[Revisions to Documents]
RX Family
RSIP(Renesas Secure IP) Module Protected Mode Firmware Integration Technology Rev.2.01

R20TS1234EJ0100
Rev.1.00
Apr. 20, 2026

Outline

RX Family RSIP(Renesas Secure IP) Module Protected Mode Firmware Integration Technology Application Note Rev.2.00 and Rev.2.01 have been corrected.

1. Applicable Documents

RX Family RSIP(Renesas Secure IP) Module Protected Mode Firmware Integration Technology Application Note, R20AN0748xj0200, Rev.2.00

RX Family RSIP(Renesas Secure IP) Module Protected Mode Firmware Integration Technology Application Note, R20AN0748xj0201, Rev.2.01

2. Errata

2.1 4.2.8.2 R_RSIP_RFC3394_KeyUnwrap, Description

Correct:

This API unwraps a key with an RFC3394-compliant algorithm.

It unwraps p_rfc3394_wrapped_target_key with the key specified in p_wrapped_kek. The unwrapped key is output to p_wrapped_target_key in the wrapped key format. For type field of p_wrapped_target_key, specify the value defined in Table 2-4※. The available value is AES128bit key or AES256bit key.

For p_ctrl, specify the pointer to the management structure used in the R_RSIP_Open() function.

Note: Table 2-4 is described in section 2.9 in the Application Note.

Incorrect:

This API unwraps a key with an RFC3394-compliant algorithm.

It unwraps p_rfc3394_wrapped_target_key with the key specified in p_wrapped_kek. The unwrapped key is output to p_wrapped_target_key in the wrapped key format. For key_type, specify the type of key to be unwrapped.

For p_ctrl, specify the pointer to the management structure used in the R_RSIP_Open() function.

2.2 4.2 Detailed Descriptions of API Functions, Format of each API

A list of errata to the format parts in each section of 4.2 Detailed Descriptions of API Functions is described below.

Correct	Incorrect	Memo
4.2.4.4 R_RSIP_AES_AEAD_Init #include fsp_err_t R_RSIP_AES_AEAD_Init(rsip_ctrl_t * const p_ctrl, **rsip_aes_aead_mode_t** mode, rsip_wrapped_key_t * const p_wrapped_key, uint8_t const * const p_nonce, uint32_t const nonce_length)	4.2.4.4 R_RSIP_AES_AEAD_Init #include fsp_err_t R_RSIP_AES_AEAD_Init(rsip_ctrl_t * const p_ctrl, **rsip_aes_aead_mode_t const** mode, rsip_wrapped_key_t * const p_wrapped_key, uint8_t const * const p_nonce, uint32_t const nonce_length)	Changed type of mode parameter
4.2.6.6 R_RSIP_SHA_Resume #include fsp_err_t R_RSIP_SHA_Resume(rsip_ctrl_t * const p_ctrl, **rsip_sha_handle_t const * const** p_handle)	4.2.6.6 R_RSIP_SHA_Resume #include fsp_err_t R_RSIP_SHA_Resume(rsip_ctrl_t * const p_ctrl, **rsip_sha_handle_t * const** p_handle)	Changed type of p_handle parameter
4.2.6.7 R_RSIP_HMAC_Compute #include fsp_err_t R_RSIP_HMAC_Compute(rsip_ctrl_t * const p_ctrl, **const rsip_wrapped_key_t *** p_wrapped_key, uint8_t const * const p_message, uint32_t const message_length, uint8_t * const p_mac)	4.2.6.7 R_RSIP_HMAC_Compute #include fsp_err_t R_RSIP_HMAC_Compute(rsip_ctrl_t * const p_ctrl, **rsip_wrapped_key_t const * const** p_wrapped_key, uint8_t const * const p_message, uint32_t const message_length, uint8_t * const p_mac)	Changed type of p_wrapped _key parameter
4.2.6.8 R_RSIP_HMAC_Verify #include fsp_err_t R_RSIP_HMAC_Verify(rsip_ctrl_t * const p_ctrl, **const rsip_wrapped_key_t *** p_wrapped_key, uint8_t const * const p_message, uint32_t const message_length, uint8_t * const p_mac)	4.2.6.8 R_RSIP_HMAC_Verify #include fsp_err_t R_RSIP_HMAC_Verify(rsip_ctrl_t * const p_ctrl, **rsip_wrapped_key_t const * const** p_wrapped_key, uint8_t const * const p_message, uint32_t const message_length, uint8_t * const p_mac)	Changed type of p_wrapped _key parameter
4.2.8.2 R_RSIP_RFC3394_KeyUnwrap #include fsp_err_t R_RSIP_AES_AEAD_Init(rsip_ctrl_t * const p_ctrl, rsip_wrapped_key_t const * const p_wrapped_kek	4.2.8.2 R_RSIP_RFC3394_KeyUnwrap #include fsp_err_t R_RSIP_AES_AEAD_Init(rsip_ctrl_t * const p_ctrl,	Deleted key_type parameter

uint8_t const * const p_rfc3394_wrapped_target_key, rsip_wrapped_key_t * const p_wrapped_target_key)	rsip_wrapped_key_t const * const p_wrapped_kek, **rsip_key_type_t const key_type,** uint8_t const * const p_rfc3394_wrapped_target_key, rsip_wrapped_key_t * const p_wrapped_target_key)	The key_type is also deleted in Parameter part.

2.3 4.1 List of APIs

In 4.1 List of APIs, added the caution when using API.

Although the code for the following APIs exists in C source files, these APIs are not supported in RX261 RSIP Protected Mode Rev.2.00 and Rev.2.01. Therefore, they cannot be used.

R_RSIP_PureEdDSA_Sign
R_RSIP_PureEdDSA_Verify
R_RSIP_KDF_HMAC_DKMKeyImport
R_RSIP_KDF_HMAC_ECDHSecretKeyImport
R_RSIP_KDF_HMAC_Init
R_RSIP_KDF_HMAC_DKMUpdate
R_RSIP_KDF_HMAC_ECDHSecretUpdate
R_RSIP_KDF_HMAC_Update
R_RSIP_KDF_HMAC_SignFinish
R_RSIP_KDF_HMAC_Suspend
R_RSIP_KDF_HMAC_Resume
R_RSIP_OTF_Init
R_RSIP_RSA_Encrypt
R_RSIP_RSA_Decrypt
R_RSIP_RSAES_PKCS1_V1_5_Encrypt
R_RSIP_RSAES_PKCS1_V1_5_Decrypt
R_RSIP_RSAES_OAEP_Encrypt
R_RSIP_RSAES_OAEP_Decrypt
R_RSIP_RSASSA_PKCS1_V1_5_Sign
R_RSIP_RSASSA_PKCS1_V1_5_Verify
R_RSIP_RSASSA_PSS_Sign
R_RSIP_RSASSA_PSS_Verify
R_RSIP_PKI_RSASSA_PKCS1_V1_5_CertVerify
R_RSIP_PKI_RSASSA_PSS_CertVerify

3. Schedule for Document Improvements

The above correction will be reflected in the next revision.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Apr.20.26	-	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