Date: Jul. 4, 2024

RENESAS TECHNICAL UPDATE

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

Product Category	MPU/MCU		Document No.	TN-RA*-A0116A/E	Rev.	1.00
Title	Notes on Usage of Secure Cryptographic Engine (SCE5)		Information Category	Technical Notification		
Applicable Product	RA4M1 Group, RA4W1 Group, RA6T2 Group	Lot No. All	Reference Document	Refer the table at the end of this document		

This document is to notify users of malfunction observed in operations of Secure Cryptographic Engine (SCE5), and the following events may occur.
If the following conditions are met, the measures described in Workaround should be applied.

Occurrence Condition

The event occurs in the following case 1) or 2).
The number in parentheses () is the related chapter number of FSP User's Manual.

1) In operations using AES keys with a key length of 256 bits, or in AES CCM or XTS operations,
In case of using Hardware Acceleration in any of the following modules

- Azure RTOS NetX Crypto HW Acceleration / rm_netx_secure_crypto (chapter 5.2.15.2)
- Mbed Crypto H/W Acceleration / rm_psa_crypto (chapter 5.2.15.3)

2) In case of injecting or updating AES key with a key length of 256 bits using the following modules

- Secure Key Injection / r_sce_key_injection (chapter 5.2.15.7)

Occurrence event

In case of the CCM operation condition is met
Message authentication passes, but some blocks of encrypted data may not be successfully decrypted.

In case of an operation of AES key with a key length of 256 bits or operation of XTS operation condition is met
An incorrect operation may be performed when unwrapping AES key used for the crypt operation, then the operation may be performed with an illegal AES key.

In case of injecting or updating AES key with a key length of 256 bits
An incorrect operation may be performed when wrapping AES key, then the unwrapping AES key for AES operation may differ from the original AES key.
Alternatively, an error may occur in the AES key unwrap for AES operation.

Workaround

Renesas Flexible Software Package(FSP) v5.2.0 or later should be used.

(c) 2024. Renesas Electronics Corporation. All rights reserved.

Reference Document Table

Product	Document name
RA4M1 Group	Renesas RA4M1 Group User's Manual: Hardware Rev.1.10
RA4W1 Group	Renesas RA4W1 Group User's Manual: Hardware Rev.1.00
RA6T2 Group	Renesas RA6T2 Group User's Manual: Hardware Rev.1.40
Renesas Flexible Software Package (FSP)	Renesas Flexible Software Package (FSP) v5.1.0 User's Manual