White Paper

A Platform Approach to Securing Your Medical Devices

Kaushal Vora, Marketing Director, Healthcare & Energy Harvesting Solutions, Renesas Electronics

Mark Schaeffer, Sr. Product Marketing Manager, Security Solutions, Renesas Electronics

November, 2017

Abstract

Problems and chaos created by the rising barrage of malicious hacking events make it clear that achieving solid cybersecurity protection should be a top priority for OEMs developing connected medical devices. A key product design challenge is to implement sufficiently effective security measures within cost budgets while producing products that are safe, easy to use and flexible—devices that also comply with regulations and can be manufactured and deployed at scale.

After briefly covering trends and issues affecting the healthcare industry, this paper focuses on security-related measures for safeguarding IoT healthcare products that communicate with network resources and the Cloud. The discussion also covers a platform approach to system design, a methodology that medical industry OEMs can use to accelerate product development, reduce engineering risk, and supplement regulatory approval among other important benefits.

Introduction

The "Internet of Medical Things" as part of the larger "Internet of Things" (IoT) has the potential to leapfrog the ways in which people around the globe receive care. Medical devices built with advanced technology can do more than just improve the quality of care and patients' outcomes. They can also substantially lower costs and facilitate the development of more effective drugs and therapies.

However, unless it's done correctly, this "IoT-ization" of electronic medical devices can have significant ramifications. For instance, it can expose patients and possibly the critical healthcare infrastructure to hacker attacks and security breaches. The number and severity of security breaches are increasing, with malfeasance occurring on a regular basis. A prime example is the "WannaCry" ransomware attack, which affected over 150 countries and disrupted Britain's National Health Service.

Given this reality, the current state perhaps might be more accurately described as the "Internet of *Insecure* Medical Things". Fortunately, though, any weakness and vulnerabilities can be greatly mitigated by the diligent application of the appropriate security measures.

Chief among the political, social, economic and technological factors that have affected and rapidly changed the environment in which healthcare and medical devices operate are the following:

- Increasing pressure to make healthcare more affordable and efficient
- Globally aging populations demanding care, with increasingly more of it provided at home
- Rapid digitization, stimulated by government initiatives like HITECH & HIPAA
- Increasing integration of devices and backend systems (EHR, PACS)
- New and quickly evolving methods for care delivery
- Greater expectations of mobility and anytime access
- Increases in targeted, sophisticated attacks on critical infrastructure elements

These factors are forcing systems to evolve from single-point, standalone implementations to inter-connected systems-of-systems. As a result, the network layer has to perform multiple tasks. It must reliably handle unique and radical variations across organizations, successfully integrate medical and non-medical grade devices, and seamlessly interface new and legacy devices. Also, despite the fact that applications and data are increasingly migrating to the cloud, data still remains fragmented across multiple systems that aren't necessarily interoperable and adjoined.

Everyone in the healthcare field today faces multi-faceted technical and business challenges. In particular, medical device manufacturers are scrambling to meet industry needs while keeping pace with changing application needs and regulatory requirements. Simultaneously, the OEMs face shortages of qualified workers and are pressed to rapidly evolve manufacturing processes. Other OEM challenges include keeping pace with and adapting new government regulations.

Until recently, the regulatory process mainly focused on patient safety and basic essential performance. It did not take into account—or screen for—security related controls. Fortunately, technical standards and regulatory thinking concerning cybersecurity issues seems to be converging and maturing.

The timeline below (Figure 1) shows notable events in medical device cybersecurity standardization in the U.S. over the last five years. In 2014, the FDA released pre- and post-market guidance for medical device cybersecurity based on the NIST cybersecurity framework. More recently, technical standards such as DTSec and UL CAP (UL 2900) have emerged. These standards seem to be well aligned with regulatory thinking and other fundamental standards and processes used for medical device design.

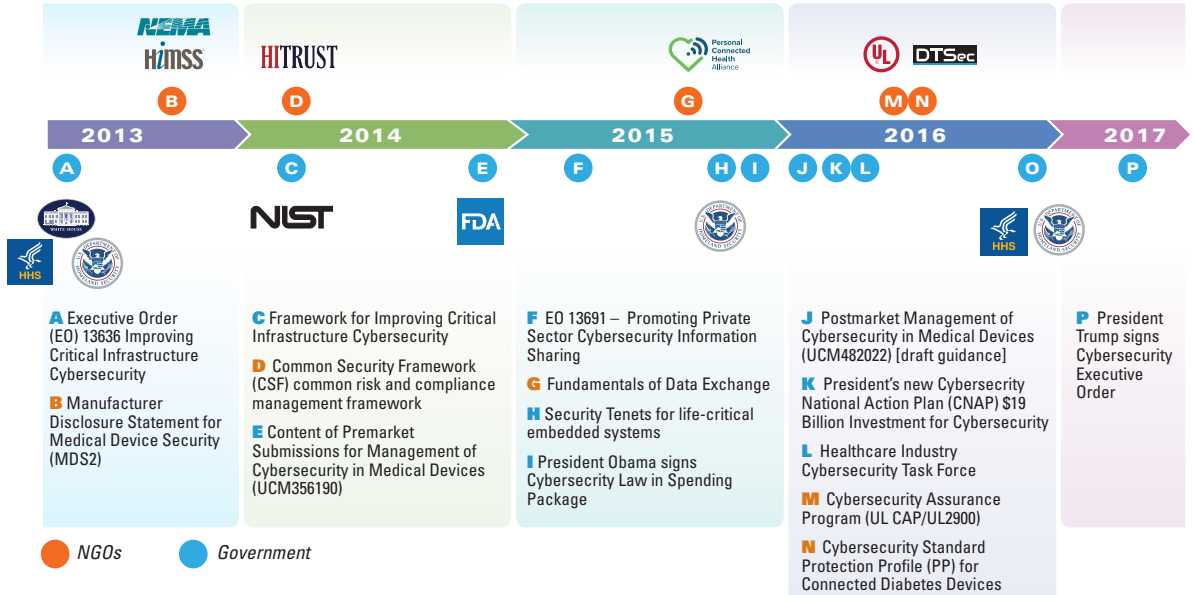

Figure 1. *Progression of regulations and standards aimed at improving the cybersecurity of medical devices.*

Ultimately, medical device security is all about achieving the business objectives of the healthcare industry. Those objectives include ensuring patient safety, maintaining long-term compliance, accommodating customers' requests for information (due diligence), and minimizing liabilities by adhering to the best practices in use today. With security now deeply embedded in the regulatory process, everyone involved in this field must address the issue directly and effectively. Therefore, planning for compliance and implementing best practices have to proceed hand-in-hand.

Security Problems and Challenges

Here are the most important problems and challenges affecting the cybersecurity of embedded medical devices today:

- **Malware** – Malware is malicious software that creates procedural abnormalities that might result in patient injury or death or cause disruptions that damage critical equipment. Thus, it is essential to ensure that the firmware in a medical device comes from a known and authorized source and has not been modified. Mechanisms must be in place to ensure the integrity of the firmware that has been flashed/installed in the manufacturing process. Additionally, safeguards must prevent that firmware from being modified without proper authorization after the medical product is deployed in the field.
- **Securely updating firmware in the field** – Standard practice in today's security environment is to have a secure, limited-access procedure in place for updating medical device security firmware as new vulnerabilities and bugs are discovered. Protections must verify that new firmware comes from a known and authorized source and hasn't been modified. Additionally, the security protocols must guard the firmware from being rolled back to a previously compromised, invalid version.
- **Unauthorized access to devices and services** – To make configuration changes and/or administer various services and treatments, a medical device can be accessed directly through its user interface or remotely via a network connection. To maintain safe operation, a verification process should be performed to confirm that any person or entity accessing the device is properly authorized.
- **Integrity and privacy of data** – Disclosure of private data causes serious problems for patients and medical staff, while exposing device manufacturers to legal liability. To forestall such difficulties, cybersecurity mechanisms must be in place to ensure that data-in-motion (data transferred over the Web or network) and data-at-rest (data stored on the device) come only from an authorized source (a valid Cloud server or authorized device) and hasn't been modified. Experts recommend enacting strong protection by encrypting the data with powerful algorithms.
- **Privacy – Anti-replay and inferring of contents of encrypted data** – The data security provided by encryption can be raised to a higher level via methods that help prevent anyone who is eavesdropping on a network connection from "replaying" the encrypted data and then modifying it for malicious purposes. Also, because specific data elements typically appear the same each time they are encrypted, cybersecurity mechanisms must prevent eavesdroppers from inferring the contents of encrypted data when that data is used repeatedly.
- **Protection of OEM firmware Intellectual Property (IP)** – In many cases it's important to encrypt the firmware installed in a medical device to make it impossible to decipher its contents. This safeguard is recommended for healthcare applications for several reasons:
  - ***To ensure that the product cannot be cloned:*** Unauthorized cloning compromises the OEM's revenue and brand. Typically, a major portion of a device's total intellectual property is contained in the firmware because many hardware components in the design are readily available to competitors.
  - ***To prevent unauthorized over-production:*** To protect an OEM's revenue, brand, and end customers, manufacturing facilities are typically authorized to produce only a designated number of products. Unless controls are in place to restrict production volume, existing hardware supplies and manufacturing equipment setups can be misused to produce counterfeit devices. Especially, strict controls must limit the number of devices that can be flashed with the OEM's secret firmware.

– ***To prevent disclosure of vulnerabilities that can be exploited:*** If the firmware in a device is hacked, an unauthorized analysis of its contents might uncover the weaknesses or bugs that are almost certain to exist, despite the best efforts of engineering teams to be rigorous in the development process.

Many ways exist to implement medical device security for preventing or minimizing cybersecurity problems. In general, the more security measures installed, the stronger the protection becomes. Primary security mechanisms include the following:

- **Cryptography** – Encrypting/decrypting data, authenticating identity, and verifying that data is unchanged
- **Secure Key/Data Storage** – Storing secret keys/data and ensuring that only authorized entities have access to them
- **Certificates** – Assigning identity to keys and then using rigorous procedures and technologies to safeguard that identity from accidental or malicious acquisition
- **Security Protocols** – Applying one or more of the many different types of security measures now available, each of which provides a specific functionality. The most basic security package typically just ensures identity. More sophisticated packages may contain mechanisms for encryption, data integrity verification, anti-replay features, and usage restrictions, among others.
- **System Design** – Controlling the way the components in a medical device communicate and work together. Although the individual components may be highly secure, security protections must prevent hackers from exploiting vulnerabilities in areas such as the installation and management of keys, data transfers between components, etc.

Security Provided by Multiple Protection Layers

In security applications, protection is most often implemented in multiple layers to prevent different types of attacks and provide redundancy and traceability. For example, a bank will have a lock on the front door, another one on the room containing the safe, and yet another one on the safe itself. To further deter criminals, a security guard, motion detectors, surveillance cameras, a forensics unit, and other protections might be employed as well.

Similarly, in the healthcare field, multiple levels of physical and operational security are applied to medical equipment. For instance, critical diagnostic or treatment equipment will be kept in a locked room and might be housed in a tamper-resistant or tamper-evident enclosure. Operational procedures will restrict access to the device and prevent its unauthorized use. Strong security precautions will also be applied during the device's manufacture, testing, transport, storage, and disposal.

For networked medical devices, maintaining security has become a dynamic rather than a static challenge. Providing effective, up-to-date protection is absolutely necessary, and doing so is a major challenge. Today it is vitally important to augment basic legacy security measures with a Technology Security Stack (see Figure 2).

Redundancy is also essential, because hackers often use multiple attack points. For example, even if a critical medical product employs robust Wi-Fi network security, this might not be the case for some devices that communicate with it. Even if an attacker gains access to an authorized device on the communication link, security mechanisms should prevent data from being stolen from the critical piece of medical equipment.

.

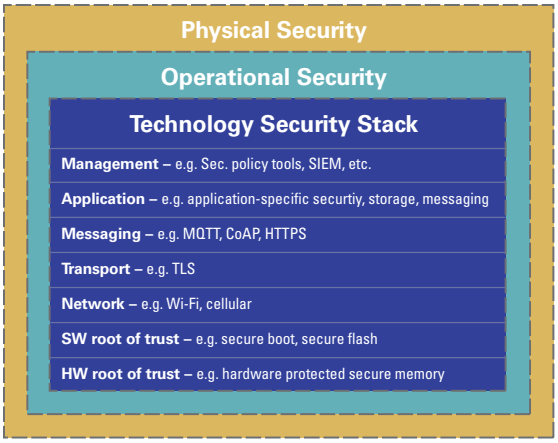

Figure 2. *Technology Security Stacks contain multiple layers of protection that combine to guard medical devices against different types of cyberattacks.*

As Figure 2 shows, a typical technology stack in an IoT-based medical device contains the following elements:

- **Hardware Root of Trust** – Robust security starts with a microcontroller that stores keys, code and data securely in its on-chip hardware. This prevents hackers from accessing or modifying that data through remote or physical attacks on the device.
- **Software Root of Trust** – Software trust typically begins with an immutable boot loader that guarantees that only valid firmware can run on the medical device or be flashed to it. This security mechanism may also include providing the device with identity and functions for decrypting firmware that has been secured with encryption.
- **Network** – Most security implementations include some level of wireless network encryption (Wi-Fi, Cellular, Bluetooth, etc.). But this is only a first line of defense to keep outside entities from getting on to the dedicated healthcare network. Typically, many devices are connected inside that network, and to maintain security, these devices have to be isolated from each other via other security layers. Also, it should be understood that the healthcare network doesn't provide any cybersecurity protection for communication via the Internet. That's because wireless security often terminates after a modem or router connects to the worldwide Web.
- **Transport** – Fortunately, many protocols exist for securing data being transferred over the Web. One, the familiar "https", is a secure web browser connection over TLS, the transport security protocol that replaced SSL and is also used in machine-to-machine communication. TLS applies authentication certificates to establish and verify the identity of parties involved in the communication activities. Thereafter, it encrypts the data being transferred and provides other security functions. TLS can be a single-direction function (connecting to a web browser), or a mutual mechanism (for an IoT device). Mutual operation is needed when both parties must authenticate each other.
- **Messaging** – The "http" communication protocol is a web browser messaging method for sending messages over a network. As mentioned above, the "https" protocol is similar, but includes TLS transport security. MQTT and CoAP are messaging protocols typically used for IoT device machine-to-machine communications. They are designed to be simple and efficient, features that are especially important in wireless environments with low-power, battery-operated devices. The security that MQTT and CoAP provide in the messaging layer is usually a username/password; however, these protocols can also deliver enhanced capabilities such as anti-replay and message integrity.
- **Application** – Medical product developers most often take advantage of available, well proven security products and solutions instead of building new designs from scratch. However, each application is different and generally will require a specifically tailored set of security protections. Common modifications include encrypting data on the device, using application-specific protocols, and requiring user logins where transport security typically manages device identity. Other device-specific modifications include functionality restrictions based on the user's identity, licensing features, and anti-counterfeiting measures. Medical product development teams are advised to use security technologies such as encryption and key storage directly, rather than assuming all the security they need is provided through other protocol layers; e.g., lower protocol layers do not encrypt data on the device and do not ensure data is secure in the Cloud ecosystem.
- **Management** – Enterprise tools, such as managing security policy across the organization, detecting and applying Security Information and Event Management (SIEM) tools to handle security events and anomalies, have long been common practice in the healthcare field. Today, SIEM tools are increasingly being integrated with new IoT environments.

Each layer in the Technology Security Stack may use one or more keys and certificates, each of which must be provisioned securely. The optimum provisioning mechanism for those keys varies, depending on the layer in the stack and on corporate policies and procedures for managing keys and identity. A Wi-Fi password, for instance, often is widely distributed inside an organization and is easy to set up. By contrast, assignments of TLS keys or user keys should be more rigorously controlled. That authorization process commonly requires a validation procedure such as sending a verification code to an email account or mandating that a validated user log into a management system to gain access to provisioning a critical key.

A sobering reality must be faced here, though. Achieving bulletproof cybersecurity protection for a medical product—or any networked product for that matter—is basically impossible, especially over an extended period of time. Nevertheless, excellent cybersecurity protection is readily attainable. The challenge is to find an acceptable balance between implementing effective security measures, while also meeting cost budgets and allowing reasonable operational complexity and acceptable levels of efficiency.

Different security issues arise in different stages of a medical device's life cycle:

1. **Provisioning identity** – This is done infrequently (perhaps once a year or less), and it likely involves a procedure to determine identity before issuing an authorization certificate. That certificate may be securely stored on the device or in an encrypted USB token when used to identify a user.
2. **Everyday operations** – Once a verified identity is established, security operations are streamlined. Two types of procedures are commonly used. Security can be implemented by quickly validating an identity, such as a certificate, that was established during the provisioning; this is called single-factor authentication. Alternately, a stronger security protocol will require the user to enter a password. This is referred to as 2-factor authentication because it combines a certificate with a password. It is an increasingly popular method for ensuring that protected medical equipment cannot be used by unauthorized personnel who might have stolen one of the factors; e.g., a USB identity token, or even a user's biometric fingerprint.
3. **Disposing of a device or account** – When a networked medical device reaches its end of life, it's prudent to revoke the product's identity. Disabling a certificate or login account can do this. Another recommended security practice is to have a mechanism to securely discard the data and/or encryption keys on the device during the disposal process.

Security Implementation in IoT-based Medical Devices

When building IoT-based products for healthcare applications, cybersecurity mechanisms must be incorporated into the design right from the very beginning of the development process. Three questions will facilitate efforts to create robust security solutions:

What kinds of attacks are expected?

Broadly speaking, medical devices are subject to four types of cyberattacks:

- **Remote Attacks:** Hackers gain access to the device through the Web or through a virus on a USB device. Remote attacks, the most common type, are within the operational scope of any connected medical device. They always must be considered in the product's design.
- **Physical Attacks from unauthorized users:** If it's possible for a hacker to gain physical access to a medical device, appropriate Cybersecurity protection should be installed to provide the maximum practical level of safety. The fact is, though, that when hackers attack a device using invasive tools like probes and drills, no security mechanism might be strong enough to prevent problems. However, architects need to consider that if hackers have physical access to a facility, there is a lot more damage they can do besides hacking a device, so a level of physical security is typically always required.
- **Physical Attacks from authorized users:** In certain cases, valid users might have reasons to hack protected devices, but such hacks need to be controlled. Examples of such situations include stopping the counterfeiting of peripherals or restricting the number of times that a peripheral can be used.
- **Physical Attacks from criminal organizations:** Hackers might want to do more than merely cause damage to a specific device. Instead, they might try to steal the device and the highly valuable data hidden within it such as firmware, sensitive keys, and patient information. Their objective may also be to cause injury or damage to hurt the brand.

What are the security objectives for the product?

Medical devices that provide critical lifesaving or life-sustaining functions require much stronger security features than equipment used for lower-level applications. Products that are always operated under the supervision of healthcare professionals need security measures different from those

appropriate for home-use products. Also, devices that operate under very strict compliance requirements most often will have very particular security issues. These factors, among others, drive the tradeoffs that product developers must make as they seek the optimum balance between security strength on one hand, and cost and operational complexity and flexibility on the other.

How will the layers of the security stack be implemented?

Many components of the technology security stack are available from trusted vendors. Developers of medical products should consider a range of issues when evaluating the choices. Those issues include the ease of integrating the necessary components, how application-specific security is implemented, the need for redundancy, and whether or not the medical device requires transaction security such as anti-replay and integrity at multiple layers. Another important consideration is the extent to which security is maintained as data flows around the healthcare system that uses the equipment; i.e., from the device to the Cloud and back again.

Are physical attacks in scope? At a minimum, all IoT connected medical devices should incorporate protection against remote cyberattacks. Additionally, security against physical attacks might be mandatory in certain applications. The nature of the threats being addressed determines the costs of installing the appropriate protection measures (see Figure 3).

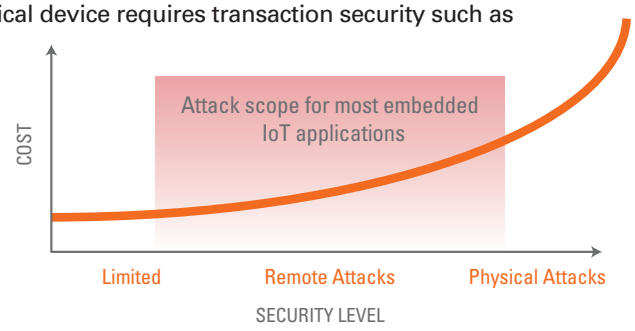

Figure 3: *The cost for cybersecurity protection varies according to the type of threat being addressed. Realistically, however, some physical attacks probably cannot be deterred except at a prohibitively high cost*

Product Design Tips for Robust Security

Before the security measures incorporated into a new medical device are decided, it's useful to understand how to design the most robust security solution. Armed with that knowledge, product engineers can select optimum sets of cybersecurity protection mechanisms for ranges of target applications.

The strongest medical device security solutions use a security architecture that establishes an unbroken chain-of-trust from the silicon on the device's circuit boards to the cloud that stores patient data. Each part of the security architecture relates to the previous one, as Figure 4 shows.

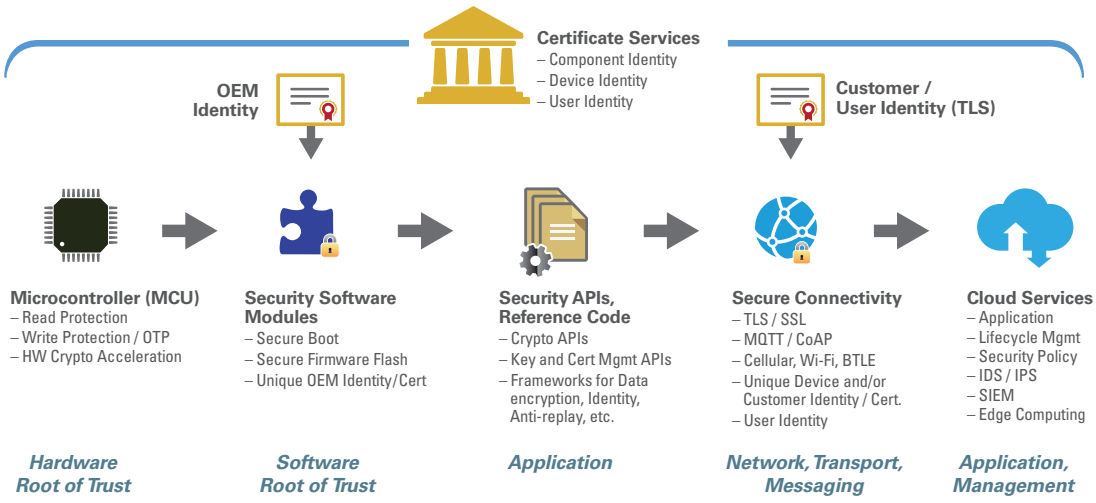

Figure 4: *The security architecture of a robust IoT-based medical device owes its strength to the incorporation of multiple protection mechanisms.*

Relationships between elements of the security architecture can be technological or operational, or both. A technological relationship, for instance, won't allow the application to execute unless the software root of trust validates a digital signature on the application firmware. By contrast, an operational relationship exists when control procedures demand that the software root of trust be installed only on microcontrollers sourced from a known vendor via a reliable distribution channel. To obtain maximum security, combinations of both technological and operational security can be applied.

Functions performed by elements of the security architecture include those described below:

- **Microcontroller (MCU)** – A special microcontroller serves as the core element of the cyber-protection architecture for an IoT networked medical device. It contains hardware features that ensure that only secure code can access vital data such as keys. Typically, code stored on the chip is partitioned into non-secure/general and secure memory areas. The latter is made as small as possible to reduce the firmware's "attack surface". If a hacker manages to break into the system—through the communication layer, for example—access to the secure data will be denied because there is a separation of that data from most of the firmware. In addition, one-time-programmable (OTP) memory prevents the boot loader from being modified, as well as any root keys that must remain unchanged over the life cycle of the product, like the root keys that create and validate other keys.
- **Software Security Modules** – The software root of trust starts with the previously mentioned boot loader that's secured in OTP memory. The boot loader verifies that only valid firmware is flashed onto the device in manufacturing operations and during field updates. As an extra level of protection, the firmware is rechecked each time the medical device is booted up. This verification procedure may be a prerequisite to using the device, accepting data from it, or issuing other certificates, including TLS certificates. Most often the OEM identity is flash-installed into the medical product by a unique device certificate signed by the OEM's Certificate Authority. This allows only the OEM to perform flash updates; it also confirms to the OEM that the product is a known and trusted one. Tools and infrastructure are provided to allow the OEM to sign and optionally encrypt firmware and install the OEM identity.
- **Security API's Reference Code** – For healthcare equipment, product development teams often increase security above and beyond the standard components such as TLS and the software root of trust. They tailor the device's security architecture to the exact requirements of its specific application. Features implemented in medical devices include the following:
  - Crypto API's that take advantage of any hardware acceleration built into the device. Cryptographic hardware acceleration functions have major advantages; they deliver faster performance than software crypto libraries while using less power, occupy smaller memory footprints, and contain optimized code.
  - Protection functions that isolate code that requires cryptographic operations. The recommended design practice is to map that code to secure memory so it can access secure keys and data that are protected by the MCU.
  - Encryption functionality to protect data, typically in two ways. One is to encrypt any data that remains on the medical device so it can't be modified. The other is to encrypt data that is shared with the cloud or other devices so only certain device or certificate users in the Cloud have access to that data. It can also prevent unauthorized modifications, validate identities, and perform anti-replay tasks.
- **Secure Connectivity** – Many products and services are available to facilitate designing secure connectivity into medical devices. These well-established offerings are use-tested, time-proven standards. To take advantage of the MCU's cryptographic acceleration and secure key and data storage, for example, engineering teams can install third-party libraries, many of which can be optimized for the specific microcontroller through a Hardware Abstraction Layer (HAL) that allows certain functionality to use hardware specific interfaces. They can take advantage of connectivity options that include wireless technologies such as Cellular, Wi-Fi and BTLE. Transport technology choices include TLS, which requires a certificate identifying the device or end customer. Messaging technology options include MQTT, CoAP, and HTTPS.

- **Cloud Services** – IoT based medical equipment often links to an application running in the Cloud. The Cloud-based software interoperates with the medical device's protection mechanisms and provides its own set of security services. Examples can include management functions such as enrolling new devices, performing analytics, detecting anomalies, generating incident responses, and enforcing security policies, as well as providing day-to-day services.
- **Certificate Services** – Certificates are provided by a Certificate Authority (CA) that assigns identity, which in turn are used to provide identity to a device. Procedures for issuing certificates vary depending on the application and are tailored to the OEM's or customer's security environment and procedures. Often multiple CA's are used. It's common for an OEM to use one CA to establish an "OEM Identity" to confirm that a medical product is a trusted device, while the end customer uses a different CA to verify that the product is a device authorized to operate in its network environment. To implement a Certificate Authority, a customer can use a public Cloud CA like Digicert/Semantic, or it can use its own CA in the Cloud. Alternately, the customer can deploy a "Delegate CA" onsite in a manufacturing facility that coordinates with the master Cloud Server. Other certification methods are also possible.

A Prefabricated Foundation for Product Designs

Medical device manufacturers often find it impossible to create every aspect of their product designs from the ground up. The highly competitive sales environment and increasingly challenging regulatory environment make time to market a key factor for a product's success. OEMs have discovered that engineering teams are the most productive when they are allowed to focus on achieving value-added differentiation for the end product, rather than developing non-differentiated, foundational software that does not translate to additional product value. Without a doubt, economic realities favor medical devices built using a platform approach because the engineering time the platform saves enables more innovation.

A brief explanation of what's meant by the term 'platform' is helpful here. At the core of most medical devices is an electronic system typically comprised of three key elements:

1. The hardware: microcontroller or microprocessor
2. Standard software: device drivers, frameworks, libraries, operating systems, middleware, stacks, etc.
3. Application-specific software: the science and intelligence behind the acquisition and measurement of external physical information and subsequent decision-making, as well as the clinical workflows for a specific device. (In other words, it is the proprietary intellectual property behind many of the OEM's marketing advantages—its 'secret sauce'.)

This document collectively refers to these three elements as the 'Platform' (see Figure 5).

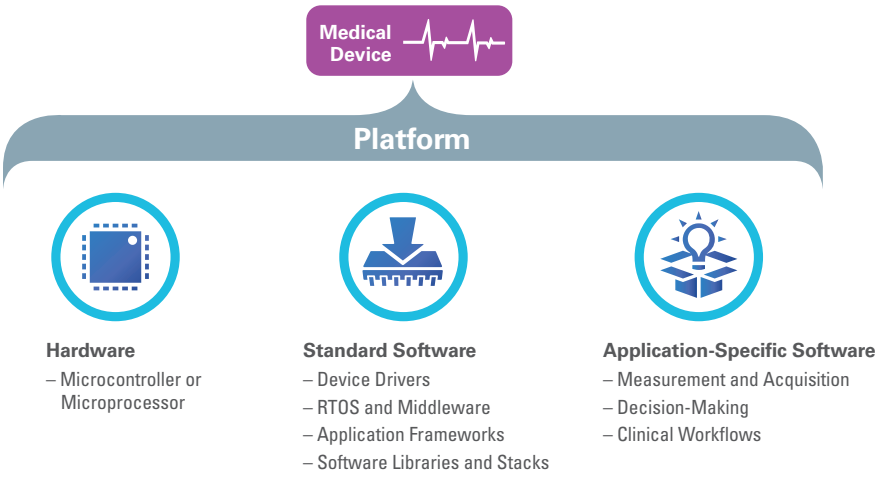

Figure 5: *Elements comprising the Platform of an electronic medical device.*

Renesas Synergy™: A Platform Approach to IoT Security

A prime example of a trusted cybersecurity protection product for accelerating the development of secure medical products is Renesas Synergy. This popular Arm®-based system platform provides IoT solutions for connected devices (see Figure 6).

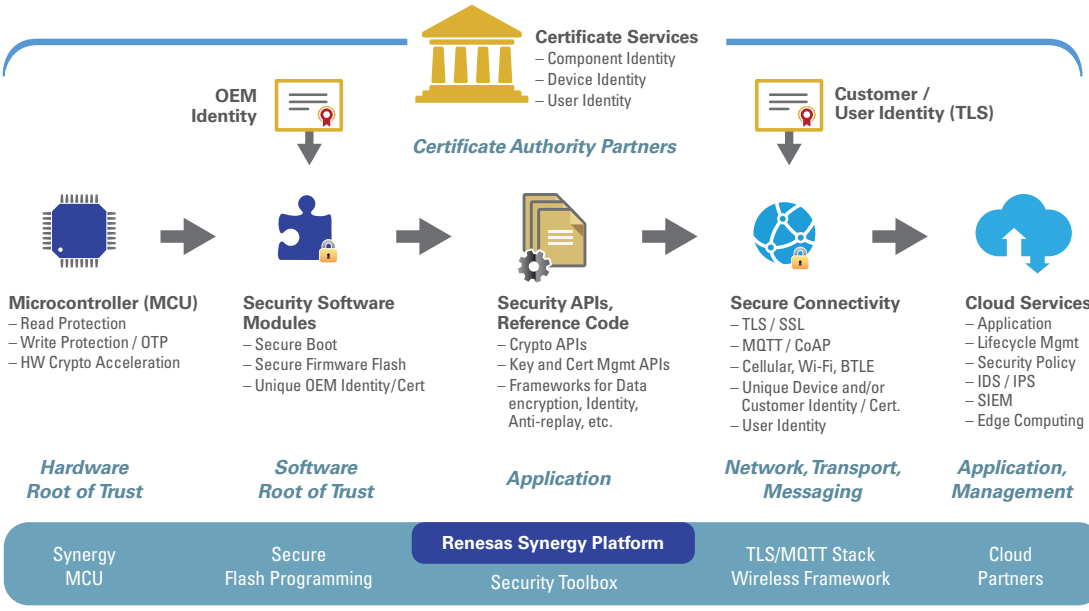

Figure 6: *Renesas Synergy covers all aspects of the Technology Security Stack. It implements robust security features while reducing design risk and shortening the time required to develop and test IoT-based medical products.*

Renesas Synergy is based on an MCU that has on-chip security hardware features. The chip is bundled with drivers, wireless connectivity capabilities, and a rugged, reliable RTOS. Its development tools and support libraries include the Synergy Software Package (SSP), which is optimized for the MCU. Additionally, a vibrant community of industry partners supports this IoT-focused platform. Partner vendors support customers that use the Synergy Platform by selling a diverse collection of valuable HW/SW products and reference designs.

OEM engineering teams producing networked medical devices gain significant advantages by adopting a platform approach to system design. Renesas Synergy lets them build upon the c apabilities and reliability of a proven open security solution. The Synergy Platform delivers robust security in conformance with the latest versions of industry standards and best practices. It is a solid, stable foundation for advanced, differentiated world-class health care products.

Here are key features of the Renesas Synergy Platform:

- **Synergy MCU** – The Renesas MCU forming the basis of the Synergy Platform provides hardware security features previously available only in dedicated Secure Element chips that were developed for specialized, highly secure identity application's support for SIM cards, VPN tokens, etc. The MCU's high level of integration eliminates the need for another chip, a socket, and a communications bus (I^2C bus). This reduces the size, complexity, power consumption, and cost of the circuit board. The special Synergy MCU also cuts system-engineering expense and decreases component costs, making it possible to add cybersecurity protection to a wider range of medical devices at little or no extra cost.

  The Synergy MCU delivers the following features:

  – Memory read/write protection via isolation of code into non-secure/general and secure segments, the latter being protected at the hardware level via a Memory Protection Unit

  - Write-Once (OTP) memory protection at the hardware level via a Flash Access Window feature
  - Hardware cryptographic acceleration supporting Asymmetrical Encryption for Identity functions, Symmetrical Encryption for data encryption, Hashing for data integrity, and True Random Number Generation (TRNG) for performing key generation, security challenges and randomization
- **Secure Flash Programming Solution**
  - Software root of trust Secure Boot and Secure Flash functions that Renesas provides as a reference design
  - Root of trust and unique OEM identity keys stored in Write-Once memory and protected against reads by a Memory Protection Unit
  - Technology partners that provide high-speed programming equipment for manufacturing (Data I/O), as well as tools for encrypting and signing the firmware (Secure Thingz)
- **Security Toolbox**
  - High-level Cryptographic APIs
  - A simple Certificate Authority that illustrates the generation of keys and certificates
  - Reference Design examples show how to use asymmetrical cryptography for digital signatures (verifying identity and integrity) and key exchange, explain the use of symmetrical cryptography for encryption and integrity, and describe how to apply hashing to ensure integrity
- **TLS/MQTT Stack, Wireless Frameworks**
  - A TLS/MQTT stack verified by Renesas and optimized to take advantage of the MCU's security capabilities
  - A wireless framework for Wi-Fi, Cellular, and BTLE that provides APIs with a hardware abstraction layer, allowing implementations to remain the same regardless of the wireless hardware being used
- **Cloud Partners**
  - Secure Connectivity to major cloud providers over TLS/MQTT
- **Certificate Authority Partners**
  - Firmware agents to generate keys and to request and download certificates from CA Partners

Summary

Security now is a major concern for medical device OEMs due to the rapidly changing IoT environment and the exponential rise in cybersecurity attacks. To be prudent, healthcare equipment OEMs must rank security on par with quality and safety. Fortunately, it is becoming easier to plan, design, and implement security on the embedded systems, which are at the heart of medical devices.

One favorable trend is that the standards landscape (DTSec, UL 2900, etc.) is starting to mature and better align with regulatory and business goals. This movement is making security objectives more consistent across the industry. System design platforms such as Renesas Synergy now allow OEMs to build products on proven security foundations, reducing engineering risk, development time, and cost, while achieving better security and reliability.

Further, design aids are helping medical OEMs start or continue the vitally important process of improving the security of their networked devices. Those design aids include definitions of best practices, regulatory guidelines like the FDA's "pre" and "post" market security recommendations, and the electronic industry's latest technical standards.

The factors just mentioned encourage investments in solutions that protect both brands and customers against the latest challenges by hackers. More and more programs are moving to a platform design approach for new product development. Experience shows that products such as the Renesas Synergy Platform accelerate innovation and enable the creation of exciting new applications to address real world challenges.

To learn more about Renesas' solutions for medical devices, please visit

https://www.renesas.com/en-us/solutions/home/healthcare.html

or contact your local Renesas sales representative.

Document No.: R01PM0049EU0000-SYNERGY