Date: Apr. 17, 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-RX*-A0277A/E	Rev.	1.00
Title	Notes on Usage of the Trusted Secure IP Lite (TSIP-Lite) Module		Information Category	Technical Notification		
Applicable Product	RX231 Group, RX23W Group, RX26TGroup, RX66T Group, RX72T Group	Lot No. All	Reference Document	User's Manual: Hardware for applicable products listed under Reference Documents on the last page		

This document is to notify users of malfunctions observed in operations of the trusted secure IP lite (TSIP-Lite) module.

1. Note

Using the trusted secure IP lite (TSIP-Lite) module to handle CCM operations, or the injection or updating of a 256-bit AES key may, depending on the timing, cause the following malfunctions on rare occasions.

(1) Malfunction in the CCM Operations

Certain blocks may not be successfully decrypted despite a pass having been received in the message authentication. Specifically, this malfunction may occur when the following functions of the TSIP driver are used.

R_TSIP_Aes128CcmDecryptUpdate

R_TSIP_Aes256CcmDecryptUpdate

(2) Malfunction in the Injection or Updating of a 256-bit AES Key

Operation for the wrapping of an AES key may be faulty. This may lead to an error in the unwrapping of a key during AES operations, or to the generation of a key that is not the same as the original key. Specifically, this malfunction may occur when the following functions of the TSIP driver are used.

R_TSIP_GenerateUpdateKeyRingKeyIndex

R_TSIP_GenerateAes256KeyIndex

R_TSIP_UpdateAes256KeyIndex

2. Workaround

Use ver.1.20 or a later version of the TSIP driver to avoid these malfunctions.

3. Reference Documents

Group	Manual Name	Rev.	Document Number
RX26T Group	RX26T Group User's Manual: Hardware	Rev.1.10	R01UH0979EJ0110
RX230 Group, RX231 Group	RX230 Group, RX231 Group User's Manual: Hardware	Rev.1.20	R01UH0496EJ0120
RX23W Group	RX23W Group User's Manual: Hardware	Rev.1.10	R01UH0823EJ0110
RX66T Group	RX66T Group User's Manual: Hardware	Rev.1.30	R01UH0749EJ0130
RX72T Group	RX72T Group User's Manual: Hardware	Rev.1.10	R01UH0803EJ0110