【注意事項】
RX ファミリ
RSIP(Renesas Secure IP)モジュール Protected Mode Firmware Integration Technology

R20TS1193JJ0100
Rev.1.00
2025.11.20

概要

タイトルに記載している製品の使用上の注意事項を連絡します。

1. KDF-SHA256 に関する注意事項
   (1) 入力メッセージ長に関する注意事項
   (2) 特定の入力メッセージ長を入力した際の動作に関する注意事項

1. KDF-SHA256 機能に関する注意事項

1.1 該当製品

- RSIP(Renesas Secure IP)モジュール Protected Mode Firmware Integration Technology（RSIP PM ドライバ）

該当するリビジョンおよびドキュメントは、以下のとおりです。

表 1　RSIP PM ドライバ該当製品一覧

RSIP PM ドライバのリビジョン	資料番号
Rev.2.00	R20AN0748JJ0200

- RX Driver Package

上記の RSIP PM ドライバは、RX Driver Package にも同梱されています。

該当する RX Driver Package の製品名、リビジョン、および同梱している RSIP PM ドライバのリビジョンおよびドキュメントは、以下のとおりです。

表 2　RSIP PM ドライバ同梱製品一覧

RX Driver Package の製品名	RX Driver Package のリビジョン	資料番号	同梱している RSIP PM ドライバのリビジョン
RX ファミリ RX Driver Package Ver.1.48	Rev.1.48	R01AN8121xx0148	Rev.2.00

1.2 該当デバイス

RX261 グループ

1.3 内容

(1) KDF-SHA256 の演算を行う API(R_RSIP_KDF_SHA_Init()/_Update()/_Finish())では、入力するメッセージ長が 65 バイト以上の場合、R_RSIP_KDF_SHA_Update()は FSP_ERR_INVALID_SIZE エラーを返します。

(2) KDF-SHA256 の演算を行う API(R_RSIP_KDF_SHA_Init()/_Update()_Finish())では、入力するメッセージ長が 55 バイトの場合、R_RSIP_KDF_SHA_Finish()から出力されるラップした DKM(p_wrapped_dkm から出力される値)が不正な値になります。

1.4 発生条件

(1) 以下のどちらかの条件に該当する場合、発生します。

- R_RSIP_KDF_SHA_Update()のメッセージ長を指定する引数 message_length に 65 以上を指定した場合
- R_RSIP_KDF_SHA_Update()を複数回呼び出す場合、入力した message_length の合計が 65 以上になる場合。

(2) 以下のどちらかの条件に該当する場合、発生します。

- R_RSIP_KDF_SHA_Update()を 1 回だけ呼び出す場合、メッセージ長を指定する引数 message_length に 55 を指定した場合。
- R_RSIP_KDF_SHA_Update()を複数回呼び出す場合、入力した message_length の合計が 55 になる場合。

1.5 回避策

回避策はありません。

1.6 恒久対策

次期バージョンで改修予定です。

以上

改訂記録

Rev.	発行日	改訂内容	
		ページ	ポイント
1.00	Nov.20.25	-	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/

商標について

ルネサスおよびルネサスロゴはルネサス エレクトロニクス株式会社の商標です。すべての商標および登録商標は、それぞれの所有者に帰属します。

TS Colophon 4.3