

Renesas Technology America, Inc.

Board ID Solution for M2M Authentication

The Board ID solution is based on Renesas' proven Smart Card IC technology that facilitates new functions and processes for Machine-to-Machine (M2M) security while also offering significant benefits for business, industry, hospitals, government, consumers and other M2M markets. The Renesas Board ID solution provides a very secure identity for the motherboard or circuit board of a system, peripheral or device using EAL4+ and FIPS Level 2 certifications. The solution offers many important features, such as:

- Proven, tamperproof smart card technology
- FIPS (Federal Information Processing Standards) certifiable
- Authentication of identity
- Secure read/write of data
- Asymmetrical key encryption option
- Resistance to a wide range of physical, electrical, and timing attacks
- Can connect to any standard MCU

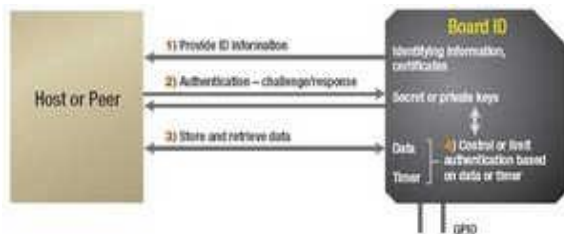


Figure 1: The Board ID solution.

The Board ID solution is further strengthened by the solid foundation of Renesas' security expertise and support; helping you to deliver machine-to-machine ("M2M") device implementation in an easy, cost-effective way. Once you select the Board ID solution for your application, you can instantly benefit from Renesas' significant track record, built up over 20+ years, of deploying M2M authentication solutions, and thereby reduce any implementation risk considerably.

The Board ID solution – consisting of security chips - provides security via the following technologies:

Cryptographic Processing

This security mechanism ensures:

- Confidentiality – encrypting and decrypting data
- Integrity – ensuring data has not been changed
- Identity – proving that you are who you claim to be
- Signature validation – proving that you signed a document

When you use Board ID solution, you use cryptography processing that is implemented in security chips via encryption technology such as Symmetrical (e.g. 3DES, AES) or Asymmetrical (e.g. Public Key Cryptography such as RSA, ECC) encryption.

Data Protection

In addition to providing cryptographic operations, Renesas' security chips also protect the data physically. The technique used is protecting keys, where keys are used to provide access to data.

Licensing and Key Management

Your solution will most likely require your security chips to be loaded with keys. This will be done by an Identity/License Authority via a third party or via secure tools you run in your operations. The two steps are:

- Creating and Managing (storing, transmitting, receiving) cryptographic keys
- Creating licenses to use in secure applications

How Board ID Authentication Process Works

In operation, the Board ID based solution makes M2M authentication a faster 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, several steps must be completed successfully before the host grants connectivity and access to an authorized device. The entire process takes place quickly - typically in a fraction of a second.

Benefits of Board ID Solution

Use the Board ID solution to ensure anti-cloning, usage control and tracking as follows:

- Only a genuine or certified component can be used by a system.
- Host system will only work with a valid peripheral as per the prescribed usage conditions (# times, duration, location)
- Host system will only work with equipment that is designated for the desired use; e.g., a phone for sale in Taiwan will only work with a PBX for use in Taiwan
- Host system will only work with a subsystem as per the specified usage profile
- Warranties and maintenance are provided for valid unit
- System configuration database that authorize downloading of proper drivers
- Secure remote downloads

Build a Secure System using Development Tools

The design of your total solution is important when you consider the security of your overall product/application design. To help your engineers and architects build effective security, Renesas provides a complete set of hardware and software support tools, including middleware products. There are two kits, as follows:

The N-Series Board ID Starter Kit, which lets you learn about basic security functions and designs, test and evaluate the N-Series BID demo board, and use the sample programs as a starting point.

The Board ID Development Kit

The Board ID Development Kit allows you to evaluate functions and designs, test and evaluate the BID N-Series chip on a full development board, and to use the sample programs as a starting point. For prototype implementations and logical design testing, qualified designers can obtain sample code for test and evaluation purposes.

For your business, Renesas' Board ID solution can open new opportunities for revenue generation today!