[Notes]
RX Family SHA Co-processor Driver,
Firmware Integration Technology

Overview

When using the products in the title, note the following point.

1. Notes on Using the SHA Operation API Function

1. Notes on Using the SHA Operation API Function

1.1 Applicable Products

RX family SHA co-processor driver module, Firmware Integration Technology

(RX SHA co-processor FIT module)

The applicable revision numbers and document numbers are as follows.

Table 1. RX SHA Co-processor FIT Module Applicable Products

Revision of the RX SHA co-processor FIT module	Document number
Rev.1.00	R20AN0354EJ0100
Rev.1.01	R20AN0354EJ0101

1.2 Applicable Devices

RX64M and RX71M groups

RENESAS

1.3   Description and Conditions

If all the following conditions are met, execution of API functions R_Sha1HashDigest(), R_Sha224HashDigest(), and R_Sha256HashDigest() does not end.

(a) Control flag R_SHA_FINISH is set.

(b) The total byte length of the message data leaves remainder 4 when divided by 64 (the length is, for example, 4, 68, 132…).

[Example 1] The following API function does not end.

```
ret = R_Sha1HashDigest
        (message, hash, 68, R_SHA_INIT | R_SHA_FINISH, work);
```

[Example 2] The second API function does not end because the total byte length of the message data is 68 and R_SHA_FINISH is specified.

```
ret = R_Sha1HashDigest
        (message, hash, 4, R_SHA_INIT, work);
ret = R_Sha1HashDigest
        (message, hash, 64, R_SHA_ADD | R_SHA_FINISH, work);
```

1.4   Workaround and Schedule for Fixing the Problem

The problem has been already rectified in Rev.1.02. Please use Rev.1.02.

Revision History

Rev.	Date	Description	
		Page	Summary
1.00	Nov.01.20	-	First edition issued

Corporate Headquarters

TOYOSU FORESIA, 3- 2- 24 Toyosu,

Koto-ku, Tokyo 135- 0061, Japan

www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:

www.renesas.com/contact/