

---

---

# Board ID — An Improved Approach to Achieving Robust Machine-to-Machine Authentication that Reduces Operating Risks and Enables Profitable Business Strategies

---

Nadaradjane Ramatchandirane, Senior Business Development Manager, System LSI Business Unit,  
Renesas Technology America, Inc.

---

## Abstract:

This white paper focuses on security solutions for machine-to-machine (M2M) authentication. It describes the most common current solution and highlights the need for and benefits of improved solutions. Then it provides an overview of the strong Board ID™ chip solution developed by Renesas Technology, describes its advantages, and explains how it can be designed into a product. Several usage examples illustrate the merits of security authentication using the Board ID solution for applications in various markets. Finally, this paper summarizes the technology and product roadmap for Renesas security solutions.

## 1. Introduction

Today the markets for secure access and/or identification technologies are expanding beyond the realm of traditional consumer segments and moving into the industrial and enterprise sectors, opening up many more business opportunities in the process. Renesas believes that robust machine-to-machine (M2M) authentication is an ideal way to capitalize on these opportunities. Thus the company has developed a solid implementation solution based on a board-identification (Board ID) chip that uses proven security technology.

## 2. Key issues in machine-to-machine authentication

Machine-to-machine authentication schemes manage the connection and interaction of devices and subsystems to equipment or systems in order to prevent unwanted illicit or unintentional activities. The cloning of electronic devices, for instance, is a widespread problem, as are unauthorized product alterations that thwart efforts to maintain regional

price differentials for different operating requirements. Depending on the situation, the consequences of products having inadequate security can range from minor to serious to disastrous. The appropriate security solution directly depends on the likelihood of security breaches and the possible consequences of those breakdowns.

## 3. Limitations of currently used M2M authentication methods

Machine-to-machine authentication methods are used in various types of products today, but the implementations typically employed are not very robust. By far the most common approach is a simple, one-way scheme based on a serial number stored in an EEPROM in a peripheral or subsystem. Other authentication methods currently in use include proprietary and/or outdated (and expensive) solutions that aren't suitable for volume markets, as well as weak solutions based on software-only components.

The authentication process used when a product has a serial number stored in an EEPROM consists of just one step. When that device attempts a connection, the host system reads the serial number and checks it against a stored authorization list. The connection is approved and predefined activities are authorized only if the serial number is valid.

This simple and cheap approach does provide a small amount of security. Nevertheless, it is a very unsafe technique. The EEPROM is unprotected and a host processor can read the serial number and modify it easily. Moreover, the method used for generating the serial numbers is not secure. For these reasons, storing serial numbers in EEPROM is an inadequate methodology for situations that require more than a minimal level of security.

## 4. Objectives of strong M2M authentication

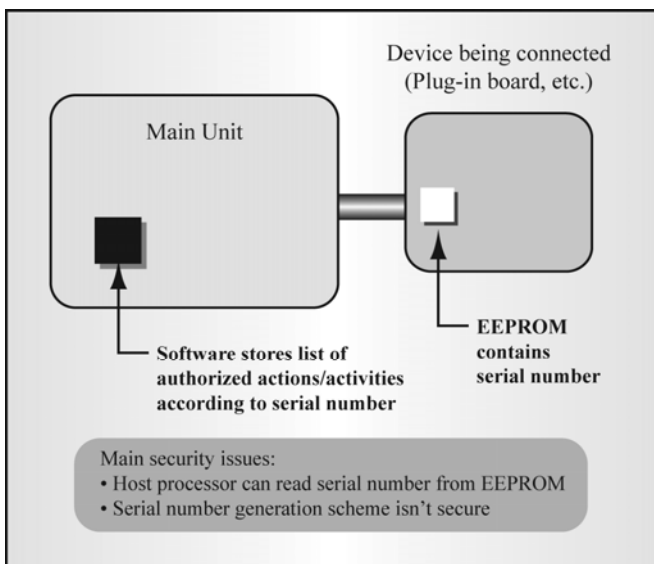


Figure 1. EEPROM solution has significant weaknesses. If an EEPROM is used to store a serial number on a peripheral or subsystem, the security provided is easy to compromise.

To safeguard equipment and protect business strategies, Renesas advocates the use of strong, proven technologies that can bring powerful and cost-effective security capabilities through the implementation of M2M authentication. These capabilities include:

- Ensuring that each peripheral is a genuine authorized product and not an unauthorized copy
- Allowing personalization of each peripheral or subsystem and ensuring its safe operation under the control of the main system
- Enabling new revenue-generating business models

#### 4.1. Capabilities of the Renesas Board ID solution

The Renesas Board ID M2M authentication solution offers strong security and delivers various access and activity management capabilities. The proprietary Board ID chip has a powerful, tamper-proof architecture with highly secure cryptographic functions derived from Renesas' proven smart card IC technology. With the Board ID approach, any MCU can be incorporated into the system, enabling maximum design flexibility. When higher security is needed, the Board ID chip can handle asymmetrical cryptosystem authentication as well symmetrical algorithms including 3DES, RSA and Hash.

The new security solution has three elements. First, a Board ID secure authentication chip mounted on the peripheral device or subsystem replaces the EEPROM containing the serial number. The Board ID chip has been initialized with a security certificate and a unique ID securely stores a unique access code (private key). Secondly, a root Certificate of Authority (CA) that cannot be changed is installed into the host system or function. That system or function provides protection against tampering for the security software it runs and disallows the authentication mechanism to be bypassed. Third, a highly secure certificate generation scheme is implemented, ensuring that full protection capabilities are implemented.

#### 4.2. The Renesas Board ID M2M authentication process

In operation, the Board ID based solution makes M2M authentication a fast process. The host authenticates the Board ID chip via a communication link that does NOT have to be secured. When a valid peripheral or subsystem attempts a connection to the host, the following seven steps occur very rapidly:

1. The host platform requests authentication from the Board ID chip built into the connecting device.
2. The Board ID chip then returns its certificate, which includes its unique ID and securely stored public key.
3. The host validates the Board ID certificate with the securely stored Certificate of Authority issued to it.
4. The host sends a challenge (random number) to the connecting device to prove that its Board ID chip has the private key associated with its certificate/ID.

5. The Board ID chip digitally signs the challenge with its private key (which is never released from the chip) — provided that it is not prevented from doing so by any specific limits (on operating time, etc.) managed by its firmware.
6. The Board ID chip returns a response (signed challenge) to the host.

Finally, the host validates challenge response using the certificate previously validated in step #3 and enables the authorized connectivity and types of activity.

#### 4.3. Basic advantages of the Renesas Board ID approach

The Renesas Board ID -based M2M authentication solution has multiple advantages:

- It delivers a very high level of security using the same security technologies rigorously tested and proven in the nearly one billion smart card ICs produced to date
- The Renesas solution can be certified (or is certifiable) to industry security standards such as the Common Criteria, Visa, Mastercard, and FIPS
- The Renesas M2M authentication solution takes a comprehensive approach to risk minimization that encompasses:
  - High security in the design and production of the elements of the solution
  - Ability to integrate with the solution's implementation in systems such as enforcement; and
  - Significant track record of deploying the M2M authentication in real-world applications, including remote security management and class control and regionalization

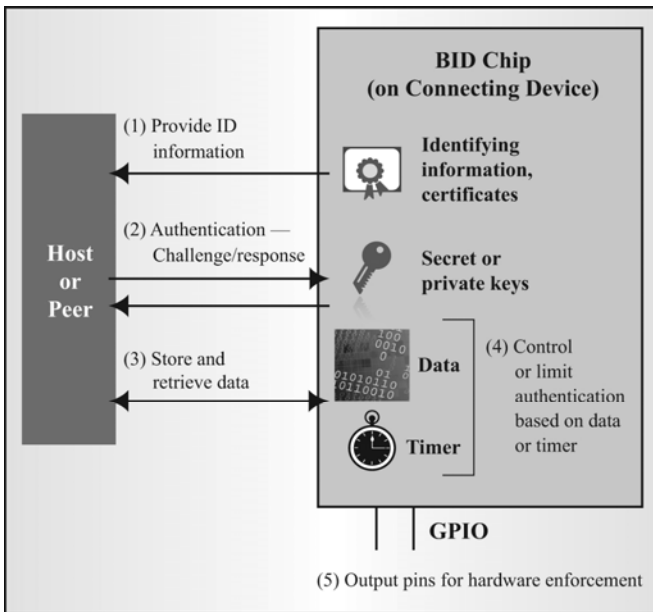


Figure 2. Device authentication using BID chip. Solid, proven encryption technology is used to ensure that the authentication process is safe and highly secure. The host won't allow the connection of a cloned connecting device that doesn't contain a valid BID chip.

Moreover, the Board ID chip itself (see Figure 2) delivers other important advantages:

- It is an easy replacement for serial EEPROM memory
- The chip has a small package (small footprint) and takes up very little circuit board space
- The device allows easy links to embedded system microcontrollers by using a standard serial communication interface (I<sup>2</sup>C, SPI, UART) instead of a smart card interface
- It is tamper-proof due to the incorporation of multiple electrical and mechanical safeguards
- It stores keys, certificates, data and programs in highly reliable nonvolatile on chip memory that has an endurance of 10,000 rewrites and retains data for 10 years
- It provides a built-in random number generator and uses a modular multiplication coprocessor to accelerate the calculation of RSA and other cryptographic algorithms
- It includes a standard suite of software components
- Virtually any standard MCUs can be plugged into the Board ID platform because most of them come with standard interfaces
- The Board ID chip is manufactured in Renesas' manufacturing facilities in Japan and Europe that meet the security standards of the smart card industry

## 5. Applications of Board ID M2M authentication

The Renesas M2M solution can enable new functions and processes offering significant benefits for business, industry,

hospitals, government, consumers and other areas of society. Generally, the Renesas Board ID chip is used to give a controlling device (usually a Host or Peer) the highest level of confidence that the connecting device (containing the Board ID chip) is authentic, before the controlling device allows a transaction to be conducted or a function to be performed. The Board ID chip can also have additional functionality, such as limiting the authentication based on defined constraints and transferring data securely. Key applications are described below.

### Use Case 1: Device authentication and control (anti-cloning)

The Renesas Board ID solution can be used to allow a host device such as a PC or a motherboard to authenticate a peripheral device or a daughter board. The host device will refuse to operate with the peripheral unless the chip confirms that the peripheral is an authentic (authorized) product. This capability can allow a system supplier that isn't plug-and-play oriented to be 100% sure that a proper piece of equipment is installed correctly at a user site, even if manufacturing and distribution are performed by third parties or 'virtual' partners based in remote countries. The Board ID solution prevents fraudulent activity or human error that can adversely impact the company's sales and safeguards the firm's reputation and the perceived quality of its products by preventing 'rogue' products from being installed in place of genuine ones. This type of connectivity management also protects sensitive information and helps ensure safe system operation. It offers security with flexibility and allows peripherals to be personalized differently, and even made disposable. The interaction between the host and the peripheral device is as follows:

- 1) Host Board ID challenges peripheral Board ID
- 2) Board ID uses secret or private key to respond
- 3) Board ID validates response and enforces security and control issues. The results of the validation are enforced generally in one of two ways:
  - a) Hardware – GPIO line on Board ID can be used to disable something in the host hardware
  - b) Hardware – A message is sent from the Board ID chip to Host software/firmware. The Host software/firmware must secure enough to enforce the validation result

### Use Case 2: Imposing restrictions on the usage of peripherals or other devices

It's possible to program the Board ID chip to ensure that the device into which it is installed must be operated according to that product's instructions and can't exceed specifically authorized usage limits. Such security and control is a very important safety factor in medical applications, for example. When installed in a peripheral or other device to enforce usage limitations, the Board ID chip can

- Limit the amount of time — or the number of times — that the peripheral can be used
- Allow the peripheral to be used only if a license has been purchased or if the host and peripheral are compatible

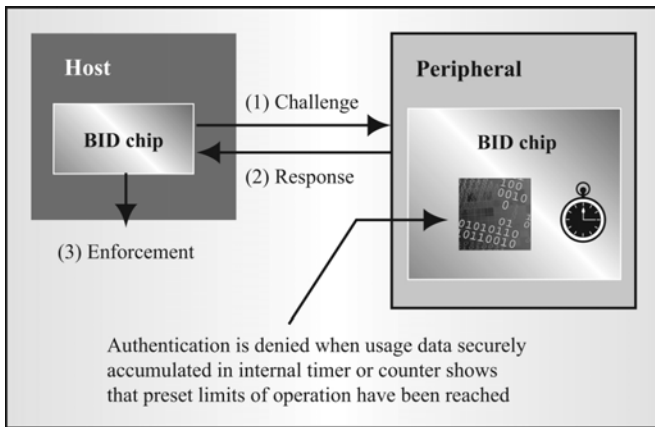


Figure 3. Restrictions on peripheral or device use. The BID chip can limit the amount or time or number of times a peripheral can be used. It can also prevent a peripheral from being used if a license hasn't been purchased or if the host and peripheral are incompatible.

### Use Case 3: Implementing new business models

The Board ID chip's ability to provide strong, effective M2M authentication for enforcing usage limitations can open up new business models. For instance, by using the Board ID chip, it becomes possible to profitably shift value from a main system to its extensions. The value proposition of system peripherals can be raised as high as that of the host system, leading to higher profit margins and flexible pricing strategies. One way to do this is to offer the basic system for a very low price, then charge fees when the user wants more functionality and thus requests the activation of daughter-board components or certain types of peripherals. Additional fees can be required to activate a new software license when usage ramps up to exceed a preset level, or when the user requires optional system capabilities. This value-added pricing marketing approach has been proven effective in selling products such as cable TV boxes. Revenue can be generated based on metered use of a product, and hardware features can be activated in the field upon receipt of a request and payment.

### Use Case 4: Preventing license bypassing of an entire system

The Renesas Board ID chip can be used to prevent the cloning of an entire system or the bypassing of licensing agreements. In this use case, it provides a secure boot operation and has enforcement functions, as described below.

- 1) Secure Boot
  - a) May be needed if hardware enforcement is not sufficient
  - b) Ensures that the system won't boot if the firmware is invalid, or will cause the Board ID chip to prevent system operation if the firmware is invalid
- 2) Enforcement
  - a) The system must be designed to not operate unless the Board ID chip is present with a valid license. This can be done in two basic ways:
    - i) Hardware enforcement – The GPIO lines on the Board ID chip disable the supporting hardware

- ii) Messaging enforcement – The firmware running on the CPU will not operate unless the appropriate message is received from the Board ID chip. (This method requires a secure boot.)

Note: That in order to fully protect against system cloning, a certain portion of the IP (such as firmware and hardware) must be secured from attack.

### Use Case 5: Enabling effective class control and regionalization

The feature set, usage class, algorithms, etc. of the same basic product often must be changed to meet the requirements of users in different parts of the world. Therefore, depending on where a hardware component is used, the company that supplies it may price it differently for technical and/or business reasons. In a typical situation, a large-volume customer in location A who wants fewer features will get a lower price than a customer in location B. This geographic pricing strategy is undermined if a distributor purchases the component intended for customer A and attempts to serve customer B by performing its own customization. Moreover, this unauthorized third-party customization can reduce the overall quality of the final system.

The Renesas M2M authentication solution facilitates the manufacture and controlled sale of products that a supplier tailors differently for different local or regional global markets. The security it provides allows firm control of both the pricing and the quality of the products, wherever they are deployed. Although the solution cannot prevent unauthorized modifications by third parties, it does deny the altered products connectivity, rendering them of no use or limited utility to buyers.

### Use Case 6: Device/board tracking for maintenance management

After the Renesas Board ID chip is installed in a peripheral device or subsystem, it can maintain and safeguard data on multiple activities that can be accessed remotely and securely. For example, the Board ID chip can enable the vendor of the equipment to verify with certainty that only authorized companies have performed maintenance operations or installed replacement parts. This would ensure better control of system integrity, make sure that repairs meet high standards of quality, and protect against the installation of counterfeit components.

## 6. Conclusion

Many benefits can be derived from strong machine-to-machine authentication. The Board ID based solution Renesas Technology now offers is based on a solid foundation of technology, products, and support that has been well tested and proven in serving the smart card markets for over 20 years. This solution is robust, easy to implement and drastically reduces risk in many areas of business, while opening up new opportunities for revenue generation for Renesas customers.

**Nadaradjane Ramatchandirane**

Joined Renesas Technology America in 2007 as the Senior Business Development Manager, System LSI Business Unit to manage business development in the security space. Before Renesas, he held executive positions in Schlumberger/Gemalto, ActivIdentity, Hypercom and Bitfone.

Note: Board ID is a trademark of Renesas Technology Corp.