Date: Apr. 3, 2020

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*-A0223A/E	Rev.	1.00
Title	Addition to the Trusted Secure IP (TSIP) Specifications in RX Family Devices		Information Category	Technical Notification		
Applicable Product	RX72M Group RX65N Group, RX651 Group	Lot No.	Reference Document	RX72M Group User's Manual: Hardware Rev.1.00 (R01UH0804EJ0100) RX65N Group, RX651 Group User's Manual: Hardware Rev.2.30 (R01UH0590EJ0230)		

The specifications for elliptic curve cryptography (ECC) by the Trusted Secure IP (TSIP) of the applicable products listed above have been disclosed.

The TSIP specifications after the ECC disclosure are as follows.

Table 1. Specifications of Trusted Secure IP (1 / 2)

Item	Description
Access control	Access management circuit ● In case of irregular access to the Trusted Secure IP due to a falsified program or runaway execution of a program, this circuit blocks all subsequent access and stops the output of data from the Trusted Secure IP.
Encryption engine	AES: Compliant with NIST FIPS PUB 197 algorithm ● Key sizes: 128, 192, or 256 bits ● Block sizes: 128 bits ● Block cipher mode of operation ECB, CBC, CTR: Compliant with NIST SP 800-38A CMAC: Compliant with NIST SP 800-38B CCM: Compliant with NIST SP 800-38C GCM: Compliant with NIST SP 800-38D XTS: Compliant with NIST SP 800-38E GCTR ● Number of cycles for execution*1 ECB, CBC, CTR, CMAC, GCTR, XTS: 11 cycles of PCLKB for 128-bit keys, 13 cycles of PCLKB for 192-bit keys, 15 cycles of PCLKB for 256-bit keys CCM: 22 cycles of PCLKB for 128-bit keys, 26 cycles of PCLKB for 192-bit keys, 30 cycles of PCLKB for 256-bit keys AES-GCM ● AES-GCM is realized by combining AES-GCTR and GHASH. RSA ● Key sizes: Up to 2048 bits ● Block sizes: Up to 2048 bits ● Number of cycles for execution: Approximately 1,300,000 cycles of PCLKB when the CRT is used*1 TDES ● Key sizes: 56 bits, 2 × 56 bits, or 3 × 56 bits ● Block sizes: 64 bits ● Block cipher mode of operation: ECB, CBC ● Number of cycles for execution*1 16 cycles of PCLKB for 56-bit keys, 32 cycles of PCLKB for 2 × 56-bit keys, 48 cycles of PCLKB for 3 × 56-bit keys ARC4 ● Key sizes: 2048 bits ● Block sizes: 128 bits ● Number of cycles for execution: 16 cycles of PCLKB*1

Table 1. Specifications of Trusted Secure IP (2 / 2)

Item	Description
Encryption engine	HASH Support for SHA1, SHA224/SHA256/MD5, GHASH ● Block sizes: 512bits ● Number of cycles for execution*[1] SHA1: 80 cycles of PCLKB SHA224/SHA256/MD5: 64 cycles of PCLKB GHASH: 9 cycles of PCLKB ECC ● Key sizes: Up to 256 bits ● Block sizes: 256 bits Key management ● Keys are only valid within the Trusted Secure IP. ● Only key generation information is output from the Trusted Secure IP. ● Keys can be regenerated by the input of key generation information to the Trusted Secure IP. Endian ● Big or little
Generation of random numbers	32-bit true random number generator ● The Trusted Secure IP library can assemble 32-bit true random numbers to generate 128- or 256-bit true random numbers. ● The generated 128-bit and 256-bit true random numbers are used as keys in encrypting and decrypting data.
Protection against illicit key copying	● An ID unique to the MCU (unique ID) is accessible from the access management circuit through the dedicated bus. ● Combining the unique ID with the key generation information prevents the illicit copying of the key to another MCU.
Supervisor mode	● The supervisor mode signal is connected to the access management circuit and is used to limit control of the Trusted Secure IP module to supervisor mode only.
Interrupt sources	11
Low power consumption	Setting of the module stop state is possible.

Note 1. This does not include the overhead for calling functions of the Trusted Secure IP library.