Release Note

CONFIDENTIAL

Security Board Support Package

Release Note: Software

R-Car Series, 3rd Generation

Renesas Electronics
www.renesas.com

Rev.3.0.4 Dec.2021

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

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/.

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Trademark

How to Use This Manual

- **[Readers]**
  This manual is intended for engineers who develop products which use the R-Car H3/M3/M3N/E3/D3 processor.

- **[Purpose]**
  This manual is intended to give users an understanding of the functions of the R-Car H3/M3/M3N/E3/D3 processor device driver and to serve as a reference for developing hardware and software for systems that use this driver.

- **[How to Read This Manual]**
  It is assumed that the readers of this manual have general knowledge in the fields of electrical
  — engineering, logic circuits, microcontrollers, and Linux.
  → Read this manual in the order of the CONTENTS.
  — To understand the functions of a multimedia processor for R-Car H3/M3/M3N/E3/D3
  → See the R-Car H3/M3/M3N/E3/D3 User's Manual.
  — To know the electrical specifications of the multimedia processor for R-Car H3/M3/M3N/E3/D3
  → See the R-Car H3/M3/M3N/E3/D3 Data Sheet.

- **[Conventions]**
  The following symbols are used in this manual.
  Data significance: Higher digits on the left and lower digits on the right
  Note: Footnote for item marked with Note in the text
  Caution: Information requiring particular attention
  Remark: Supplementary information
  Numeric representation: Binary ... ××××, 0b××××, or ××××B
  Decimal ... ××××
  Hexadecimal ... 0x×××× or ××××H
  Data type: Double word … 64 bits
  Word … 32 bits
  Half word ... 16 bits
  Byte ... 8 bits

Table of Contents

1. Introduction

1.1 Objectives

This manual explains the package construction of R-Car H3/M3/M3N/E3/D3/H3e/M3e/M3Ne/E3e/D3e Security Board Support Package.

1.2 References

[1] Renesas Electronics Corp., *Linux Interface Specification Yocto recipe Start-Up Guide.*

[2] Renesas Electronics Corp., *Security Board Support Package User's Manual.*

This manual refers to the latest edition of the references.

2. Components

The following is components included in this package.

2.1 Software components

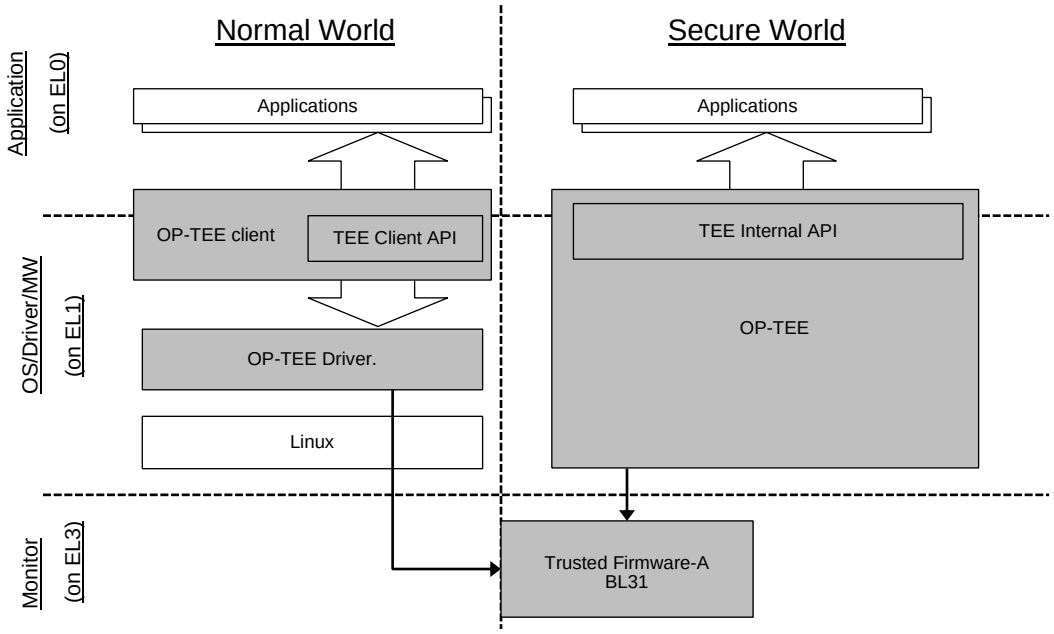

Figure 1 Software components

2.2 Software

Software is provided by the R-Car H3/M3/M3N/E3/D3 Yocto recipe.

2.2.1 Trusted Firmware-A (BL31)

This component is porting to R-Car H3/M3/M3N/E3/D3 platform.
Arm provides "Trusted Firmware-A", which is a reference implementation of Arm interface standards, such as Secure Monitor, PSCI (Power State Coordination Interface).
The software is provided under a BSD 3-Clause license.

2.2.2 OP-TEE OS

This component is porting to R-Car H3/M3/M3N/E3/D3 platform.
The OP-TEE OS is the Trusted OS that using the Arm(R) TrustZone(R) technology and provides the TEE Internal API v1.0 as defined by the Global Platform TEE Standard for the development of Trusted Applications.
The software is distributed mostly under the BSD 2-Clause open source license, apart from some files in the optee_os/lib/libutils directory which are distributed under the BSD 3-Clause or public domain licenses.

2.2.3 OP-TEE Driver

This component is Linux driver.
It implements TEE driver that allows communication between Linux and OP-TEE OS.
And it is customized function for output of logs from OP-TEE OS when executing on debug mode.
The software is provided under the GPL-2.0 license.

2.2.4 OP-TEE Client

This package provides the TEE client library and TEE supplicant.
It contains API defined by the GlobalPlatform TEE standard for communication with the Trusted OS.
The software is provided under the BSD 2-Clause license.

3. Change History

Following change histories are representative lists.

3.1 v1.0.0

First release version.

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.0
OP-TEE OS	1.0.0
OP-TEE Linux Driver	1.0.0
OP-TEE Client	1.0.0

3.2 v1.0.1

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.1
OP-TEE OS	1.0.1
OP-TEE Linux Driver	1.0.1
OP-TEE Client	1.0.1

Fix and add about following restrictions and functions.

No.	Module	Description
#77205	ARM Trusted Firmware (BL31)	Version up the base version of arm-trusted-firmware. https://github.com/ARM-software/arm-trusted-firmware Commit e234ba038b0b997bd4325dad384deab5863babdd ➔ 41099f4e7468d872857c52608dcc2a51bae68174
#75084	OP-TEE OS OP-TEE Linux Driver OP-TEE Client	Version up the base version of OP-TEE from 0.2.0 to 1.0.0. OP-TEE OS : https://github.com/OP-TEE/optee_os/releases/tag/1.0.0 OP-TEE Linux Driver : https://github.com/OP-TEE/optee_linuxdriver/releases/tag/1.0.0 OP-TEE Client : https://github.com/OP-TEE/optee_client/releases/tag/1.0.0 At the same time as the above changes, we support that OP-TEE OS architecture operates in AArch64. However, Trusted Application operates in AArch32.
#77790	ARM Trusted Firmware (BL31)	Add the following build option for arm-trusted-firmware BL31. “PSCI_DISABLE_BIGLITTLE_IN_CA57BOOT” If this option value is 0, Cortex-A57 and Cortex-A53 both cores will start. If this option value is 1, Cortex-A53 cores will not start. Only if Cortex-A53 is set as boot CPU, Cortex-A57 and Cortex-A53 both cores will start. In default, this option value is 1.

3.3 v1.0.2

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.2
OP-TEE OS	1.0.1
OP-TEE Linux Driver	1.0.1
OP-TEE Client	1.0.1

Fix and add about following restrictions and functions.

No.	Module	Description
#76010	ARM Trusted Firmware (BL31)	Add PSCI function.

3.4 v1.0.3

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.4
OP-TEE OS	1.0.1
OP-TEE OS Linux Driver	1.0.1
OP-TEE Client	1.0.1

Fix and add about following restrictions and functions.

No.	Module	Description
#83588	ARM Trusted Firmware (BL31)	Change Generic Timer setting (frequency).

3.5 v1.0.4

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.5
OP-TEE OS	1.0.2
OP-TEE Linux Driver	1.0.2
OP-TEE Client	1.0.2

Fix and add about following restrictions and functions.

No.	Module	Description
#74306	OP-TEE OS	Add secure boot of Dynamic TA.
#81198	ARM Trusted Firmware (BL31)	Prohibited CPU_OFF from the other cores other than the primary core.
#82386	OP-TEE Linux Driver OP-TEE Client	Add the TEE Client library for 32bit Linux applications. Change the base version of OP-TEE Linux Driver from 1.0.0 to d4463ddb6be6f5737ff819113ba846567a3db773. Change the base version of OP-TEE Client from 1.0.0 to 6b08c092f79e1aade3a5ee1b78c4ddb345f8a1f0.
#83174	OP-TEE Client	Add register the tee-supplicant to systeme service.
#83298	OP-TEE OS	Fix to test complete of optee_test.
#85092	ARM Trusted Firmware (BL31)	Fix deadlock of log output.
#85819	OP-TEE OS	Remove the unused source code for getting a random value from the hardware.
#81609	OP-TEE OS	Fix to generate the correct key in the case of generating ssk.
#85284	OP-TEE OS	Add to not write the log of interrupt context in the default settings.
#85534	OP-TEE OS	Fix to build successfully with setting optimization options enable when using gcc version 4.9.3 or later.

3.6 v1.0.5

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.6
OP-TEE OS	1.0.3
OP-TEE Linux Driver	1.0.3
OP-TEE Client	1.0.3

Fix and add about following restrictions and functions.

No.	Module	Description
#84157	ARM Trusted Firmware (BL31)	Delete size of version character.
#87459	OP-TEE OS	Add the address of Mask ROM API for M3
#86327	ARM Trusted Firmware (BL31)	Add setting for M3 CCI500 slave port and L2 cache for Cortex-A57.
#87678	ARM Trusted Firmware (BL31)	Remove the FIQ setting of SYS-DMAC2 to allocate security state by BL31.
#88225	OP-TEE OS	Fix cache attribute for the logging area in RAM to Non-cacheable.
#88237	ARM Trusted Firmware (BL31)	Fix cache attribute for the logging area in RAM to Non-cacheable.

3.7 v1.0.6

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.7
OP-TEE OS	1.0.3
OP-TEE Linux Driver	1.0.3
OP-TEE Client	1.0.3

3.8 v1.0.7

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.8
OP-TEE OS	1.0.4
OP-TEE Linux Driver	1.0.4
OP-TEE Client	1.0.4

No.	Module	Description
#92138	ARM Trusted Firmware (BL31)	Fix when compiling ARM Trusted Firmware opteed building failed.
#84416	ARM Trusted Firmware (BL31)	Add supported by PMIC control of SYSTEM_OFF and SYSTEM_RESET
#84590	ARM Trusted Firmware (BL31)	Modify ARM Trusted Firmware with version-up OP-TEE OS.
#84590	OP-TEE OS OP-TEE Linux Driver OP-TEE Client	Version up the base version. OP-TEE OS : change from https://github.com/OP-TEE/optee_os/releases/tag/1.0.0 to f06bddf5c0bc9be8013820e86523793c44930148. OP-TEE Linux Driver: change from d4463ddb6be6f5737ff819113ba846567a3db773 to f9779c6095dd2e2f492e27a6d79f2c766d3e5714. OP-TEE Client: change from 6b08c092f79e1aade3a5ee1b78c4ddb345f8a1f0 to db9c64d45818d146200297eaaedbd421a8b59e3a.

3.9 v1.0.8

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.9
OP-TEE OS	1.0.5
OP-TEE Linux Driver	1.0.5
OP-TEE Client	1.0.5

No.	Module	Description
#86022	ARM Trusted Firmware (BL31)	Add the feature of Suspend to RAM.
#97222	ARM Trusted Firmware (BL31)	**[H/W Restriction No.58]** Change CA5xBAR address from SystemRAM to SDRAM.
#99015	ARM Trusted Firmware (BL31)	Change a path of #include header file to not use a related path.
#97457	ARM Trusted Firmware (BL31)	Fix the issue that does not start in the CPU SUSPEND.(case of the StateType0)
#77395	OP-TEE OS	Add QSPI/HyperFlash driver.
#77380	OP-TEE OS	Add SecureStorage Stand-alone FS.
#87648	OP-TEE OS OP-TEE Linux Driver	Add function to use RPMB.
#91497	OP-TEE OS	Add System Watch Dog timer driver and MFIS driver.
#77333	OP-TEE OS	Add function of get_hw_unique_key and get_die_id.
#98537	OP-TEE OS	Add the default setting for Secure Storage.

3.10 v1.0.9

The following table represents a revision of the software in this version.

The revision of ARM Trusted Firmware has been updated due to change of the function of ARM Trusted Firmware other than BL31, but there is no change as Secure Board Support Package.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.9.10
OP-TEE OS	1.0.5
OP-TEE Linux Driver	1.0.5
OP-TEE Client	1.0.5

3.11 v1.0.10

The following table represents a revision of the software in this version.

The revision of ARM Trusted Firmware has been updated due to change of the function of ARM Trusted Firmware other than BL31, but there is no change as Secure Board Support Package.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.10
OP-TEE OS	1.0.5
OP-TEE Linux Driver	1.0.5
OP-TEE Client	1.0.5

3.12 v1.0.11

The following table represents a revision of the software in this version.

The revision of ARM Trusted Firmware has been updated due to change of the function of ARM Trusted Firmware other than BL31, but there is no change as Secure Board Support Package.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.11
OP-TEE OS	1.0.5
OP-TEE Linux Driver	1.0.5
OP-TEE Client	1.0.5

3.13 v1.0.12

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.12
OP-TEE OS	1.0.6
OP-TEE Linux Driver	1.0.6

The following table represents a version of the OSS.

Module	Git repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	db9c64d45818d146200297eaaedbd421a8b59e3a	-

No.	Module	Description
#108783	ARM Trusted Firmware (BL31)	Version up the base version of arm-trusted-firmware. https://github.com/ ARM-software/arm-trusted-firmware Commit ID 6bb37adc203567c2f9322dfbe34058a5f12d4c70 [Tag: v1.3]
#106615	ARM Trusted Firmware (BL31)	Add the compile option for power management IC condition.
#108422	ARM Trusted Firmware (BL31)	Fix that turning on the secondary CPU power fails when created with DEBUG option.
#81745	ARM Trusted Firmware (BL31)	Change the CPU ON sequence.
#108771	ARM Trusted Firmware (BL31)	Add stack area to be used when panic occurs to MMU table.
#103206	ARM Trusted Firmware (BL31)	Change the sequence to save timer register on Suspend to RAM.
#108759	ARM Trusted Firmware (BL31)	Change the format of the time displayed in the log.
#111572	ARM Trusted Firmware (BL31)	Delete processing when the RESET_TO_BL31 option is enabled.
#96118	OP-TEE OS	Version up the base version of OP-TEE OS. https://github.com/OP-TEE/optee_os Commit ID c0c5d399d81a0669f5c8e3bcb20039d65649a78d [Tag: 2.2.0]
#101690	OP-TEE OS	Add the feature of Suspend to RAM. [Framework]
#103076	OP-TEE OS	Add the feature of Suspend to RAM. [MFIS driver]
#100742	OP-TEE OS	Fix bug of signal request to GPIO or INTC. [MFIS driver]
#103081	OP-TEE OS	Add the feature of Suspend to RAM. [System Watch Dog timer driver]
#107082	OP-TEE OS	Add the feature of Suspend to RAM. [QSPI/HyperFlash driver]
#101690	OP-TEE Linux Driver	Add the feature of Suspend to RAM.
#107189	OP-TEE OS	Add the feature of Suspend to RAM. [Provider]
#108079	OP-TEE OS	Fix the variable type conversion for the asymmetric algorithm
#109321	OP-TEE OS	Fix the process replacing RSA definition value
#109320	OP-TEE OS	Fix the random value generate function to generate data exceeding 64KB
#100308	OP-TEE OS	Add the LCS check error code to the AES unwrap function.
#101712	OP-TEE Client	Fix the virtual device setting value of RPMB.
#102397	OP-TEE Linux Driver	Fix the multiple block frames writing of RPMB.
#102161	OP-TEE OS	Fix the return value is different from expectation. [HyperFlash driver]
#105270	OP-TEE OS	Fix the error in root directory specification. [Stand-alone FS]
#105388	OP-TEE OS	Fix the parameter leakage in argument. [Stand-alone FS]
#107261	OP-TEE OS	Fix it can detect tampering of the Encrypted IV. [Stand-alone FS]
#107264	OP-TEE OS	Fix to be able to find additional files after corruption of record meta detection. [Stand-alone FS]
#108566	OP-TEE OS	Fix the 6010’s optee_test fails. [Stand-alone FS]
#109123	OP-TEE OS	Fix the reads beyond sector range. [Stand-alone FS]
#111051	OP-TEE OS	Fix the disable IRQ execution while executing update_current_ctx().
#111238	OP-TEE OS	Fix the cache attribute of Crypto Engine Work area.
#111238	OP-TEE OS	Fix the include condition of the header file. [Provider]

3.14 v1.0.13

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.13
OP-TEE OS	1.0.7
OP-TEE Linux Driver	1.0.6

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	db9c64d45818d1462002 97eaaedbd421a8b59e3a	-

No.	Module	Description
#110830	ARM Trusted Firmware (BL31)	Add processing to check the intended duplication of the MMU table.
#106065	ARM Trusted Firmware (BL31)	Delete or replace assert() processing of bl31.
#113961	ARM Trusted Firmware (BL31)	Change CCI-500 Slave(snoop) port for H3 Ver.2.0.
#109970	ARM Trusted Firmware (BL31)	Add guard processing for CPU_OFF to boot cpu.
#116626	ARM Trusted Firmware (BL31)	Delete initial setting of Generic Timer from bl31. The debug code changed by the REE patch has also been deleted.
#116611	ARM Trusted Firmware (BL31)	Fix the event sender of bl31 for CPU Suspend and System Suspend.
#117318	ARM Trusted Firmware (BL31)	Add shutdown and reboot processing when PMIC is not connected. Change System Suspend to invalid when PMIC is not connected.
#110644	OP-TEE OS	Improve the read performance of Stand-alone_FS.
#112716	OP-TEE OS	Fix the problems that optee's operation is unstable when OP-TEE debug log (Linux terminal output) is enabled.
#112997	OP-TEE OS	Add the address of MaskROM API for H3 Ver.2.0 to OP-TEE.
#114084	OP-TEE OS	Add the processing of extended key length for Dynamic TA authentication.
#114503	OP-TEE OS	Fix the include condition of the header file. [Provider]
#114660	OP-TEE OS	Fix the event receiver of OP-TEE for CPU Idle.
#116871	OP-TEE OS	Add the table of MaskROM API start address for each LSI type and version.
#117905	OP-TEE OS	Fix the register setting of HyperFlash driver.
#117645	OP-TEE OS	Add TEE Internal API for SS6.3-Secure Driver.

3.15 v1.0.14

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.14
OP-TEE OS	1.0.8
OP-TEE Linux Driver	1.0.6

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	db9c64d45818d146200297eaaedbd421a8b59e3a	-

No.	Module	Description
#119342	ARM Trusted Firmware (BL31)	rcar: memdrv: Replace readreg_cntpct_el0() by read_cntpct_el0()
#120324	ARM Trusted Firmware (BL31)	Add I-Cache clear for processing of Suspend to RAM.
#118603	OP-TEE OS	Fix buffering function in AES-CTS mode of TEE Internal API. This fix was backported from the following OP-TEE OS. https://github.com/OP-TEE/optee_os Commit ID b1ecda78bab43d76bc570ecff30ddd232caecf18 Commit ID bf7a587fd9a1ce486e001e3f16fb88d17dc448e8

3.16 v1.0.15

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.15
OP-TEE OS	1.0.8
OP-TEE Linux Driver	1.0.6

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	db9c64d45818d146200297eaaedbd421a8b59e3a	-

No.	Module	Description
#122654	ARM Trusted Firmware (BL31)	Change not to accept SYSTEM_SUSPEND request from other than Master Boot Processor (CPU0).
#123163	ARM Trusted Firmware (BL31)	Change the guard processing for CPU_OFF to be valid only for R-Car.

3.17 v1.0.16

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.16
OP-TEE OS	1.0.9
OP-TEE Linux Driver	1.0.7

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	db9c64d45818d146200297eaaedbd421a8b59e3a	-

No.	Module	Description
#128344	ARM Trusted Firmware (BL31)	Replace PMIC_ON_BOARD macro with some new macros that correspond to the function.
#130795	ARM Trusted Firmware (BL31)	**[H/W Restriction No.95]** Delete L2 shutdown mode setting.
#134325	ARM Trusted Firmware (BL31)	Add control DBSC write protect.
#124410	OP-TEE OS	Change MFIS driver to receive only security errors.
#128028	OP-TEE OS	Delete DDR training process in OP-TEE.
#124543	OP-TEE OS	Change not to perform redundant initialization when generating random numbers.
#128580	OP-TEE Linux Driver	Fix variable types to use the TEE Client API in the kernel space.
#130217	OP-TEE Linux Driver	Fix memory management function of TEE Client API in the kernel space.
#129846	OP-TEE OS	Add exclusive control to the Dynamic TA authentication.

3.18 v1.0.17

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.17
OP-TEE OS	1.0.10
OP-TEE Linux Driver	1.0.7

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	db9c64d45818d146200297eaaedbd421a8b59e3a	-

No.	Module	Description
#135282	ARM Trusted Firmware (BL31)	Add M3N compatible processing.
#143674	OP-TEE OS	Change operating frequency for data writes of OP-TEE HyperFlash driver.

3.19 v1.0.18

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.18
OP-TEE OS	1.0.11
OP-TEE Driver	1.0.8

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	73b4e490a8ed0b4a7714818e80998b9d8a7da958	2.6.0

No.	Module	Description
#135840	ARM Trusted Firmware (BL31)	Version up the base version of arm-trusted-firmware. https://github.com/ARM-software/arm-trusted-firmware Commit ID b762fc7481c66b64eb98b6ff694d569e66253973 [Tag: v1.4]
#143418	ARM Trusted Firmware (BL31)	Remove PSCI_DISABLE_BIGLITTLE_IN_CA57BOOT options.
#139409	OP-TEE OS	Version up the base version of OP-TEE from 2.2.0 to 2.6.0. https://github.com/OP-TEE/optee_os Commit ID 6d57389f9eec0c213da917e35861a8eca4b205b3 [Tag: 2.6.0]
#143048	OP-TEE OS	Update of Provider with base version up of optee_os
#139423	OP-TEE OS	Update of Stand-alone_FS with base version up of optee_os.
#147681	OP-TEE OS	Update of SPI/HyperFlash_Drv with base version up of optee_os.
#142588	OP-TEE OS	Update of RPMB_FS with base version up of optee_os.
#141945	OP-TEE OS	Update of MFIS_Drv with base version up of optee_os.
#141952	OP-TEE OS	Update of SWDT_Drv with base version up of optee_os.
#142564	OP-TEE OS	Supports RSA key sizes of 3072-bit and 4096-bit
#139431	OP-TEE Driver	OP-TEE Linux Driver will cease use and transition to OP-TEE Driver. OP-TEE Driver uses the source code under drivers/tee/optee/ of Linux v4.14.
#142528	OP-TEE Driver	Update of TEE Client API for a kernel space with base version up of OP-TEE Driver. https://github.com/linaro-swg/linux Commit ID b762fc7481c66b64eb98b6ff694d569e66253973
#146762	OP-TEE Driver	Fixed a memory release function of TEE Clinet API for kernel which does not release memory when the function is called.
#148818	OP-TEE OS	Fix the bug that Stand-alone FS API returned an error code different from expected value.

3.20 v1.0.19

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.19
OP-TEE OS	1.0.12
OP-TEE Driver	1.0.8

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	73b4e490a8ed0b4a7714818e80998b9d8a7da958	2.6.0

No.	Module	Description
#153299	ARM Trusted Firmware (BL31)	Fix the primary CPU decision function that runs at startup.
#152437	ARM Trusted Firmware (BL31)	Change the SelfRefresh sequence of Suspend To RAM.
#157621	ARM Trusted Firmware (BL31)	Add the DVFS SCL setting of E3.
#152562	OP-TEE OS	Add the setting of the RPC clock of R-Car E3.
#152248	OP-TEE OS	Change the RPC clock of HyperFlash to up to 160MHz.

3.21 v1.0.20

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.20
OP-TEE OS	1.0.13
OP-TEE Driver	1.0.8

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	73b4e490a8ed0b4a7714818e80998b9d8a7da958	2.6.0

No.	Module	Description
#156230	ARM Trusted Firmware (BL31)	Add processing to read MSTP status into BL31.
#156697	OP-TEE OS	Add processing to read MSTP status into MFIS.

3.22 v1.0.21

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.21
OP-TEE OS	1.0.14
OP-TEE Driver	1.0.8

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#153406	ARM Trusted Firmware (BL31)	Backport the workaround for CVE-2017-5715.
#168187	ARM Trusted Firmware (BL31)	Apply the local workaround for CVE-2018-3639.
#165907	ARM Trusted Firmware (BL31)	Add processing of preserve the DRAM contents during a system reset.
#166317	ARM Trusted Firmware (BL31)	Add L2 shutdown mode setting.
#166045	OP-TEE OS	Version up the base version of OP-TEE from 2.6.0 to 3.1.0. https://github.com/OP-TEE/optee_os Commit ID 0ab9388c0d553a6bb5ae04e41b38ba40cf0474bf [Tag: 3.1.0]
#166141	OP-TEE OS	Update of Provider with base version up of optee_os.
#168590	OP-TEE OS	Fix the RPC register specification violation of HyperFlash driver.
#170808	OP-TEE OS	Fix to process ECDSA with LibTomCrypt when an input hash size is larger than a key length.
#170018	OP-TEE OS	Fix TEE_CopyOperation to copy the tag size value from a source buffer to a destination buffer.

3.23 v1.0.22

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.22
OP-TEE OS	1.0.15
OP-TEE Driver	1.0.8

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#177241	ARM Trusted Firmware (BL31)	Add the wait processing that is placed in the system RAM area for Suspend To RAM.
#177304	OP-TEE OS	Fix the polling process of the HyperFlash driver waiting for HW completion.
#173341	OP-TEE OS	Fix incorrect memory access in RSA processing using a provider for a HW engine driver.
#182900	OP-TEE OS	Fix a conditional branch in a mutex_destroy function.
#179179	OP-TEE OS	Fix AES CBC routines. https://github.com/OP-TEE/optee_os Commit ID e77020396508fc086d7a4d6137388b116e4a662f Note: Commit ID is applied by 'git cherry-pick' from yocto recipe (optee-os_git.bb).

3.24 v1.0.23

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	1.0.23
OP-TEE OS	1.0.16
OP-TEE Driver	1.0.9

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#171982	ARM Trusted Firmware (BL31)	Version up the base version of arm-trusted-firmware. https://github.com/ARM-software/arm-trusted-firmware Commit ID ed8112606c54d85781fc8429160883d6310ece32 [Tag: v1.5]
#168894	ARM Trusted Firmware (BL31)	Backport the workaround for CVE-2018-3639.
#151762	OP-TEE Driver	Change workqueue to kthread in debug log function.
#188122	OP-TEE OS	Fix to exclusive control in ECDSA operation used by HW engines.
#188185	OP-TEE OS	Fix a context size allocated by OP-TEE OS with a HW engine.
#190194	OP-TEE OS	Fix to set the initial value for a parameter in TEE_AEInit.
#190112	OP-TEE OS	Fix to clear the read cache of standalone_fs_create.

3.25 v2.0.0

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.0
OP-TEE OS	2.0.0
OP-TEE Driver	1.0.9

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#190241	ARM Trusted Firmware (BL31)	Add API for getting DRAM capacity information.
#186044	ARM Trusted Firmware (BL31)	Change the execution timing of system RAM copy process to BL31 startup.
#191587	OP-TEE OS	Fix the MMU configuration of shared memory.
#190510	OP-TEE OS	Merge the following pull request. https://github.com/renesas-rcar/optee_os/pull/2
#195670	OP-TEE OS	Change a cipher method of AES-CTR from a block cipher to a stream cipher.

3.26 v2.0.1(Internal)

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.1
OP-TEE OS	2.0.1
OP-TEE Driver	1.0.10

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#194870	ARM Trusted Firmware (BL31)	plat: rcar: BL31: Add SiP for getting board ID
#197735	ARM Trusted Firmware (BL31)	plat: rcar: BL31: Add support for M3 Ver.1.3/Ver.3.0
#202712	OP-TEE OS	plat-rcar: Fix initial value for RPC register of SPI/HyperFlashDriver
#201794	OP-TEE Driver	tee: optee: Modify duration of spinlock for list
#201717	OP-TEE Driver	tee: optee: Change wait to interruptible

3.27 v2.0.2

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.2
OP-TEE OS	2.0.2
OP-TEE Driver	1.0.10

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#209217	OP-TEE OS	core: Delete the modification used by enabling CFG_WITH_PAGER

3.28 v2.0.3

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.3
OP-TEE OS	2.0.2
OP-TEE Driver	1.0.10

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#210724	ARM Trusted Firmware (BL31)	plat: rcar: BL31: Change to restore timer counter value at resume
#211021	ARM Trusted Firmware (BL31)	plat: rcar: BL31: Add DBSC4 setting before self-refresh mode

3.29 v2.0.4

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.4
OP-TEE OS	2.0.4
OP-TEE Driver	1.0.10

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#214736	OP-TEE OS	core: Change error code of HW-Engine provider layer
#219684	OP-TEE OS	plat-rcar: Add mask processing of interrupt distribution CPU
#220070 #220310	OP-TEE OS	core: Fix the return value from HW-Engine provider different from expected value
#221920	ARM Trusted Firmware (BL31)	plat: rcar: BL31: Fix missing RCAR_SYSTEM_SUSPEND encapsulation

3.30 v2.0.6

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.6
OP-TEE OS	2.0.6
OP-TEE Driver	1.0.10

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	3f16662284a69fdec97b1712064be94d1fed7ae7	3.1.0

No.	Module	Description
#249996	OP-TEE OS	plat-rcar: Change check of load address and size of TA for Dynamic TA authentication

3.31 v3.0.0

The following table represents a revision of the software in this version.

Module	Revision
ARM Trusted Firmware (BL31)	2.0.6
OP-TEE OS	3.0.0
OP-TEE Driver	1.0.11

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	be4fa2e36f717f03ca46e574aa66f697a897d090	3.8.0

No.	Module	Description
#256203	OP-TEE OS	plat-rcar: Version up the base version of OP-TEE from 3.1.0 to 3.8.0 https://github.com/OP-TEE/optee_os Commit ID 023e33656e2c9557ce50ad63a98b2e2c9b51c118 [Tag:3.8.0]
#256203	OP-TEE OS	core: libcryptoengine: Update Provider with base version up of OP-TEE from 3.1.0 to 3.8.0
#256203	OP-TEE OS	plat-rcar: Change memory mapping function macro and add START_DLOG_OUTPUT for R-Car logging function
#256203	OP-TEE OS	plat-rcar: Change memory type of area for Rom API
#256203	OP-TEE OS	plat-rcar: Add exclusive control when calling Rom API
#256203	OP-TEE Driver	tee: optee: Added SMC of START DLOG OUTPUT to rcar_optee_init_debug_log()
#271460	OP-TEE OS	plat-rcar: Fix initial value for RPC register of SPI/HyperFlashDriver for M3
#271460	OP-TEE OS	lib: fix build issue when building for non-RCAR platform

3.32 v3.0.1

The following table represents a revision of the software in this version.

Module	Revision
Trusted Firmware-A (BL31)	3.0.0
OP-TEE OS	3.0.1
OP-TEE Driver	1.0.11

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	be4fa2e36f717f03ca46e574aa66f697a897d090	3.8.0

No.	Module	Description
#276250	OP-TEE OS	plat-rcar: Fix build issue of RPMB for RCAR platform
#275854	OP-TEE OS	core: Fixed a problem with the xtest 4002 TEE_ALG_AES_CBC_MAC_PKCS5 algorithm
#275853	OP-TEE OS	core: Fixed a problem with the DES algorithm of xtest 4002
#275848	OP-TEE OS	core: Fixed a hang when running xtest 1013 and 2002
#275855	OP-TEE OS	core: Fixed a problem with the xtest 4006 TEE_ALG_RSASSA_PKCS1_V1_5 algorithm
#275857	OP-TEE OS	core: Fixed a problem with the xtest 4006 TEE_ALG_SM2_DSA_SM3 algorithm
#275858	OP-TEE OS	core: Fixed a problem with xtest 4013
#275851	OP-TEE OS	core: Fixed a problem that the context data of xtest 4002 is not copied
#290681	OP-TEE OS	plat-rcar: Fix the judgment of first smc in tee_entr_fast()
#276359	OP-TEE OS	plat-rcar: Expand the heap size for OP-TEE core
#276638	OP-TEE OS	plat-rcar: Fix cording style and CWE pointed out
#293913	OP-TEE OS	core: libcryptoengine: Remove debug message of unused valuable
#296189	OP-TEE OS	core: libcryptoengine: Remove dead code
#296116	OP-TEE OS	core: fs_htree: Fix authenc_init() error path for HW-Engine
#293067	OP-TEE OS	plat-rcar: Add support for disabling direct mapping
#293072	OP-TEE OS	core: move static IRQC data to nexus memory
#290814	OP-TEE OS	plat-rcar: Move global valuables to nexus memory
#290814	OP-TEE OS	plat-rcar: Add rcar_nex_mutex_lock() and rcar_nex_mutex_unlock()
#290814	OP-TEE OS	plat-rcar: platform_config.h: Remove unused defines
#296933	OP-TEE OS	plat-rcar: Change initialization of set_rpc_clock_mode() to read-modify-write
#297635	OP-TEE OS	core: libcryptoengine: Add error case to error translation of HW-Engine PKA provider layer
#297641	OP-TEE OS	core: libcryptoengine: Add error case to error translation of HW-Engine provider layer
#298330	OP-TEE OS	core: libcryptoengine: Add RSA decrypt error of HW-Engine provider layer
#298642	OP-TEE OS	plat-rcar: Fix callback functions to call init program when Suspend to RAM for second time.
#298267	OP-TEE OS	core: Add product register to direct mapping area
#298311	OP-TEE OS	plat-rcar: Add masking process to set RPC register with read-modify -write
#290814	OP-TEE OS	plat-rcar: Add configurations to enable dynamic shared memory when CFG_VIRTUALIZATION=y
#285917	Trusted Firmware-A (BL31)	rcar_gen3: Version up the base version of Trusted Firmawre-A from v1.5 to v2.3 https://github.com/ARM-software/arm-trusted-firmware Commit ID 8ff55a9e14a23d7c7f89f52465bcc6307850aa33 [Tag: v2.3]
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: Fixed Makefile
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL31: Add SiP Service
#275289	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Remove CPG_CPGWPR redefinition
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Fix CPG registers redefinition
#283702	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Fix I2C operation
#285917	Trusted Firmware-	rcar_gen3: plat: BL31: Add a check not to stop a boot CPU

	A (BL31)	
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL31: Change the migrate information for OP-TEE
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Delete enabling interrupt of SGIs, PPIs, and SPIs
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Change RAM protection configurations
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Enable the stack protection
293066	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL2/BL31: Add new board revision for Salvator-XS/H3ULCB
#299291	Trusted Firmware-A (BL31)	rcar_gen3: lib: psci: Fix a boot CPU check
#299128	Trusted Firmware-A (BL31)	rcar_gen3: lib: psci: Add clear process for psci_locks
#299487	Trusted Firmware-A (BL31)	rcar_gen3: plat: console: Fix a return value of console_rcar_init
#299128	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL31: Disable stack protector
#285917	Trusted Firmware-A (BL31)	rcar_gen3: plat: Update IPL and Secure Monitor Rev.3.0.0

3.33 v3.0.2

The following table represents a revision of the software in this version.

Module	Revision
Trusted Firmware-A (BL31)	3.0.1
OP-TEE OS	3.0.2
OP-TEE Driver	1.0.11

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	be4fa2e36f717f03ca46e574aa66f697a897d090	3.8.0

No.	Module	Description
#297399	OP-TEE OS	plat-rcar: Change register access method
#300902	OP-TEE OS	core: Add product register to direct mapping area when CFG_VIRTUALIZATION=y
#308248	OP-TEE OS	plat-rcar: Add support for D3
#312466	OP-TEE OS	plat-rcar: Change setting of CPG mask
#299487	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Add process to back up X6 and X7 register's value
#308925	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Modified operation register from SYSCISR to SYSCISCR
#304259	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Add SYSCEXTMASK bit set/clear in scu_power_up

3.34 v3.0.3

The following table represents a revision of the software in this version.

Module	Revision
Trusted Firmware-A (BL31)	3.0.2
OP-TEE OS	3.0.3
OP-TEE Driver	1.0.12

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	7c9c423d00e96bf51debd5fe10fd70dce83be5cc	3.13.0

No.	Module	Description
#317014	OP-TEE OS	plat-rcar: Version up the base version of OP-TEE from 3.8.0 to 3.13.0 https://github.com/OP-TEE/optee_os Commit ID 30c13f9e2ff178c9a299e409de75d50529cf5064 [Tag:3.13.0]
#322400	OP-TEE OS	plat-rcar: Remove access to SMSTPCR2 register
#297389	OP-TEE OS	plat-rcar: Fix the static analysis tools point out
#319884	OP-TEE OS	core: Add TEE_ALG_DES3_CMAC algorithm to case of HW-Engine provider layer
#317014	OP-TEE OS	plat-rcar: Remove the compile option defined in R-Car
#317014	OP-TEE OS	plat-rcar: Change the power saving function call
#317014	OP-TEE OS	core: entry_a64.S: Change to assembly macro
#317014	OP-TEE OS	libutee: Remove copying ae_tag_len in TEE_CopyOperation
#317014	OP-TEE OS	core: libcryptoengine: Add parameter check of key_size
#297389	OP-TEE OS	core: libcryptoengine: Fix integer overflow checks of HW acipher, hmac, aesmac
#319375	Trusted Firmware-A (BL31)	Version up the base version of arm-trusted-firmware. https://github.com/ARM-software/arm-trusted-firmware Commit ID 1e13c500a0351ac4b55d09a63f7008e2438550f8 [Tag: v2.5]
#304884	Trusted Firmware-A (BL31)	rcar_gen3: plat: BL31: Remove SiP Service
#299128	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Change process that copy code to system ram
#299128	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Remove compilation switch of stack protector canary function
#299128	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Change process for Suspend To RAM

3.35 v3.0.4

The following table represents a revision of the software in this version.

Module	Revision
Trusted Firmware-A (BL31)	3.0.3
OP-TEE OS	3.0.4
OP-TEE Driver	1.0.13

The following table represents a version of the OSS.

Module	Git Repository URL	Commit ID	Tags
OP-TEE Client	https://github.com/OP-TEE/optee_client.git	7c9c423d00e96bf51debd5fe10fd70dce83be5cc	3.13.0

No.	Module	Description
#340059	OP-TEE OS	core: Changed the suspend/resume sequence for R-Car
#335739	OP-TEE OS	plat-rcar: Fixed key data acquisition failure using Rom API
#337356	OP-TEE OS	core: libcryptoengine: Fixed a problem with the RSA key generation algorithm
#337350	OP-TEE OS	libutee: Fixed a problem with the TEE_ALG_AES_XCBC_MAC algorithm
#341212	OP-TEE OS	core: Changed the interrupt mask of suspend/resume sequence for R-Car
#336300	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Fix to bit operation for WUPMSKCA57/53
#336300	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Modify sequence for update value for WUPMSKCA57/53
#337987	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Modify type for Internal function argument
#340915	Trusted Firmware-A (BL31)	plat: BL31: Fix SYSTEM_OFF processing for R-Car D3
#343008	Trusted Firmware-A (BL31)	rcar-gen3: plat: BL31: Change stack size of BL31

4. Confirming the execution software components

When you confirm executing software components in this package, please follow the documents [1] .
The hardware environment is below.

- SoC
  R-Car H3/M3/M3N/E3/D3
- Board
  System Evaluation Board "Salvator-X"
  System Evaluation Board "Salvator-XS"
  System Evaluation Board "Ebisu"
  System Evaluation Board "Ebisu-4D"
  System Evaluation Board "Draak"

5. Restrictions

There is no restriction in this revision.

REVISION HISTORY	Security Board Support Package Release Note: Software

Rev.	Date	Description	
		Page	Summary
1.0.0	Sep. 30, 2015	—	New creation.
1.0.1	Nov. 23, 2015	1	1.2 References Updated Linux Interface Specification Yocto recipe Start-Up Guide.
		4	3.Changes between previous revision Updated changes between previous revision.
		6	5.Restrictions Updated the description of the contents are not supported in this revision.
1.0.2	Dec. 07, 2015	4	3.Change History The title was changed from “3.Changes between previous revision” to “3.Change History” 3.3 add history of v1.0.2.
1.0.3	Feb. 23, 2016	4	3.Change History 3.4 add history of v1.0.3.
1.0.4	Mar. 25, 2016	4	3.Change History 3.5 add history of v1.0.4. Add module revision list in each section.
		8	5.Restrictions Updated the description of the contents are not supported in this revision.
1.0.5	Apr. 27, 2016	1	1.1 Objectives Add platform ‘M3’. 1.2 References Updated Linux Interface Specification Yocto recipe Start-Up Guide. Add Security Board Support Package User's Manual.
		2	2.2 Software 2.2.1 ARM Trusted Firmware (BL31) 2.2.2 OP-TEE OS Add platform ‘M3’ in each section.
		6	3.Change History 3.6 add history of v1.0.5.
		7	4.Confirming the execution software components Add platform ‘M3’.
		8	5.Restrictions Updated the description (1) arm-trusted-firmware (BL31) V. restriction about LOG_LEVEL.
1.0.6	May 27, 2016	1	1.2 References Add description about revision of the references.
		7	3.Change History 3.7 add table of software revisions in security BSP package Rev1.0.6.
1.0.7	Jun. 30, 2016	7	3.Change History 3.8 add table of software revisions in security BSP package Rev1.0.7.
		9	5.Restrictions Removed restrictions in this revision (1)-I,III,IV,V and (2)-I.
1.0.8	Aug. 29, 2016	8	3.Change History 3.9 add table of software revisions in security BSP package Rev1.0.8.
		10	5.Restrictions Removed restrictions in this revision (1)-I and (2)-I,II.
1.0.9	Nov. 2, 2016	8	3.Change History 3.10 add history of v1.0.9.
1.0.10	Oct. 26, 2016	9	3.Change History 3.11 add history of v1.0.10.
1.0.11	Nov. 22, 2016	9	3.Change History

			3.11 add history of v1.0.11.
1.0.12	Jan. 13, 2017	10 11	3.Change History 3.12 add table of software revisions in security BSP package Rev1.0.11.
		13	5.Restrictions Added the description (1) arm-trusted-firmware (BL31) I. restriction about SYSTEM_OFF. Removed restrictions in this revision (3). Add restrictions in this revision (2)-II, III.
1.0.13	Mar. 15, 2017	11	3.Change History 3.14 add history of v1.0.13.
		13	5.Restrictions Deleted the Log output restrictions. Added the Debug log (Linux terminal output) restrictions.
1.0.14	Apr. 14, 2017	11	3.Change History 3.15 add history of v1.0.14.
1.0.15	May. 17, 2017	13	3.Change History 3.16 add history of v1.0.15.
1.0.16	Aug. 24, 2017	—	Fixed the format of the document (trademark, etc.)
		14	3.Change History 3.17 add history of v1.0.16.
		15	4. Confirming the execution software components Add "Salvator-XS" to Board.
1.0.17	Nov. 14, 2017	1	1.1 Objectives Add platform ‘M3N’.
		2	2.2 Software 2.2.1 ARM Trusted Firmware (BL31) 2.2.2 OP-TEE OS Add platform ‘M3N’ in each section.
		15	3.Change History 3.18 add history of v1.0.17.
		16	4.Confirming the execution software components Add platform ‘M3N’.
1.0.18	Jan. 12, 2018	—	Fixed the format of the document(trademark, etc.)
		16	3.Change History 3.19 add history of v1.0.18
		18	5. Restrictions Removed the restriction of the DRAM training of the OP-TEE OS. Add Secure storage using RPMB Filesystem is restrictions. Change the Debug log (Linux terminal output) restrictions.
1.0.19	Mar. 14, 2018	1	1.1 Objectives Add platform ‘E3’.
		2	2.2 Software 2.2.1 ARM Trusted Firmware (BL31) 2.2.2 OP-TEE OS Add platform ‘E3’ in each section.
		17	3.Change History 3.20 add history of v1.0.19
		18	4.Confirming the execution software components Add platform ‘E3’. Add "Ebisu" to Board.
		19	5. Restrictions Change Secure storage using RPMB Filesystem is restrictions.
1.0.20	Apr. 11, 2018	2	2.1 Software components 2.2.3 OP-TEE Driver Change the from OP-TEE Linux Driver to OP-TEE Driver.
		14	3.17 v1.0.16 Change the Description of #130795.

		18	3.Change History 3.21 add history of v1.0.20
1.0.21	Jun. 11, 2018	19	3.Change History 3.22 add history of v1.0.21
1.0.22	Sep. 3, 2018	20	3.Change History 3.23 add history of v1.0.22
1.0.23	Oct. 12, 2018	21	3.Change History 3.24 add history of v1.0.23
		22	4.Confirming the execution software components Add "Ebisu-4D" to Board.
2.0.0	Nov. 26, 2018	—	Fixed the format of the document (Address List.)
		21	3.Change History 3.24 add #190194 and #190112 to the history of v1.0.23
		22	3.Change History 3.25 add history of v2.0.0
		24	Removed restrictions from this revision (1)-I, (2)-II and moved the description to Security Board Support Package User's Manual.
2.0.1(Internal)	Feb. 15, 2019	23	3.Change History 3.26 add history of v2.0.1(Internal)
2.0.2	Mar. 11, 2019	24	3.Change History 3.27 add history of v2.0.2
2.0.3	Mar. 22, 2019	25	3.Change History 3.28 add history of v2.0.3
		27	5.Restrictions Change the description of the eMMC device about restrictions of RPMB file system. Add a work-around about restrictions of Secure storage using RPMB Filesystem.
2.0.4	Jul. 12, 2019	26	3.Change History 3.29 add history of v2.0.4
		28	5.Restrictions Removed the restriction of Secure storage using RPMB Filesystem.
2.0.6	Feb. 9, 2020	27	3.Change History 3.30 add history of v2.0.6
3.0.0	Jun. 12, 2020	28	3.Change History 3.31 add history of v3.0.0
		30	5.Restrictions Add the restriction of RPMB Filesystem, MFIS Driver, setting of build option, R-Car logging fucntion and repeating executing optee_test.
3.0.1	Dec. 11, 2020	2	Changed the software name from ARM Trusted Firmware to Trusted Firmware-A.
		29 30 31	3.Change History 3.32 add history of v3.0.1
		33	5.Restrictions
3.0.2	Apr. 6, 2021	1	1.1 Objectives Add platform ‘D3’.
		2	2.2 Software 2.2.1 ARM Trusted Firmware (BL31) 2.2.2 OP-TEE OS Add platform ‘D3’ in each section.
		2	2.2.1 ARM Trusted Firmware (BL31) 2.2.2 OP-TEE OS Changed ARM notation to Arm.
		32	3.Change History 3.33 add history of v3.0.2
		33	4.Confirming the execution software components Add platform ‘D3’. Add "Draak" to Board.

		34	5.Restrictions Removed the core dump limit when running xtest with virtualization enabled on M3N.
3.0.3	Aug. 16, 2021	—	Fixed the format of the document (Notice, Address List.)
		—	Add information of Gen3e.
		33	3.Change History 3.34 add history of v3.0.3
		35	5.Restrictions Change the description of restrictions to tabular format.
3.0.4	Dec, 1, 2021	34	3.Change History 3.35 add history of v3.0.4
		36	5.Restrictions Removed following restrictions and moved the description to Security Board Support Package User's Manual. ・The limit when executing multiple processes in parallel. ・The restrictions of virtualization environment.

CONFIDENTIAL

Security Board Support Package Release Note: Software

Publication Date: Rev.1.0.0 Sep. 30, 2015
Rev.3.0.4 Dec. 1, 2021

Published by: Renesas Electronics Corporation

SALES OFFICES

Renesas Electronics Corporation

http://www.renesas.com

Refer to "http://www.renesas.com/" for the latest and detailed information.

Renesas Electronics Corporation
TOYOSU FORESIA, 3-2-24 Toyosu, Koto-ku, Tokyo 135-0061, Japan

Renesas Electronics America Inc. Milpitas Campus
1001 Murphy Ranch Road, Milpitas, CA 95035, U.S.A.
Tel: +1-408-432-8888, Fax: +1-408-434-5351

Renesas Electronics America Inc. San Jose Campus
6024 Silver Creek Valley Road, San Jose, CA 95138, USA
Tel: +1-408-284-8200, Fax: +1-408-284-2775

Renesas Electronics Canada Limited
9251 Yonge Street, Suite 8309 Richmond Hill, Ontario Canada L4C 9T3
Tel: +1-905-237-2004

Renesas Electronics Europe GmbH
Arcadiastrasse 10, 40472 Düsseldorf, Germany
Tel: +49-211-6503-0, Fax: +49-211-6503-1327

Renesas Electronics (China) Co., Ltd.
Room 101-T01, Floor 1, Building 7, Yard No. 7, 8th Street, Shangdi, Haidian District, Beijing 100085, China
Tel: +86-10-8235-1155, Fax: +86-10-8235-7679

Renesas Electronics (Shanghai) Co., Ltd.
Unit 301, Tower A, Central Towers, 555 Langao Road, Putuo District, Shanghai 200333, China
Tel: +86-21-2226-0888, Fax: +86-21-2226-0999

Renesas Electronics Hong Kong Limited
Unit 1601-1611, 16/F., Tower 2, Grand Century Place, 193 Prince Edward Road West, Mongkok, Kowloon, Hong Kong
Tel: +852-2265-6688, Fax: +852 2886-9022

Renesas Electronics Taiwan Co., Ltd.
13F, No. 363, Fu Shing North Road, Taipei 10543, Taiwan
Tel: +886-2-8175-9600, Fax: +886 2-8175-9670

Renesas Electronics Singapore Pte. Ltd.
80 Bendemeer Road, #06-02 Singapore 339949
Tel: +65-6213-0200, Fax: +65-6213-0300

Renesas Electronics Malaysia Sdn.Bhd.
Unit No 3A-1 Level 3A Tower 8 UOA Business Park, No 1 Jalan Pengaturcara U1/51A, Seksyen U1, 40150 Shah Alam, Selangor, Malaysia
Tel: +60-3-5022-1288, Fax: +60-3-5022-1290

Renesas Electronics India Pvt. Ltd.
No.777C, 100 Feet Road, HAL 2nd Stage, Indiranagar, Bangalore 560 038, India
Tel: +91-80-67208700

Renesas Electronics Korea Co., Ltd.
17F, KAMCO Yangjae Tower, 262, Gangnam-daero, Gangnam-gu, Seoul, 06265 Korea
Tel: +82-2-558-3737, Fax: +82-2-558-5338

Colophon 7.0

ルネサス エレクトロニクス株式会社

■営業お問合せ窓口

http://www.renesas.com

※営業お問合せ窓口の住所は変更になることがあります。最新情報につきましては、弊社ホームページをご覧ください。

ルネサス エレクトロニクス株式会社 〒135-0061 東京都江東区豊洲3-2-24（豊洲フォレシア）

■技術的なお問合せおよび資料のご請求は下記へどうぞ。
総合お問合せ窓口：https://www.renesas.com/contact/

Colophon 3.1

Security Board Support Package Release Note

Renesas Electronics Corporation