

Board ID™ Solution for Embedded Security

A Powerful, Flexible Solution for Machine-to-Machine Authentication (M2M)

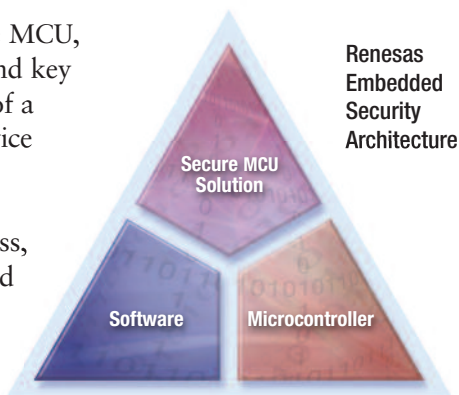
Renesas' Board ID solution includes: a secure MCU, proven firmware with security application, and key programming services to enable easy design of a complete security solution. The Board ID device facilitates new functions and processes for M2M security.

It also offers significant benefits for business, industry, medical, government, consumers and other M2M markets, relative to traditional, less secure machine identification technologies such as serial EEPROM ICs.

Board ID Security Applications

The Board ID solution is built with thoroughly tested and proven software that accelerates the development of user applications. The solution provides an API to allow for an easy implementation of a strong authentication. Its core utilizes the hardware security features of the device combined with a powerful public key cryptographic (RSA) unit to compute the authentication algorithms.

The Renesas Board ID solution is ideal for implementing powerful and cost-effective security solutions, as summarized below.



FEATURES

Cryptographic functions

- ▶ Asymmetric encryption:
 - RSA with up to 1024-bit encryption
 - RSA CRT with up to 2048-bit encryption
- ▶ RSA on-chip key generation
- ▶ RSA CRT on-chip key generation

Digital signatures with asymmetric encryption

- ▶ RSA with SHA-1, PKCS v1.5,
- ▶ FIPS 186-2 DSS

Cryptographic algorithms are secure against

- ▶ SPA (Simple Power Analysis)
- ▶ DPA (Differential Power Analysis)
- ▶ DFA (Differential Fault Analysis)

Security functions

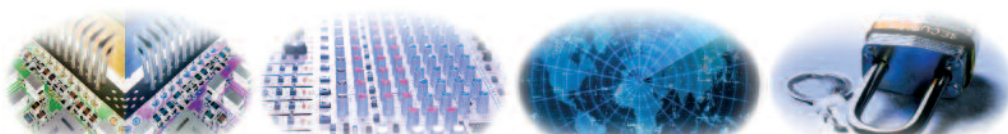
- ▶ Firewall for application separation that is secure against:
 - DFA
 - Software attacks
- ▶ Security domains
- ▶ Encrypted storage for confidential data (PINs, keys, etc.)

Secure communication functions

- ▶ Supports I²C

Chip

- ▶ 16-bit High-security microcontroller



Anti-cloning

Protects against contact manufacturers producing more of a product than were ordered, as well as unauthorized firms copying a product.

Usage Control

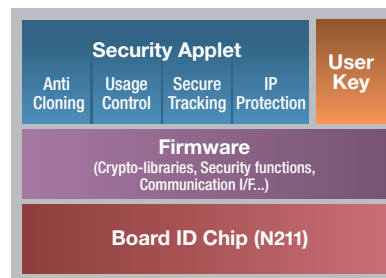
Limits use of a product to only those features and applications for which a service contract has been paid.

Secure Tracking

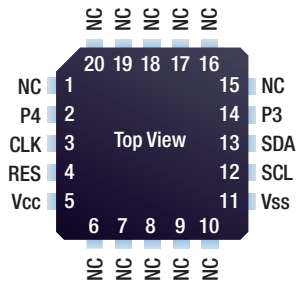
Verifies that only approved companies perform maintenance operations, and that they install only genuine replacement parts.

IP Protection

Implements a security procedure that safeguards sensitive and valuable IP on a circuit board.

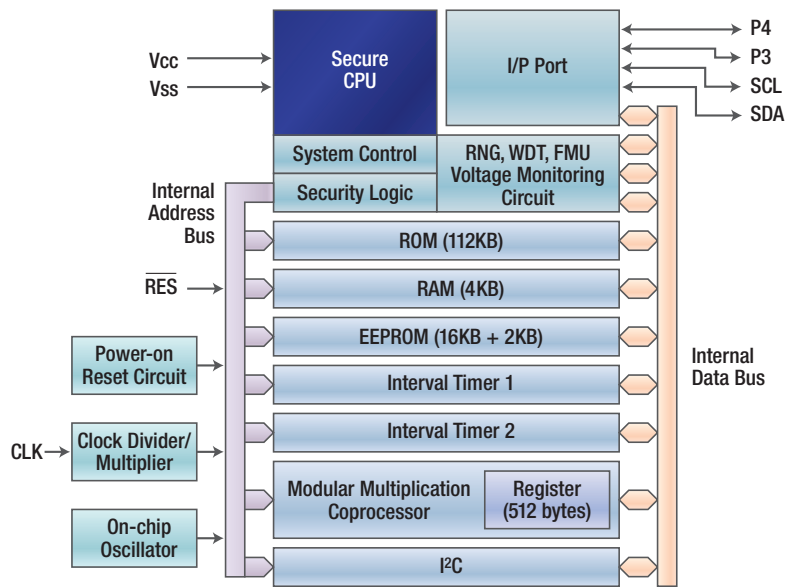


Board ID Pin Assignments



► The compact 4.2x4.2mm package of the device has pin connections on only two sides, simplifying board layout. Special anti-tamper features are incorporated into the design of the package.

Board ID Chip Block Diagram



► The Renesas Board ID solution integrates all of the necessary signal processing and data storage functions on a chip manufactured in a secure facility under the control of tight security procedures and protocols.

Board ID Chip Features

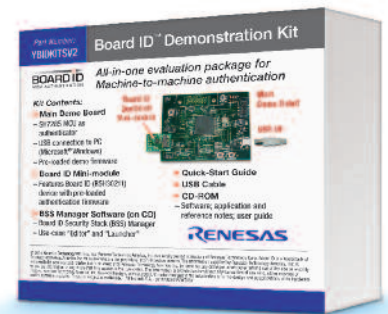
The security chip is based on Renesas Electronics' extensive experience building devices for smart cards. Its features have been further developed and refined to meet the needs of M2M authentication applications in which valuable physical or intellectual property might be threatened by theft, misuse or any other form of malfeasance. The chip is easy to apply and is priced to be a cost-effective product enhancement. It ensures a high level of protection against unauthorized application or misappropriation.

Product family	N-Series N211
Type no.	R5H30211
Processor	Secure 16-bit CPU core Modular multiplication co-processor
Interface	I2C
EEPROM	16KB + 2KB
Clock	On-chip oscillator
I/O ports	4 GPIOs including serial I/F (multiplexed)
Temperature range	Commercial temp.: -20 to +75 °C Optional wide temp. range: -40 to +85 °C
Power supply	1.8V to 3.6V
Tamper proof	On-chip detectors and shield against security attacks
Package	QFN20 (4.2mm x 4.2mm)
Production	Secure manufacturing and testing site

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.



For more information on the Board ID Solution, please visit www.am.renesas.com/boardid

Renesas Electronics America Inc. | 2880 Scott Boulevard, Santa Clara, CA 95050-2554 | Phone: 1 (408) 588-6000, Literature/technical support: 1 (800) 366-9782 | www.am.renesas.com

© 2010 Renesas Electronics America Inc. (REA). All rights reserved. All trademarks are the property of their respective owners. REA believes the information herein was accurate when given but assumes no risk as to its quality or use. All information is provided as-is without warranties of any kind, whether express, implied, statutory, or arising from course of dealing, usage, or trade practice, including without limitation as to merchantability, fitness for a particular purpose, or non-infringement. REA shall not be liable for any direct, indirect, special, consequential, incidental, or other damages whatsoever, arising from use of or reliance on the information herein, even if advised of the possibility of such damages. REA reserves the right, without notice, to discontinue products or make changes to the design or specifications of its products or other information herein. All contents are protected by U.S. and international copyright laws. Except as specifically permitted herein, no portion of this material may be reproduced in any form, or by any means, without prior written permission from renesas electronics america inc. Visitors or users are not permitted to modify, distribute, publish, transmit or create derivative works of any of this material for any public or commercial purposes.

Printed on Recycled Paper. 0410/200/VIP/BCD/SP Document No. R30PF0004EU0100