

# Addressing Gaps in Medical Device Security

Key Requirements for Building a Secure Code-Signing  
Infrastructure



White Paper

# Contents

<b>02</b>	<b>Executive Summary</b>
<b>03</b>	<b>Introduction: Evolving Technologies and Threats in Healthcare</b>
<b>03</b>	<b>Vulnerabilities in Medical Devices Being Exposed</b>
<b>04</b>	<b>Opportunity: Importance of Code Signing in Addressing Medical Device Vulnerabilities</b>
<b>04</b>	<b>Secure Keys - the Foundation of a Secure Code-Signing Environment</b>
<b>05</b>	<b>The Role of HSMs in a Secure Code-Signing Environment</b>
<b>05</b>	<b>Conclusion</b>
<b>05</b>	<b>About Thales</b>

## Executive Summary

In healthcare organizations today, medical devices are increasingly being targeted, and proving susceptible to attack. These medical devices can contain sensitive medical and payment information, and they can provide capabilities for monitoring and controlling patient health—so they represent vital assets. By establishing a secure code-signing infrastructure, medical device manufacturers can address a range of security gaps, and a significant market demand. This paper reveals why code signing is so vital today, and it offers insights for establishing a code-signing infrastructure that effectively secures medical devices.

# Introduction: Evolving Technologies and Threats in Healthcare

In just a few years, the makeup of the technology infrastructure within healthcare organizations has undergone significant change. While these technology transitions can usher in unprecedented benefits—including improved staff efficiency, better patient results, and more—they can also present security professionals and medical device manufacturers with substantial security and patient privacy challenges. Following are just a few of the transformations that have been happening, and their respective risks:

- **Increased digitization.** More than ever, healthcare professionals, administrators, and management are now reliant on a wide range of applications, which are being accessed through an increasingly diverse set of platforms, including laptops, smart phones, and tablets. In addition, the provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act—in particular, the expanded formulation and usage of health information exchanges (HIEs)—have spurred an increased investment and reliance upon digitized health records. Consequently, more healthcare information is available digitally than ever before. The increased digitization of patient information means it is exposed to cyber attacks from both inside and outside the organization.
- **Increased interconnectedness.** Now, all manner of systems—from a physician's tablet to an implanted medical device, from a back-end server in a data center to a diagnostic device—are connected to the healthcare organization's wireless network. The array of wirelessly interconnected systems and devices creates a fluid, dynamic environment that is difficult to secure. Plus, this interconnectedness creates a scenario where the vulnerabilities of one device can enable an attacker to gain access not just to any sensitive controls or data available on that device but also to other systems on the network.
- **Increased reliance on common software.** Many medical devices are now running on at least some component of common software, or are connected to a system that is. This proliferation of broadly available applications, operating systems, and other software can make medical devices increasingly susceptible to the cyber attacks that plague other enterprise systems. Further, in some cases, this software isn't being updated with security patches in a timely manner, either due to resource constraints among hospital staff or restrictions that can be imposed by regulators and device manufacturers, which can exacerbate the risks.

## Vulnerabilities in Medical Devices Being Exposed

Within healthcare organizations today, a broad assortment of networked medical devices are being employed—and relied upon daily for a range of critical tasks. This can include implanted medical devices that are used to monitor and treat conditions within the individual's body, such as pacemakers, drug delivery systems, and neurostimulators. In addition, there are many other networked devices employed within hospitals, including rolling workstations, ventilators, portable ultrasound units, and x-ray machines.

These devices, and the healthcare organizations that deploy them, are increasingly being targeted and proving vulnerable to attacks. Consider the following statistics and examples:

- Ninety-four percent of healthcare organizations surveyed have suffered from a breach during a two-year period.<sup>1</sup>
- Nearly three-quarters of healthcare organizations don't secure medical devices—in spite of the critical functions they perform and the sensitive data they may contain.<sup>2</sup>
- An ethical hacker demonstrated how medical devices that have been implanted in patients, including an insulin pump and a heart defibrillator, could be compromised.<sup>3</sup>
- Given the increasing number of unpatched software running in medical devices, malware in these systems is now "rampant".<sup>4</sup>

<sup>1</sup> Ponemon Institute, "Third Annual Benchmark Study on Patient Privacy & Data Security", Page 5

<sup>2</sup> Healthcare Information and Management Systems Society (HIMSS), "Anatomy of a Breach: Medical Devices Under Cyber Attack", Gary Weiner and Axel Wirth, September 20, 2013

<sup>3</sup> Healthcare Info Security, "How to Minimize Medical Device Risks", Marianne Kolbasuk McGee, November 29, 2012, [www.healthcareinfosecurity.com/how-to-minimize-medical-device-risks-a-5310](http://www.healthcareinfosecurity.com/how-to-minimize-medical-device-risks-a-5310)

<sup>4</sup> Forbes, "Hospital Medical Devices 'Rampant' With Computer Viruses", Adrian Kingsley-Hughes, October 17, 2012, [www.forbes.com/sites/adriankingsleyhughes/2012/10/17/hospital-medical-devices-rampant-with-computer-viruses/](http://www.forbes.com/sites/adriankingsleyhughes/2012/10/17/hospital-medical-devices-rampant-with-computer-viruses/)

# Opportunity: Importance of Code Signing in Addressing Medical Device Vulnerabilities

While the timing and nature of future regulation changes isn't clear, what is evident is that, in time, healthcare organizations will be subject to increasingly rigorous policies and mandates. The breaches and vulnerabilities being reported in the press make clear that, when it comes to security, the status quo won't be viable for long. The security gaps being exposed today should serve as a wake-up call to governing bodies, auditors, and security leadership. In addition, the HITECH act will continue to boost demand for more secure systems.

By leveraging medical devices that deliver more robust security controls, healthcare organizations will be able to address a significant gap in their security defenses. Those medical device manufacturers that can meet these needs for increased security will be poised to capitalize on a significant market opportunity.

In particular, medical device manufacturers can address an urgent market demand and expand market share by delivering medical devices that have the security assurances afforded by a robust code-signing environment. Through code signing, device manufacturers can establish a trusted ecosystem that enables timely, secure delivery of new software and code updates. As a result, device manufacturers can help customers mitigate the exposure associated with unpatched systems and devices.

Code signing represents a critical means for device manufacturers to establish a trusted environment for their customers. However, the code-signing environment has to be secure to fulfill this objective, and this requires that code-signing certificates are adequately protected.



## Secure Keys - the Foundation of a Secure Code-Signing Environment

In code-signing environments, public key infrastructure (PKI) technology is used to create a digital signature. The digital signature is based on a private key and the contents of a program file. In distributing its code, the device manufacturer packages the digital signature, either with the file itself or in an associated catalog file. Upon receipt of the signed code, users or devices will combine the file, certificate, and associated public key to verify both the identity of the file signer and the integrity of the file.

For device manufacturers managing these environments, safeguarding code-signing certificates is essential. If private keys associated with code signing are compromised, device manufacturers can be vulnerable to significant implications. In the near term, organizations have to contend with the high costs associated with damage control, including notifying customers, investigating the breach, and replacing code. Longer term, they can be exposed to lawsuits, erosion of customer loyalty, and increased customer churn to name just a few potential penalties. In addition, healthcare organizations and their patients are also clearly vulnerable if the code-signing environment is compromised—especially if implanted medical devices are in the picture.

## The Role of HSMs in a Secure Code-Signing Environment

In order to effectively secure the private keys used in code signing, it is vital for organizations to leverage hardware security modules (HSMs). Keys stored on general-purpose servers or other systems are too susceptible to unauthorized access and compromise. Storing keys in robust, tamper-evident HSMs can eliminate these vulnerabilities.

However, in order to maximize the security of private keys and other cryptographic assets, there are several critical requirements that HSMs must address:

- **Standards certification.** Device manufacturers should leverage HSMs that have security mechanisms certified to be compliant with such standards as FIPS 140-2 Level 3 and Common Criteria.
- **Secure key generation and storage.** HSMs should offer true secure key generation. The only place keys should ever be generated and stored in the clear is within the confines of the HSM.
- **High availability and reliability.** Given the critical, central role they play in the code-signing environment, device manufacturers should leverage HSMs that offer a range of capabilities for maximizing availability and reliability. This includes support for redundancy and failover, so even after a platform outage, cryptographic processing can continue uninterrupted. In addition, HSMs should offer remote backup features for disaster recovery.
- **Performance and scalability.** It is vital that HSMs can accommodate the performance and throughput requirements of manufacturers and their customers. For many device manufacturers, this will entail offering the scalability to support tens of thousands of keys.
- **Support for elliptic curve cryptography (ECC).** As manufacturers look to deliver smaller device form factors, the use of ECC, which provides significantly stronger cryptographic keys in a smaller key size, will grow increasingly prevalent. Therefore, security architects should look for HSMs that support the development of solutions that leverage the ECC standard.
- **Robust administrative access controls.** Establishing granular, robust control over administrative access and tasks is a critical security requirement. All administrative access should be controlled by multi-factor authentication. Further, HSMs should offer capabilities for separating administrative duties with multi-level access control and multi-part splits for all access control keys, which is essential in mitigating exposure to the damage that can be inflicted by a rogue administrator.

## Conclusion

By establishing a secure code-signing environment, medical device manufacturers can address some of the critical vulnerabilities customers are contending with today. Those device manufacturers that leverage robust HSMs will optimize the security of the cryptographic keys that represent a core foundational element of code signing, so they can better establish and sustain a trusted ecosystem for customers.

## About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.



#### Americas

Arboretum Plaza II, 9442 Capital of Texas Highway North,  
Suite 100, Austin, TX 78759 USA  
Tel: +1 888 343 5773 or +1 512 257 3900  
Fax: +1 954 888 6211 | E-mail: [sales@thalessec.com](mailto:sales@thalessec.com)

#### Asia Pacific – Thales Transport & Security (HK) Ltd

Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East  
Wanchai, Hong Kong | Tel: +852 2815 8633  
Fax: +852 2815 8141 | E-mail: [asia.sales@thales-esecurity.com](mailto:asia.sales@thales-esecurity.com)

#### Europe, Middle East, Africa

350 Longwater Ave, Green Park,  
Reading, Berkshire, UK RG2 6GF  
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550  
E-mail: [emea.sales@thales-esecurity.com](mailto:emea.sales@thales-esecurity.com)

> [thalesgroup.com](https://www.thalesgroup.com) <

