[Notes]

RX Family

RSIP(Renesas Secure IP) Module Protected Mode Firmware Integration Technology

R20TS1193EJ0100
Rev.1.00
Nov. 20, 2015

Outline

When using the product in the title, note the following points.

1. Caution when to use KDF-SHA256 function
   (1) Caution about input message length
   (2) Caution about behavior of specific input message length

1. Caution when to use KDF-SHA256 function

1.1 Applicable Products

- RSIP (Renesas Secure IP) Module Protected Mode Firmware Integration Technology (RSIP PM driver)

The applicable revision number and document number are as follows.

Table 1 RSIP PM driver Applicable Product

Revision of the RSIP PM driver	Document number
Rev.2.00	R20AN0748xx0200

- RX Driver Package

The RSIP PM driver in above is also included in the RX Driver Package products.
The product name and revision number of the applicable RX Driver Package and the revision number and document of the included RSIP PM driver are as follows.

Table 2 Product Which includes the RSIP PM driver

Product name of the RX Driver Package	Revision of the RX Driver Package	Document number	Revision of the included RSIP PM driver
RX Driver Package for RX Family, Ver.1.48	Rev.1.48	R01AN8121xx0148	Rev.2.00

1.2 Applicable Devices

RX261 group

1.3 Details

(1) In case of using KDF-SHA256 APIs (R_RSIP_KDF_SHA_Init()/_Update()/_Finish()), R_RSIP_KDF_SHA_Update() returns with FSP_ERR_INVALID_SIZE error when the input message length is more than 65 bytes.

(2) In case of using KDF-SHA256 APIs (R_RSIP_KDF_SHA_Init()/_Update()/_Finish()), the value of the wrapped DKM (p_wrapped_dkm) is invalid when the input message length is 55 bytes.

1.4 Conditions

(1) The behavior occurs when the condition matches either of the below.

- When the argument message_length of R_RSIP_KDF_SHA_Update() which is used to specify input message length is set to more than 65.
- In case of R_RSIP_KDF_SHA_Update() is called multiple times, when sum of the message_length becomes more than 65.

(2) The behavior occurs when the condition matches either of the below.

- In case of R_RSIP_KDF_SHA_Update() is called only once, when the argument message_length which is used to specify input message length is set to 55.
- In case of R_RSIP_KDF_SHA_Update() is called multiple times, when sum of the message_length becomes 55.

1.5 Workaround

There is no workaround.

1.6 Schedule for Revising the Items

These items will be revised in the next version.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Nov.20.25	-	First edition issued

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

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/

TS Colophon 4.3