Date: Jun. 16, 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-RA*-A0004A/E	Rev.	1.00
Title	Errata for User's Manual: Hardware for SCE5		Information Category	Technical Notification		
Applicable Product	RA4M1 Group	Lot No. All	Reference Document	RA4M1 Group User's Manual Hardware Rev.1.00		

SCE5 is used in user mode and privileged mode. Therefore, the following descriptions should be deleted.

- In Table 46.1 SCE5 specifications, specification, Privileged mode: The privileged mode access signal is connected to the access management circuit and is used to limit control of the SCE5 module to privileged mode only.
- In Figure 46.1 SCE5 block diagram, Privileged mode access.

Table 46.1 SCE5 specifications

Item	Description
Access control	Access management circuit • In case of irregular access to the SCE5 due to a falsified program or runaway execution of a program, this circuit blocks all subsequent accesses and stops the output of data from the SCE5.
Encryption engine	Advanced Encryption Standard (AES): Compliant with NIST FIPS PUB 197 algorithm • Key sizes: 128 or 256 bits • Block size: 128 bits • Chaining modes - ECB, CBC, CTR: Compliant with NIST SP 800-38A - GCM: Compliant with NIST SP 800-38D - XTS: Compliant with NIST SP 800-38E. - GCTR • Throughput for 128-bit data - 44 PCLKA cycles for 128-bit key - 61 PCLKA cycles for 256-bit key. AES-GCM • AES-GCM is realized by combining AES-GCTR and GHASH. Key management • Wrapped keys are only valid within the SCE5.
Generation of random numbers	32-bit true random number generator
Unique ID	• 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 illicit copying of data to another MCU.
~~Privileged mode~~	~~• The privileged mode access signal is connected to the access management circuit and is used to limit control of the SCE5 module to privileged mode only.~~
Low power consumption	Setting of the module-stop state is possible

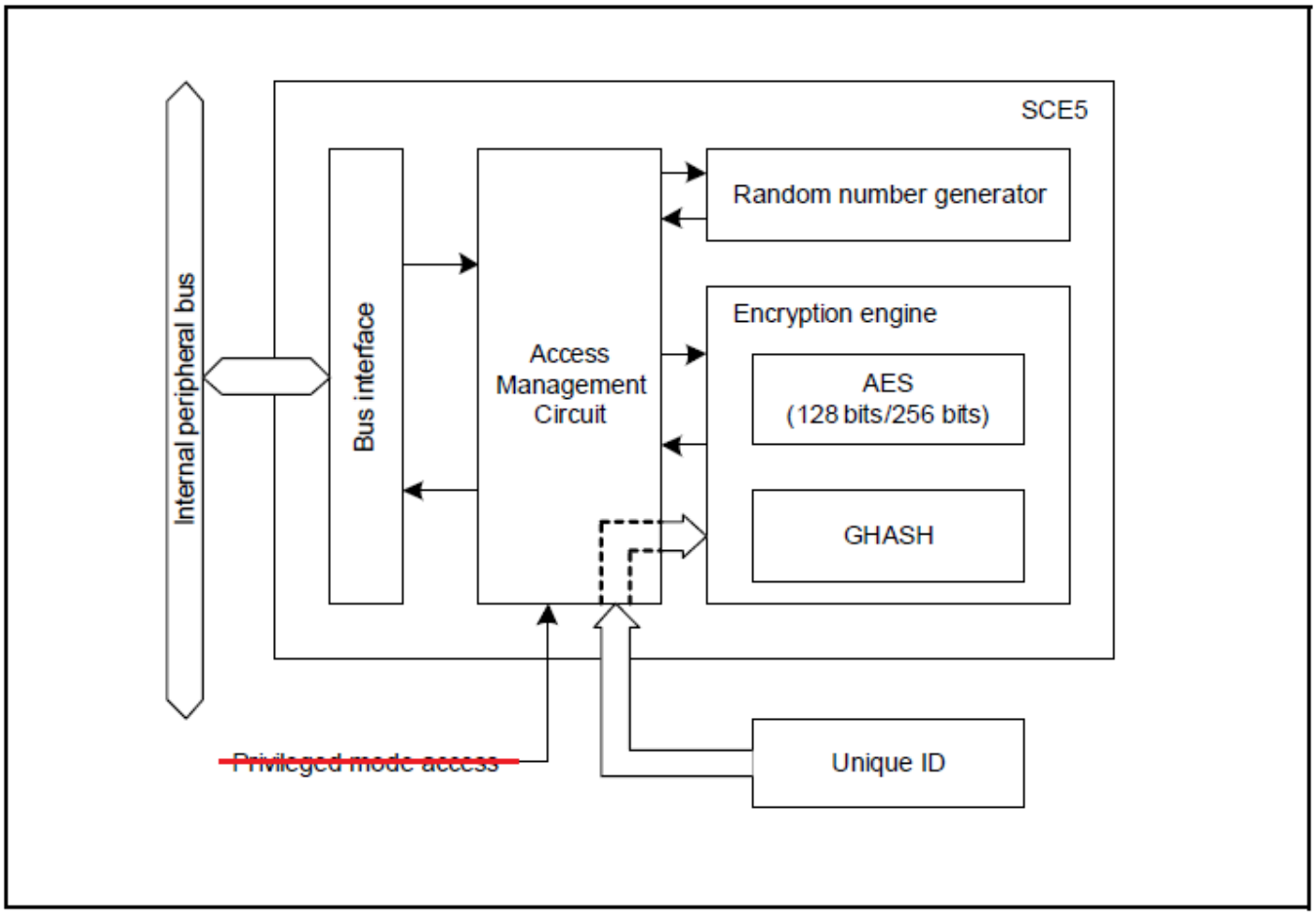

Figure 46.1 SCE5 block diagram