

# Renesas Board ID™ Firmware

## Flexible and Secure Operating System for Authentication Applications

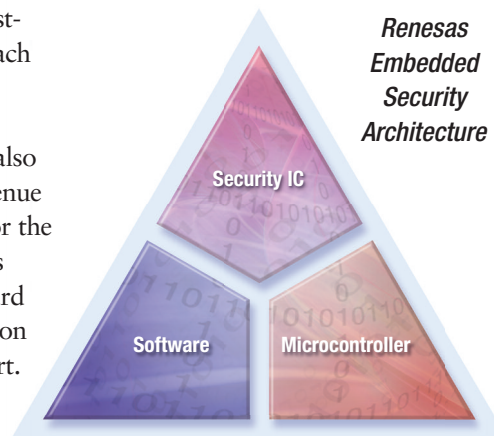


The Renesas Board ID chip is a cost-effective, easy-to-implement approach that drastically reduces risk in Machine-to-Machine (M2M) authentication applications, while also opening new opportunities for revenue generation. Designed specifically for the M2M market, the Board ID chip is based on Renesas' proven smart card IC technology and a solid foundation of technology, products and support. The powerful, tamper-proof architecture has highly secure cryptographic functions and the Board ID platform allows any MCU to be incorporated into the system, for maximum design flexibility.

Renesas' flexible architecture for M2M security facilitates new functions and processes. It offers significant benefits for business, industry, hospitals, government, consumers and other M2M markets.

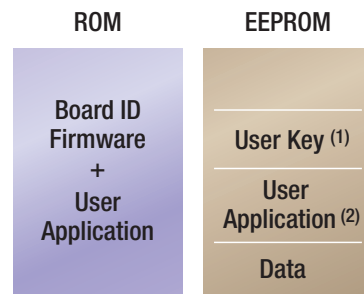
### Board ID Firmware

The Board ID Firmware system is a thoroughly tested and proven code that accelerates the development of user applications for the Renesas Board ID series of devices. The Board ID operating system provides an API for various cryptographic, math and system-resource functions in a secure environment. Its core utilizes the hardware security features of the device firewall management unit (FMU), allowing the OS to be separated from the user applications.



### Secure Download Operation

The host must first download the user application. It should then install and specify the user application entry address so the user application can be initialized after the next reset. The user application uses the core as needed for any math, crypto and EEPROM-access functions. The download operation can only be performed with a mechanism protected with security keys. Renesas will provide customers with a test key that is valid only for test and evaluation purposes.



(1) can be programmed either at Renesas or by the customer

(2) can be securely downloaded

No data can be written in these two areas after application is downloaded with the secure downloader

### Cryptographic functions:

- ▶ Symmetric encryption:
  - 3DES
- ▶ Asymmetric encryption:
  - RSA with up to 1024-bit encryption
  - RSA CRT with up to 2048-bit encryption
- ▶ RSA on-card key generation
- ▶ RSA CRT on-card key generation
- ▶ Hash algorithm SHA-1
- ▶ Digital signatures with asymmetric encryption
  - RSA with SHA-1, PKCS v1.5,
  - FIPS 186-2 DSS
- ▶ Cryptographic algorithms are secure against:
  - SPA
  - DPA
  - DFA

### Security functions:

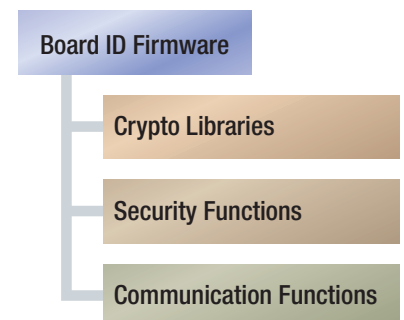
- ▶ Firewall for application separation is secure against:
  - DFA
  - Software attacks
- ▶ Security Domains
- ▶ Encrypted storage of confidential data (PINs, keys, etc.)

### Communication functions:

- ▶ Supports I2C, SPI, UART

### Chip:

- ▶ 16-bit High-Security Microcontroller



## Implement Robust Security Measures Quickly!

Adding highly secure M2M authentication capabilities to a product isn't difficult – not anymore. To accelerate and facilitate the development process, Renesas now offers the Board ID Demonstration Kit. It provides a complete set of tools and software for designing machine-to-machine authentication and security implementations. Clear instructions and a short tutorial eliminate the need to become an expert in security technology in order to put a proven protection methodology to work on a board in any product.



**Renesas Board ID  
Demonstration Kit**



For more information, please contact us at 408-382-7500 or [www.america.renesas.com/boardid](http://www.america.renesas.com/boardid).

© 2009 Renesas Technology America, Inc. Renesas Technology America, Inc. is a wholly owned subsidiary of Renesas Technology Corporation. Board ID is a trademark of Renesas Technology Corp. All other trademarks are the property of their respective owners. The information supplied by Renesas Technology America, Inc. is believed to be accurate and reliable, but in no event shall Renesas Technology America, Inc. be liable for any damages whatsoever arising out of the use or inability to use the information or any errors that may appear in this publication. The information is provided as is without any warranties of any kind, either express or implied. Renesas Technology America, Inc. reserves the right, without notice, to make changes to the information or to the design and specifications of its hardware and/or software products. Products subject to availability. Printed in U.S.A.



Printed on Recycled Paper 1009/in-house/BCD/SP REU01A0004-0002



Renesas Technology America, Inc.

450 Holger Way, San Jose, CA 95134

Tel:408-382-7500 Fax:408-382-7501

[www.america.renesas.com](http://www.america.renesas.com)