【ドキュメント修正】
RX ファミリ
RSIP(Renesas Secure IP)モジュール Protected Mode Firmware Integration Technology Rev.2.01

R20TS1234JJ0100
Rev.1.00
2026.04.20

概要

RX ファミリ RSIP(Renesas Secure IP)モジュール Protected Mode Firmware Integration Technology アプリケーションノート Rev.2.00, Rev.2.01 の訂正を連絡します。

1. 対象ドキュメント

RX ファミリ RSIP(Renesas Secure IP)モジュール Protected Mode Firmware Integration Technology アプリケーションノート、R20AN0748xj0200、Rev.2.00

RX ファミリ RSIP(Renesas Secure IP)モジュール Protected Mode Firmware Integration Technology アプリケーションノート、R20AN0748xj0201、Rev.2.01

2. 改訂個所

2.1 4.2.8.2 R_RSIP_RFC3394_KeyUnwrap、Description

正：

RFC3394 に準拠したアルゴリズムで鍵をアンラップします。

p_wrapped_kek で指定した鍵を使用して、p_rfc3394_wrapped_target_key をアンラップします。アンラップされた鍵は Wrapped Key で p_wrapped_target_key に出力されます。p_wrapped_target_key の type フィールドには表 2-4※に定義される値からアンラップされる鍵の種類を指定してください。指定できる鍵の種類は、AES128bit 鍵または AES256bit 鍵です。

p_ctrl には、R_RSIP_Open()関数で使用した管理構造体のポインタを指定します。

※表 2-4 はアプリケーションノート 2.9 章に記載されています。

誤：

RFC3394 に準拠したアルゴリズムで鍵をアンラップします。

p_wrapped_kek で指定した鍵を使用して、p_rfc3394_wrapped_target_key をアンラップします。アンラップされた鍵は Wrapped Key で p_wrapped_target_key に出力されます。key_type にアンラップされる鍵の種類を指定してください。

p_ctrl には、R_RSIP_Open()関数で使用した管理構造体のポインタを指定します。

2.2 4.2 API 詳細、各 API の Format

4.2 API 詳細の各 API の章において、Format の記載に誤りのある章と該当箇所を以下の表に示します。

正	誤	備考
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)	引数 mode の型の変更
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)	引数 p_handle の型の変更
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)	引数 p_wrapped _key の型の変更
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)	引数 p_wrapped _key の型の変更
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,	引数 key_type の削除

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)	Parameters においても key_type の説明は削除

2.3 4.1 API 一覧

4.1 API 一覧について、注意事項を追加します。

以下 API は C ソースファイルにコードが存在していますが、RX261 RSIP Protected Mode Rev.2.00 もしくは Rev.2.01 では、未サポートの API です。使用することはできません。

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. ドキュメント改善計画

本訂正内容については、次回改版時に反映予定です。

以上

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	Apr.20.26	-	新規発行

本社所在地

〒135-0061 東京都江東区豊洲 3-2-24（豊洲フォレシア）

www.renesas.com

お問合せ窓口

弊社の製品や技術、ドキュメントの最新情報、最寄の営業お問合せ窓口に関する情報などは、弊社ウェブサイトをご覧ください。

www.renesas.com/contact/