment. Encrypted Keyring is the data that Keyring is encrypted with a device-specific key. Encrypted Keyring can only be accessed by TSIP and are never decrypted into RAM.

Encrypted Keyring is used to securely bring in data from the outside, such as Provisioning of the User Data and Firmware Update.

4.1.2 Provisioning

Provisioning is the process of building Secure Boot environment on the evaluation board.

The provisioning process performed by the customer is shown below.

Step 1 Process on the build environment

1. Generation of Keyring
2. Temporary encryption of Keyring
3. Temporary encryption of User Data

Step 2 Process on the target environment

4. Re-Encryption of Keyring
5. Re-Encryption of User Data

The following is an overview of each step in the Provisioning process.

4.1.2.1 Generation of Keyring

Keyring is a bunch of Session Keys. Session Keys is used to temporarily encrypt the User Data and Keys prepared in the external environment.

This process generates Session Keys and Keyring in the external environment.

4.1.2.2 Temporary encryption of Keyring

This process encrypts Keyring using Provisioning Key. Encrypting Keyring prevents the session key from leaking between the external environment and the user product environment.

4.1.2.3 Temporary encryption of User Data

This process encrypts User Data for Secure Boot using the Temporary Encryption Key for User Data included in Keyring. User Data is signed with a private key that is paired with Temporary Verification Key for Signature of User Data before it is encrypted.

4.1.2.4 Re-Encryption of Keyring

This process re-encrypts Temporarily Encrypted Keyring using Device-Specific Key by TSIP. Re-encryption of Keyring requires Encrypted Provisioning Key to decrypt Temporarily Encrypted Keyring.

Re-Encrypted Keyring is stored in non-volatile memory and is used for "Re-encryption of User Data" and Secure Boot. Re-Encrypted Keyring cannot be used on other devices because it is encrypted using Device-Specific Key.

4.1.2.5 Re-Encryption of User Data

This process re-encrypts Temporarily Encrypted User Data using Device-Specific Key by TSIP. Re-encryption of User Data requires Re-Encrypted Keyring to decrypt Temporarily Encrypted User Data.

Re-Encrypted User Data is stored in non-volatile memory and decrypted and validated during Secure Boot. Re-Encrypted User Data cannot be decrypted and verified on other devices because it is encrypted using Device-Specific Key.

4.2 Provided Items

The following is included in RZ/G2 Secure IP Package provided by Renesas. This package is only available to users who have agreed to the license agreement.

Table 4-1 Provided Items

Type	File Name	Description
Binary	ProvisioningKey.bin	Key used to temporarily encrypt Keyring created in the build environment. By encrypting Keyring with this key prevents the session key from leaking between the external environment and the user product environment.
	ProvisioningKey_Enc.bin	Provisioning Key encrypted with the Hidden Root Key managed by Renesas. Used to re-encrypt the temporarily encrypted Keyring in the user product environment.
	libr_secure_ip_lib_g2X.a	A symbolic link to libr_secure_ip_lib_g2X.a.X.X.X.
	libr_secure_ip_lib_g2X.a.X.X.X	Secure IP library to provide TSIP features. In "TEE for RZ/G2", it is referred to in the build of the following software. • Security Module • Secure IP driver implemented on OP-TEE OS

Note: “X.X.X” given to the library name is the version number of the library. Please use the version of the library that are defined in Security Module or Secure IP driver.

ProvisioningKey.bin and ProvisioningKey_Enc.bin, included in this package, are sample keys. In the product version, it is necessary to newly create these keys in the customer environment. Please refer to "Related Document No.5" for how to create new provisioning keys.

File configuration of the provided items shown below.

```
<Package>
├── README.md
└── binary
    ├── ek874
    │   ├── key
    │   │   └── Provisioning
    │   │       ├── ProvisioningKey.bin
    │   │       └── ProvisioningKey_Enc.bin
    │   └── lib
    │       ├── libr_secure_ip_lib_g2e.a
    │       └── libr_secure_ip_lib_g2e.a.X.X.X
    ├── hihope-rzg2h
    │   ├── key
    │   │   └── Provisioning
    │   │       ├── ProvisioningKey.bin
    │   │       └── ProvisioningKey_Enc.bin
    │   └── lib
    │       ├── libr_secure_ip_lib_g2h.a
    │       └── libr_secure_ip_lib_g2h.a.X.X.X
    ├── hihope-rzg2m
    │   ├── key
    │   │   └── Provisioning
    │   │       ├── ProvisioningKey.bin
    │   │       └── ProvisioningKey_Enc.bin
    │   └── lib
    │       ├── libr_secure_ip_lib_g2m.a
    │       └── libr_secure_ip_lib_g2m.a.X.X.X
    └── hihope-rzg2n
        ├── key
        │   └── Provisioning
        │       ├── ProvisioningKey.bin
        │       └── ProvisioningKey_Enc.bin
        └── lib
            ├── libr_secure_ip_lib_g2n.a
            └── libr_secure_ip_lib_g2n.a.X.X.X
```

Figure 4-2 File configuration of the provided items

4.3 Build Images

This section explains the procedure for building RZ/G2 Linux BSP image that implements Secure Boot. "Temporary encryption of Keyring" and "Temporary encryption of User Data" in the Provisioning process are performed during this build procedure. This procedure assumes that “3.1 Build Images” has been executed in advance.

Step 1 Install Secure IP Package

Unpack the RZ/G2 Secure IP Package and store the binary data in the directory.

```
$ tar zxvf <Secure IP Package>.tar.gz
$ mkdir -p ${HOME}/.secprv
$ cp -rf <Secure IP Package>/binary/* ${HOME}/.secprv
```

The storage destination directory is defined in the following recipe file.

On ${WORK}/meta-rzg2/recipes-bsp/security/secprv-native_1.0.bb

DIRPATH_SEC_STORAGE = "**${HOME}/.secprv**"

Step 2 Enable Secure Boot

To enable Secure Boot, change the “RZG2_SECURE_BOOT” option defined in the recipe file below to “ENABLE”.

On ${WORK}/meta-rzg2/include/rzg2-security-config.inc

RZG2_SECURE_BOOT = **'ENABLE'**

Step 3 Generate Keyring

Run the following command to generate Keyring.

```
$ bitbake secprv-native -c newkey -f
```

The generated Keyring is stored in the directory defined in the following recipe file.

On ${WORK}/meta-rzg2/recipes-bsp/security/secprv-native_1.0.bb

DIRPATH_GEN_KEY_ROOT = "**${DIRPATH_SEC_STORAGE}/${MACHINE}/key**"

Step 4 Build

Please build as follows.

```
$ bitbake core-image-weston
```

Note: Please refer to “Related Document No.1” for the image types supported by RZ/G2 Linux BSP.

The data file is stored in the ${WORK}/build/tmp/deploy/images/<board> directory.

4.4 Board Settings

Write RZ/G2 Linux BSP images implemented Secure Boot into the evaluation board flash memory. The tool to be written to the flash memory, please use the flash writer that has been created in the procedure of “4.3.Build Images”. Refer to “Related Document No.1” for the procedure for booting the Flash Writer and setting the evaluation board.

4.4.1 Writing data

The writing data is the “fip-<board>.mot” only. The “fip-<board>.mot” is the file that packages multiple firmware images into one.

Note: <board>: ek874, hihope-rzg2m, hihope-rzg2n, hihope-rzg2h.

The firmware images packaged in “fip-<board>.mot” is shown below.

- Loader(Boot Parameter)
- Loader (BL2)
- Loader(Certification)
- Security Module
- Temporarily Encrypted “Keyring”
- Temporarily Encrypted “Trusted Firmware-A (BL31)”
- Temporarily Encrypted “OP-TEE OS (BL32)”
- Temporarily Encrypted “U-Boot”

4.4.2 How to write

Please connect RZ/G2 System Evaluation Board, Windows Host PC with terminal software for console and Linux Host PC.

Step 1 connect cable and setting the terminal software

For step of "connect cable" and "setting the terminal software", please refer to "Related Document No.1".

Step 2 write data file to SPI Flash

A file is written in SPI Flash in the following procedures.

- Set dip switch “SCIF download mode”.
- Reset board then start SCIF download mode.
- After “please send !” displayed, In case of Tera Term, transmit file AArch64_Flash_writer_SCIF_DUMMY_CERT_E6300400_<board>.mot which is stored in ${WORK}/build/tmp/deploy/images/<board>, by "File -> Send file (S)".
- Execute xls2s command (unpack FIP and load program to flash).

```
SCIF Download mode (w/o verification)
 (C) Renesas Electronics Corp.

-- Load Program to SystemRAM ---------------
please send !

Flash writer for RZ/G2M V1.04 Dec.02,2020
>xls2s

===== Qspi writing of RZ/G2 Board Command =====
Load Program to SPI Flash
Writes to any of SPI address.
 Winbond : W25M512JW

Work RAM(H'50000000-H'53FFFFFF) Clear....
please send ! ('.' & CR stop load)
```

- After "please send ! ('.' & CR stop load)" is displayed, In case of Tera Term, transmit “fip-<board>.mot” by "File -> Send file(S)".
- If there are some data in writing area, "SPI Data Clear(H'FF) Check :H'00000000-0003FFFF Clear OK?(y/n)" is displayed. Then input "y".
- After "Finish!" is displayed, the prompt returns. It means finish.
- Power OFF.
- Set dip switch to “Boot Mode”.

Step 3 Confirm Secure Boot

Turn on the power after changing the DIP switch to "Boot Mode". Confirm that the following log is output to the terminal software.

```
NOTICE:  BL2: Secure boot
NOTICE:  BL2: dst=0xe631d300 src=0x8180000 len=512(0x200)
NOTICE:  BL2: dst=0x43f00000 src=0x8180400 len=10240(0x2800)
NOTICE:  rzg_file_len: len: 0x0001e000
NOTICE:  BL2: dst=0x440e0000 src=0x8400000 len=122880(0x1e000)
NOTICE:  rzg_file_len: len: 0x00001000
NOTICE:  BL2: dst=0x440fe000 src=0x8500000 len=4096(0x1000)
NOTICE:  Verification Successful for image id = 43
NOTICE:  rzg_file_len: len: 0x0003e000
NOTICE:  BL2: dst=0x44000000 src=0x81c0000 len=253952(0x3e000)
NOTICE:  Verification Successful for image id = 3
NOTICE:  rzg_file_len: len: 0x00100000
NOTICE:  BL2: dst=0x44100000 src=0x8200000 len=1048576(0x100000)
NOTICE:  Verification Successful for image id = 4
NOTICE:  rzg_file_len: len: 0x00100000
NOTICE:  BL2: dst=0x50000000 src=0x8300000 len=1048576(0x100000)
NOTICE:  Verification Successful for image id = 5
NOTICE:  BL2: Booting BL31
```

- "NOTICE: BL2: Secure boot" is displayed when secure boot is implemented.
- "NOTICE: Verification Successful for image id = 43" is displayed when the encrypted keyring is successfully verified.
- "NOTICE: Verification Successful for image id = 3" is displayed when the encrypted BL31 is successfully decrypted and verified.
- "NOTICE: Verification Successful for image id = 4" is displayed when the encrypted OP-TEE OS is successfully decrypted and verified.
- "NOTICE: Verification Successful for image id = 5" is displayed when the encrypted U-Boot is successfully decrypted and verified.

5. Build Test suite

To check the operation of TEE for RZ/G2 built on the evaluation board, please build OP-TEE Test, which is a test suite of OP-TEE. This procedure assumes that “3.1 Build Images” has been executed in advance.

Step 1 Build

Please build as follows.

```
$ bitbake optee-test
```

The “optee-test-<board>.tar.gz” is stored in the ${WORK}/build/tmp/deploy/images/<board> directory.

Step 2 Run optee-test on board

For details on how to run OP-TEE Test, please refer to the following site.

https://optee.readthedocs.io/en/latest/building/gits/optee_test.html

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Mar. 31,2021	-	First edition issued.
1.01	May. 31,2021	5	Update version of optee to v3.12.0

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/.