



## **Board ID Use Cases for the Medical Device Market**



The Renesas Technology Board ID solution allows for the rapid implementation and deployment of security/risk management solutions for the medical device industry. The U.S. FDA, both domestically and abroad, has been working with the biotech industry to establish guidelines to meet an ever-growing need for managing risk, and some standards have emerged as a result of this effort.

For the purpose of this discussion, we will focus on two standards that have emerged as a basis for determining the existence of Good Manufacturing Practices (GMPs) by the FDA and associated regulatory agencies:

**ISO 14971** – An ISO standard which specifies a process for a manufacturer to identify the hazards associated with medical devices, including in vitro diagnostic (IVD) medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.

**ICH Q9** – A standard developed within the Expert Working Group (Quality) of the International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) that has been subject to consultation by the regulatory parties (including the FDA), in accordance with the ICH process.

The principle difference that exists between these two standards is that ISO 14971 focuses on medical devices, and ICH Q9 focuses on drugs. It should be noted, however, that the line between medical devices and drugs is blurring, and one should be familiar with standards that apply to both medical devices and drugs in order to prevent being blindsided.

An example of this blurring would be Drug Eluting Stents, which are stents (a medical device) that are coated with drugs in order to prevent rejection by the human body. They cannot be defined solely as either devices or drugs because of this duality.

The Renesas Board ID solution offers features which can directly (and indirectly) assist in meeting these standards and (just as importantly) help to assure that the business models of medical device manufacturers are indeed secured.

Ultimately, what any medical device manufacturer is most interested in securing is a constant and consistent positive financial stream. Let's examine how Board ID can help by examining 4 specific use cases:

1. Anti-Cloning
2. Usage Control
3. Secure Tracking
4. Intellectual Property Protection

Bear in mind that with each use case there is some overlap, and in examining each use case, repetition of objectives and principals will occur.

## **Use Case 1 - Anti-Cloning**

Anti-cloning refers to a situation where a medical device manufacturer produces a main base unit (a capital asset) that has a peripheral or peripherals attached to the capital asset. The business model in this case is one where the capital asset may or may not be a loss leader, and the peripherals are meant to have finite life spans that are considerably shorter than the lifespan of the capital asset. The peripherals are the recurring source of revenue for the device manufacturer, and there are several dynamics at work within this framework. Here are a few examples:

- The medical device manufacturer's reputation hinges on the consistent availability and reliability of the peripherals. If the peripherals fail to operate as designed, or cannot be obtained with a high degree of consistency, then patients could be put at extreme risk.
- The cost of manufacturing these peripherals needs to be kept as low as possible to maximize profit.
- The market penetration needs to be maximized as quickly as possible, to avoid competition in an ever-growing global market (i.e., you need to build market share).
- The peripherals must not be ones that could be easily duplicated by an unauthorized entity.

How can Board ID help? Lets begin with the first bullet point, and speak specifically to reliability. The intense testing which must occur in order to bring a medical device to market is one of the best ways to insure reliability. Consequentially, a user of such devices who obtains them from an authorized supplier can and will rely on the supply chain the manufacturer puts in place. This can, however, introduce some challenges. How can a user be assured that the device he is receiving is indeed one that came from the manufacturer's authorized manufacturing facility? If the manufacturing facility is in the United States, and the end user is also in the United States, it may be easy to control the supply chain, but if the device is produced overseas, this becomes exceedingly more difficult.

This leads to the second bullet point, which refers to the need to keep manufacturing costs low. A medical device manufacturer in the USA is quite likely to consider manufacturing overseas in order to drive costs down,

but that increases the risks much more. Quality assurance, as well as the protection of trade secrets, can quickly become unwieldy, and this can then lead to the third problem, which is an inability to achieve market penetration before a competitor figures out how to do what you are doing.

If a competitor (especially one overseas) can set up shop (often due to proprietary information leaks), then he can penetrate the market for a fraction of the cost that the original device manufacturer could due to the lack of a need to absorb development costs (which can be HUGE).

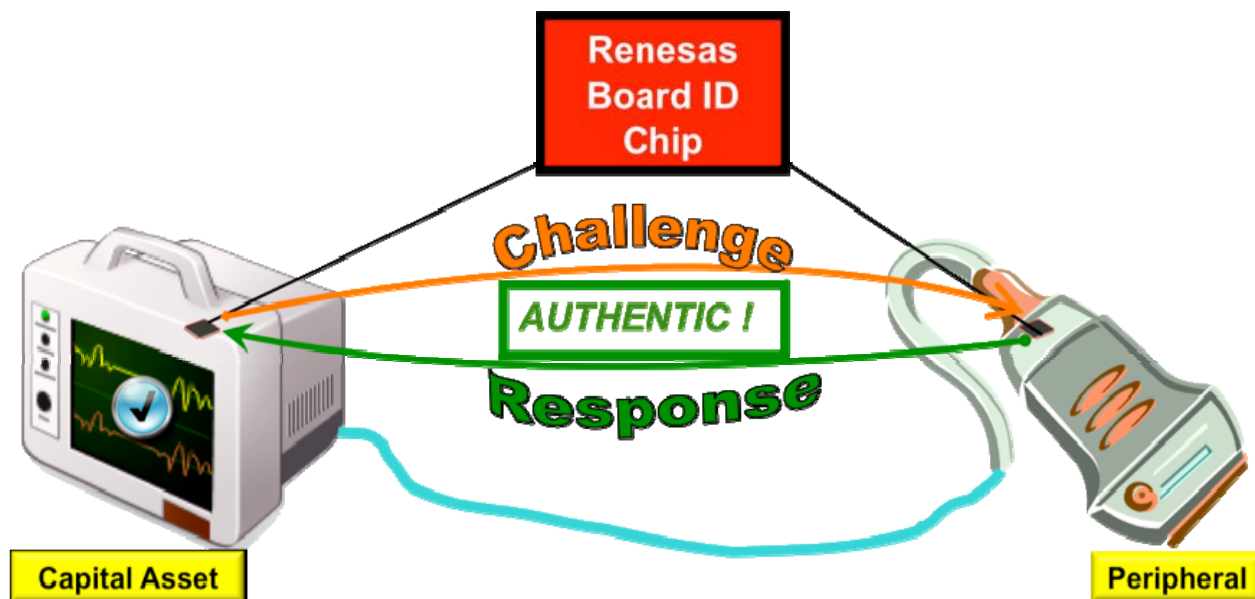
Which finally leads us to our fourth bullet point: how do we prevent the duplication (or cloning) of the peripherals?

The Renesas Board ID solution can address this in a very elegant and simple way.

The Board ID solution provides two distinct and important components. One component is the Board ID Security Chip, and the other is the Board ID Provisioning Process. By incorporating a Board ID Chip into the design of the capital asset and peripheral, a robust and highly secure means of authentication is introduced. Let us see how the authentication works (see [Figure 1](#)):

## Use Case: Anti-Cloning

Authentic Peripheral Used



- 1. Board ID Security Chips Are Put Into The Host (Capital Asset) and Peripheral**
- 2. Once The Peripheral Is Attached And The Unit Is Powered On, The Host Issues An Authentication Challenge To The Peripheral.**
- 3. The Peripheral Sends Back An Authentication Response**
- 4. Once The Response Is Authenticated The System Becomes Fully Operational.**

*Figure 1*

The Board ID Chips come pre-loaded with keys as part of the provisioning process, which can be facilitated by Renesas Technology (either directly or through a Renesas Technology partner).

Traditionally, provisioning was facilitated by device manufacturers. This can become an unwieldy process in and of itself. By providing the provisioning process as part of the entire Board ID solution, the medical device manufacturer can focus on the functionality of the device rather than the sometimes complex task of managing security solution implementation and management.

What do we accomplish with this solution? In terms of ISO 14971, we directly address the very real risks associated with the introduction of a

counterfeit or unauthorized peripheral entering the supply chain. If a peripheral does not contain a provisioned Board ID chip, it will fail to function when used with the capital asset since there is no way for authentication to occur in the absence of a provisioned Board ID chip.

What about risks associated with overseas manufacturing? The allure of the low manufacturing costs associated with going overseas, is hard to pass up, but the associated risks increase dramatically when facilities are moved to places like China. If a manufacturer must manage the security of such facilities overseas, the cost benefits could quickly evaporate as the overhead associated with management costs escalates. Relying on the use of foreign management teams is risky at best, since their loyalties may indeed be skewed towards their own interests (i.e., family, friends, “entrepreneurship”).

The inclusion of provisioned Board ID chips within the manufacturing process can effectively eliminate the ability of counterfeiters to successfully introduce an unauthorized product into the supply chain.

It is extremely important to understand the need to have a robust security solution in place proactively (rather than reactively) because if a counterfeit item enters the supply chain, it could be years before a device manufacturer overcomes the loss of revenue associated with such activities. This is extremely risky because the rapid advances in technology tend to make brilliant discoveries obsolete within a short period of time, and for a company to dedicate financial resources towards recovering a lost business model could mean the loss of all profitability.

In a worst-case scenario, a peripheral may be a Class II/III device, and the introduction of counterfeit Class II/III devices could (and more than likely would) mean exposing a patient to great harm. In this case, the reputation of the device manufacturer could be irreparably damaged. Even though it may indeed be provable that the peripheral was not authorized for use with the capital asset, the associated damages would more than likely eclipse any explanation put forth.

## **Use Case 2 – Usage Control**

Usage Control refers to a situation where a medical device manufacturer produces a main base unit (a capital asset) that has a peripheral or peripherals attached to the capital asset. The business model in this case is one where the capital asset may or may not be a loss leader, and the peripherals are meant to have finite lifespans which are considerably shorter than the lifespan of the capital asset. This use case is similar to the [Anti-Cloning use case](#), with the addition of a secure counter/timer for monitoring and controlling the amount of time and or uses of the peripheral. Bear in mind that the secure timer feature is included with the Renesas Board ID solution and simply needs to be “activated” by implementing an included piece of software.

In this case, the peripherals themselves are part of the recurring source of revenue for the device manufacturer, and the number of uses and time in use can also be harnessed as a revenue source. There are several dynamics at work within this framework. Here are a few examples:

- The medical device manufacturer’s reputation hinges on the consistent availability and reliability of the peripherals. If the peripherals fail to operate as designed, or cannot be obtained with a high degree of consistency, then patients could be put at extreme risk.
- The cost of manufacturing these peripherals needs to be kept as low as possible to maximize profit.
- The market penetration needs to be maximized as quickly as possible, to avoid competition in an ever-growing global market (i.e., you need to build market share).
- The peripherals must not be ones that could be easily duplicated by an unauthorized entity.
- The number of times or length of time a peripheral can be used must not be easily compromised.

How can Board ID help? Let us begin with the first bullet point and speak specifically to reliability. The intense testing which must occur in order to bring a medical device to market is one of the best ways to insure reliability. Consequentially, a user of such devices who obtains them from an authorized supplier can and will rely on the supply chain the manufacturer puts in place. This can, however, introduce some challenges. How can a

user be assured that the device he is receiving is indeed one that came from the manufacturer's authorized manufacturing facility? If the manufacturing facility is in the United States, and the end user is also in the United States, it may be easy to control the supply chain, but if the device is produced overseas, this becomes exceedingly more difficult.

This leads to the second bullet point, which refers to the need to keep manufacturing costs low. A medical device manufacturer in the USA is quite likely to consider manufacturing overseas in order to drive costs down, but in return, the risk is greater. Quality assurance, as well as the protection of trade secrets, can quickly become unwieldy, and this can then lead to the third problem, which is an inability to achieve market penetration before a competitor figures out how to do what you are doing.

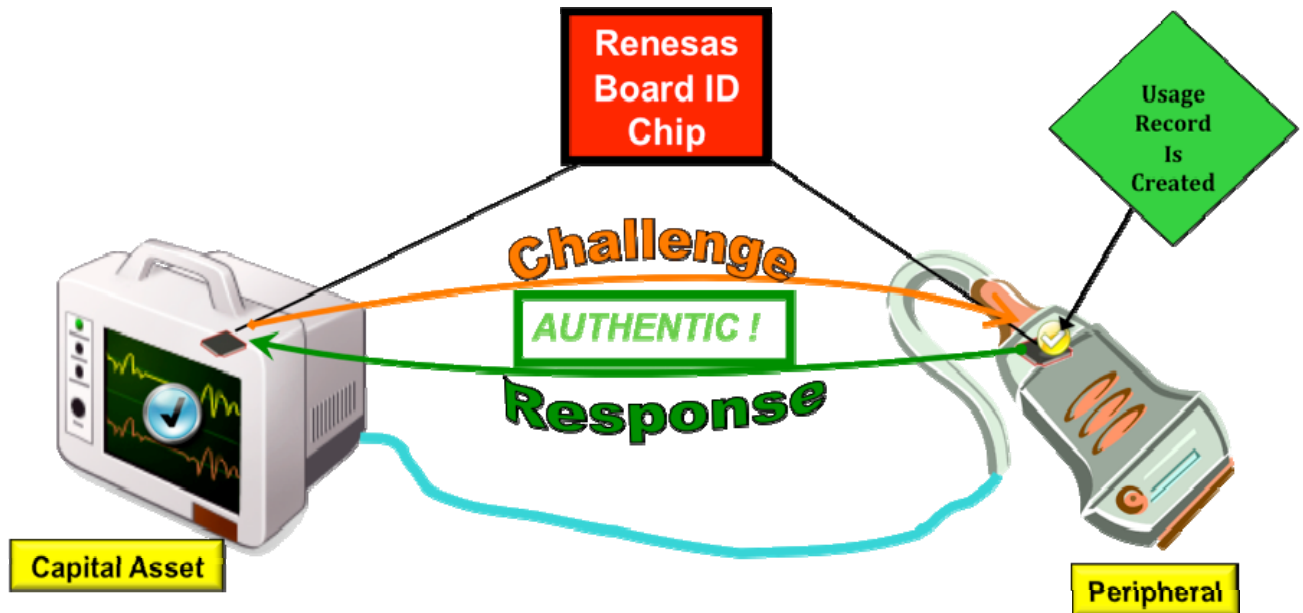
If a competitor (especially one overseas) can set up shop (often due to proprietary information leaks), then he can penetrate the market for a fraction of the cost that the original device manufacturer could due to the lack of a need to absorb development costs (which can be HUGE).

Which finally leads us to our fourth bullet point: how do we prevent the duplication (or cloning) of the peripherals?

The Renesas Board ID solution can address this in a very powerful and simple way.

The Board ID solution provides two distinct and important components. One component is the Board ID security chip, and the other is the Board ID provisioning process. By incorporating a Board ID chip into the design of the capital asset and peripheral, a robust and highly secure means of authentication is introduced. Let's see how the authentication works (see [Figure 2](#)):

**Use Case: Usage Control**  
Authentic Peripheral Used – First Use



- 1. Board ID Security Chips Are Put Into The Host and Peripheral**
- 2. Once The Peripheral Is Attached And The Unit Is Powered On, The Host Issues An Authentication Challenge To The Peripheral.**
- 3. The Peripheral Sends Back An Authentication Response And Creates A Record Indicating The Device Has Been Used**
- 4. Once The Response Is Authenticated The System Becomes Fully Operational.**

*Figure 2*

The Board ID chips come pre-loaded with keys as part of the provisioning process, which can be facilitated by Renesas Technology (either directly or through a Renesas Technology partner).

Traditionally, provisioning was facilitated by device manufacturers. This can become an unwieldy process in and of itself. By providing the provisioning process as part of the entire Board ID solution, the medical device manufacturer can focus on the functionality of the device rather than the sometimes complex task of managing security solution implementation and management.

What do we accomplish with this solution? In terms of ISO 14971, we directly address the very real risks associated with the introduction of a counterfeit or unauthorized peripheral entering the supply chain, as well as implementing a mechanism for insuring that a peripheral is not used past a pre-determined useful lifespan. If a peripheral does not contain a provisioned Board ID chip, it will fail to function when used with the capital asset since there is no way for authentication to occur in the absence of a provisioned Board ID chip. If the time and/or number of preset uses have expired, then the peripheral will also fail to authenticate.

What about risks associated with overseas manufacturing? The allure of the low manufacturing costs associated with going overseas is hard to pass up, but the associated risks increase dramatically when facilities are moved to places like China. If a manufacturer must manage the security of such facilities overseas, the cost benefits could quickly evaporate as the overhead associated with management costs escalates. Relying on the use of foreign management teams is risky at best, since their loyalties may indeed be skewed towards their own interests (i.e., family, friends, “entrepreneurship”).

The inclusion of provisioned Board ID chips within the manufacturing process can effectively eliminate the ability of counterfeiters to successfully introduce an unauthorized product into the supply chain.

It is extremely important to understand the need to have a robust security solution in place proactively (rather than reactively) because if a counterfeit item enters the supply chain, it could be years before a device manufacturer overcomes the loss of revenue associated with such activities. This is extremely risky because the rapid advances in technology tend to make brilliant discoveries obsolete within a short period of time, and for a company to dedicate financial resources towards recovering a lost business model could mean the loss of all profitability.

In a worst-case scenario, a peripheral may be a Class II/III device, and the introduction of counterfeit Class II/III devices could (and more than likely would) mean exposing a patient to great harm. In this case, the reputation of the device manufacturer could be irreparably damaged. Even though it may indeed be provable that the peripheral was not authorized for use with the capital asset, the associated damages would more than likely eclipse any explanation put forth.

Additionally, in the case of timed and/or decremented usage business models, an end user may wish to extend the usability of the peripheral beyond what he has paid for. This opens up a potential market for rogue licensing “services” which may attempt to offer a means for end users to sidestep the time and usage limitations. This could indeed be a HUGE moneymaking opportunity for such rogue service providers (as is evidenced by the large profits made by those who have successfully hacked pay TV systems) and creates an enormous incentive to “beat the system.”

## **Use Case 3 – Secure Tracking**

Secure Tracking refers to a situation where a medical device manufacturer may wish to either track a capital asset and/or peripheral for the purposes of service and support, or (as in the [Usage Control Use Case](#)) securely manage a remote provisioning process.

In the case of a high cost capital asset, it makes a lot of sense to design it in such a way as to allow for a fairly long lifecycle from a hardware perspective and manage the features/functionality of the device through firmware (software running on embedded hardware). Rather than replacing a costly unit with new hardware (at great expense to the customer, and potentially to the manufacturer), an upgrade can be handled through the secure downloading of new software code. Additionally, a common business model being deployed by hardware manufacturers today is the sale of support contracts with hardware, which are sometimes required as part of the licensing agreement for the hardware and can often exceed the cost of the hardware itself. Bear in mind that this same paradigm can be applied to peripherals as well. This business model introduces some interesting dynamics:

- The firmware must be delivered to the capital asset/peripheral in a secure manner.
- The cost of delivering the firmware to the capital asset/peripheral must be minimized wherever possible.
- The capital asset/peripheral must not be capable of accepting unauthorized (rogue) firmware.
- In the case of an end user who may have multiple capital assets/peripherals and only some of them are under support agreements, it is imperative to support only devices which are under a support agreement.

How can Board ID help? Let us begin by first examining how a firmware update could be delivered to a capital asset. How can a user be assured that the firmware update the device is receiving is indeed one that came from the manufacturer? One method would be to have the device manufacturer send a representative to the facility where the device is housed and have the firmware hand delivered via a secure token. In the case of a large capital

asset, this may not be an important issue, but if provisioning updates for peripherals this could lead to high costs associated with sending the representative to the location (i.e., labor and travel expenses).

This leads to the second bullet point, which refers to the need to keep costs low. A medical device manufacturer could send the firmware upgrade directly to the end user via a secure token, who could then perform the firmware upgrade himself through an automated and secure process, or the device could connect to a remote server hosted by the device manufacturer which could securely deliver the authorized firmware updates.

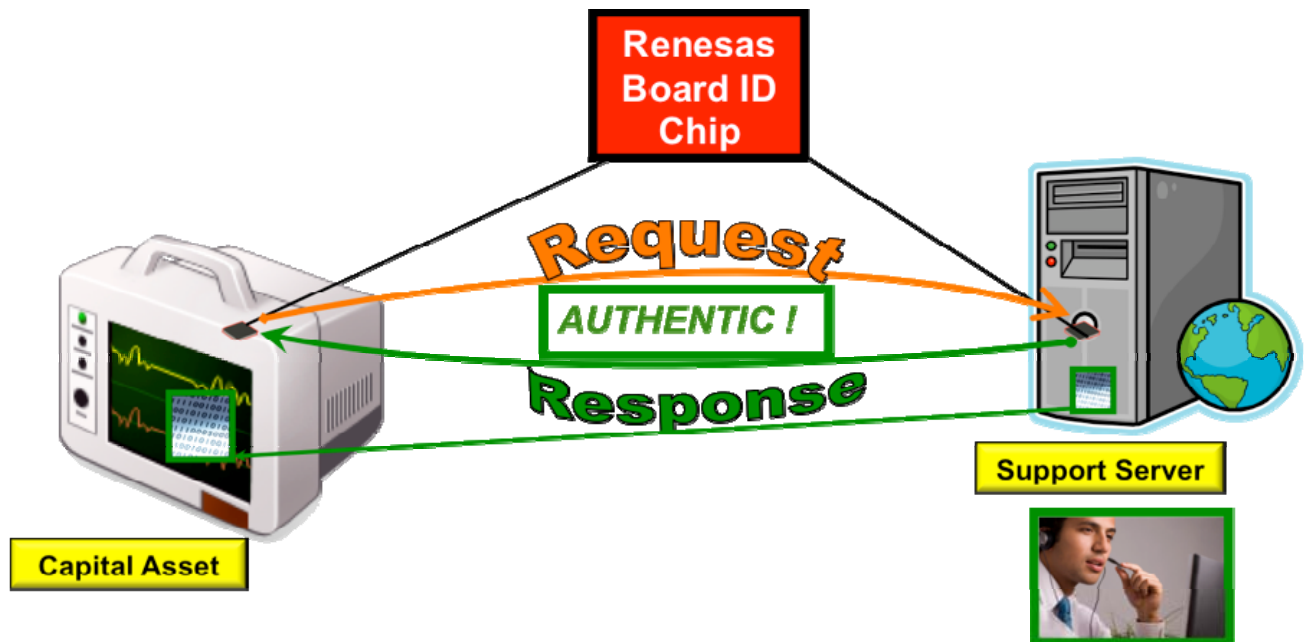
This, of course, leads to the third bullet point, which is the importance of preventing the device from being capable of receiving an unauthorized firmware upgrade. This point speaks not only to managing potentially catastrophic risks which could occur if the rogue firmware alters the functionality of a Class II/III device, but also to the potential revenue lost to someone who performs an unauthorized update on a device with authorized firmware. This can indeed be a worthwhile consideration in light of ISO 14971.

From a risk management perspective, the support of a device thought to be of one firmware profile may differ significantly from another firmware profile. This may lead to erroneous settings and improper usage. This speaks to the fourth bullet point, which is the management of support agreements. If an end user needs support for a medical device, the device could be securely authenticated via a remote server before the support staff delivers the support to the user. This serves to prevent incorrectly supporting a device with an unknown firmware revision, as well as insuring that costly support resources are not delivered for unlicensed devices.

The Renesas Board ID solution can address this in a very effective and simple way.

By incorporating a Board ID chip into the design of the capital asset and peripheral, as well as in support/provisioning servers managed by the device manufacturer, these challenges are dramatically curtailed. Let's see how the authentication works (see [Figure 3](#)):

### Use Case: Secure Tracking



- 1. Board ID Security Chips Are Put Into The Device and Support Server.**
- 2. The Device Sends A Request To The Support Server For Service (Updates, Support, Etc.).**
- 3. The Server Sends Back An Authentication Response.**
- 4. Once The Response Is Authenticated The Support Server Will Send Firmware Updates and/or Allow Support Services.**

*Figure 3*

The Board ID chips come pre-loaded with keys as part of the provisioning process, which can be facilitated by Renesas Technology (either directly or through a Renesas Technology partner).

Traditionally, provisioning was facilitated by device manufacturers. This can become an unwieldy process in and of itself. By providing the provisioning process as part of the entire Board ID solution, the medical device manufacturer can focus on the functionality of the device rather than the sometimes complex task of managing security solution implementation and management.

What do we accomplish with this solution? In terms of ISO 14971, we directly address the very real risks associated with the introduction of a counterfeit or unauthorized firmware entering the supply chain, as well as implementing a mechanism for insuring that a capital asset and/or peripheral are up to date from a support perspective.

The inclusion of provisioned Board ID chips within the manufacturing process can effectively eliminate the ability of counterfeiters to successfully introduce unauthorized firmware into a device, as well as prevent the alteration of firmware by someone with malicious intent (i.e., viruses or malware which could infect a network where a device shares a network connection).

It is extremely important to understand the need to have a robust security solution in place proactively (rather than reactively) because if a rogue firmware enters the supply chain, it could be years before a device manufacturer overcomes the loss of revenue associated with such activities. This is extremely risky because the rapid advances in technology tend to make brilliant discoveries obsolete within a short period of time, and for a company to dedicate financial resources towards recovering a lost business model could mean the loss of all profitability.

In a worst-case scenario, a peripheral may be a Class II/III device, and the introduction of rogue firmware could (and more than likely would) mean exposing a patient to great harm. In this case, the reputation of the device manufacturer could be irreparably damaged. Even though it may indeed be provable that the peripheral was not authorized for use with the capital asset, the associated damages would more than likely eclipse any explanation put forth.

## **Use Case 4 – IP Protection**

IP Protection refers to a situation where a medical device manufacturer has invested a great deal of time and money into the development of intellectual property and wishes to prevent the reverse engineering (and consequent duplication) of this valuable asset.

Modern electronic devices are generally composed of off-the-shelf parts, and what differentiates one manufacturer device from their potential competitors is the IP Protection the device manufacturer can “build into” the system. IP Protection over the last several decades has focused on legal protection (i.e., patents and copyrights), but the rapid rise in global marketplaces has created enormous challenges to legal protections. Lets examine the dynamics of IP Protection:

- The firmware of a device may indeed be the only factor differentiating the device from a potential competitor.
- Modern technology has dramatically reduced the time it would take for someone to reverse engineer the firmware.
- The market penetration for a device manufacturer needs to be maximized as quickly as possible to avoid competition in an ever-growing global market (i.e., you need to increase market share).
- If a counterfeiter succeeds in reverse engineering firmware, he must not have the ability to use this firmware to create counterfeits.
- Laws governing patents and copyright vary greatly on a global level, and it may be impossible to recover losses from someone who refuses to honor your patents and copyrights.

How can Board ID help? Let us begin by first examining how a counterfeiter might attempt to duplicate your device. If the components of your medical device are off-the-shelf parts, then finding the parts can be exceedingly simple. The cost of most hardware components is infinitesimally small compared to the cost of a finished medical device (to the end user), and this creates a fantastic market opportunity for a counterfeiter.

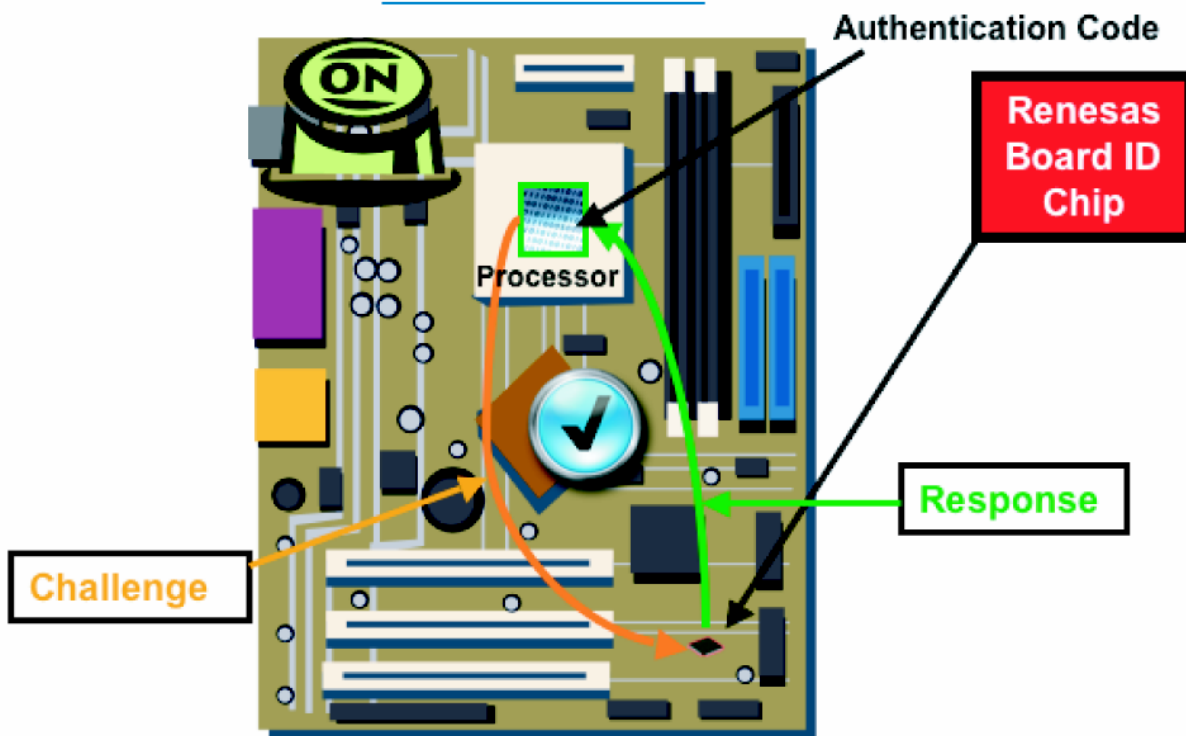
Modern desktop computers and software tools are all that are required for the reverse engineering of firmware. This can, in many cases, be accomplished within minutes if the hacker is skilled. If a counterfeiter is

highly motivated, he may even go as far as examining the contents of a chip through the use of a scanning electron microscope (freely available at many universities) to find where code is hidden. Once the counterfeiter has this code, he can then create duplicates of the devices. Attempts to challenge this in a legal environment can be extremely costly and time consuming, which could lead to the evaporation of any profits, as well as the irrelevance of the original manufacturer in the marketplace.

The Renesas Board ID solution can address this in a very effective and simple way.

By incorporating a Board ID chip into the design of the device, the challenges are dramatically curtailed. It is important to understand that when using a single Board ID chip for authentication (as we are illustrating here), it is important to use a microcontroller where the firmware is not easily inspected for the presence of statements which force it to authenticate to a Board ID, because if these statements can be identified, it may be trivial to simply delete them. Let us see how the authentication works with a microcontroller. (See [Figure 4](#)):

### Use Case: IP Protection



1. A Renesas Board ID Chip Is Put On The Device Motherboard.
2. Code Containing Authentication Instructions Is Loaded Into The Processor.
3. Once The Device Is Powered On, The Processor Sends An Authentication Request To The Board ID Chip.
4. Board ID Chip Sends Back A Valid Response.
5. Once The System Authentication Is Complete, The Device Becomes Operational.

*Figure 4*

The Board ID chips come pre-loaded with keys as part of the provisioning process, which can be facilitated by Renesas Technology (either directly or through a Renesas Technology partner).

Traditionally, provisioning was facilitated by device manufacturers. This can become an unwieldy process in and of itself. By providing the provisioning process as part of the entire Board ID solution, the medical device manufacturer can focus on the functionality of the device rather than the sometimes complex task of managing security solution implementation and management.

What do we accomplish with this solution? In terms of ISO 14971, we directly address the very real risks associated with the introduction of a counterfeit or unauthorized firmware entering the supply chain, as well as implementing a mechanism for insuring that a device cannot be easily duplicated by reverse engineering firmware.

The inclusion of provisioned Board ID chips within the manufacturing process can effectively eliminate the ability of counterfeiters to successfully introduce unauthorized firmware into a device, as well as prevent the alteration of firmware by someone with malicious intent (i.e., viruses or malware which could infect a network where a device shares a network connection).

It is extremely important to understand the need to have a robust security solution in place proactively (rather than reactively) because if a rogue firmware enters the supply chain, it could be years before a device manufacturer could overcome the loss of revenue associated with such activities. This is extremely risky because the rapid advances in technology tend to make brilliant discoveries obsolete within a short period of time, and for a company to dedicate financial resources towards recovering a lost business model could mean the loss of all profitability.

In a worst-case scenario, a device may be a Class II/III device, and the introduction of rogue firmware could (and more than likely would) mean exposing a patient to great harm. In this case, the reputation of the device manufacturer could be irreparably damaged. Even though it may indeed be provable that the device was not authorized for use with the capital asset, the associated damages would more than likely eclipse any explanation put forth.

© 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