KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

WHITE PAPER

How to Build Trusted & Secure IoMT Devices

KEY CONSIDERATIONS FOR FDA CYBERSECURITY GUIDANCE

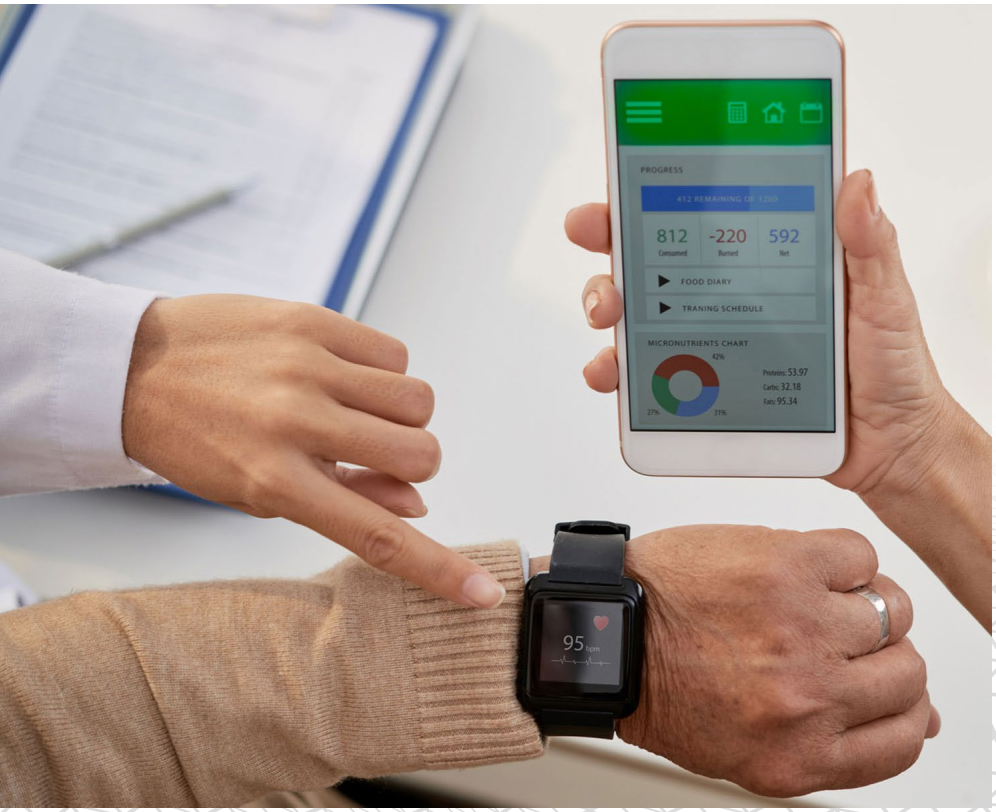

Table of Contents

Overview

INTRODUCTION

The emerging “Internet of Medical Things” (IoMT) and next-generation connected medical devices – such as pacemakers and insulin pumps – have enabled physicians and patients alike to better manage chronic conditions, improve outcomes, and reduce the overall cost of care. But every medical device carries with it a certain amount of both benefit and risk, and the industry is counting on medical device manufacturers (MDMs) to ensure that advantages from these emerging technologies outweigh the potential risks to patients and their data.

INTRODUCTION

Connected medical devices have the power to transform the way people engage with and manage their own healthcare. At the same time, these devices can potentially expose millions of patients to sophisticated hackers and cybercriminals across the Internet. As the complexity of software and hardware continues to grow, so too do the challenges for manufacturers, including time-to-market delays and increased security concerns that threaten to impede innovation.

In response to these challenges, the Food and Drug Administration (FDA) released an update to its pre-market guidance for MDMs – also known as the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. While the guidance is still in draft form, there are practical security measures that MDMs can and should implement today to streamline product launches and assure that every device pushed from production to patient can be trusted from activation to end of life.

WHAT YOU'LL LEARN

Throughout this white paper, we’ll define cybersecurity risks in manufacturing next-generation connected medical devices and the IoMT, the advantages of public key infrastructure (PKI), and practical steps that integrate security into design and development to address emerging FDA cybersecurity guidelines for effective pre-market review.

Let's Talk Security

As the Internet of Medical Things continues to grow, the potential risks to hospital networks, patients, and their data become more serious. The industry is counting on MDMs to design devices that ensure the benefits outweigh potential risks.

EMERGING CYBERSECURITY RISKS

NETWORK BREACHES

Medical IoT devices often have little to no security built-in due to limited resources available on the device itself. But these devices are connected to a huge array of applications, sensors, and backend infrastructure – making them ideal entry points to larger hospital networks.

DATA EXPOSURE

As more devices join the network, the sheer volume of data being generated is immense. Without security in place, the opportunities for breaches, data theft, and privacy loss multiply exponentially. In fact, 78% of IT decision-makers think it is at least somewhat likely their business will suffer a data loss or theft enabled by IoT devices.[1]

DEVICE HIJACKING

It's not just about stealing data anymore. Cyber attacks are now targeting medical devices. As far back as 2011, researchers have found numerous security risks in network-enabled pacemakers and insulin pumps, leaving them vulnerable to medical device hijacking, also known as medjacking.[2]

FDA WARNINGS & RECALLS

Researchers continue to disclose device vulnerabilities to the public, putting pressure on manufacturers to respond. Recent FDA recalls and notifications have caused serious reputational damage and immediate financial losses – not to mention the undue expense to remediate vulnerabilities and rebuild trust with patients, physicians, and investors.

YOUR RESPONSIBILITIES

As the regulatory body responsible for medical devices, the US Food and Drug Administration (FDA) recognizes that cybersecurity is a shared responsibility between medical device manufacturers and healthcare delivery organizations. It starts at design and continues through the lifespan of every device.

> "Manufacturers must adequately address device cybersecurity from the design phase through the device's time on the market ..."[3]

SECURITY BY DESIGN

Security must be inherent in the design of connected medical devices. The FDA continuously stresses that manufacturers must take steps to address cybersecurity risks before devices are deployed into the 'wild' – or in this case – inside the body or on the skin of patients.

LIFECYCLE MANAGEMENT

Risks and vulnerabilities will inevitably arise – in protocols, in devices, and in the cryptographic algorithms used to protect them. Ensuring integrity of devices throughout their lifecycle relies entirely on your ability to securely update devices without putting patients at risk.

Sources:
1. https://www.wired.com/brandlab/2017/06/iot-is-coming-even-if-the-security-isnt-ready-heres-what-to-do/
2. https://www.darkreading.com/vulnerabilities-and-threats/insulin-pump-hack-controversy-grows/d/d-id/1099825
3. https://www.fda.gov/news-events/fda-brief/fda-brief-fda-proposes-updated-cybersecurity-recommendations-help-ensure-device-manufacturers-are

FDA Guidance on Cybersecurity

FDA pre- and post-market guidance on cybersecurity in medical devices was little more than a “tap on the shoulder” for device manufacturers – until now.[4]

WHY THE CHANGE?

Cybersecurity isn’t a new issue for medical devices – the FDA published its first guidance back in 2005. But in 2013, the FDA became much more vigilant about cybersecurity requirements in the pre-market approval process. In an effort to help manufacturers address these requirements in the design and development of their products, the FDA released pre-market (2014) and post-market (2016) guidance on cybersecurity.

Since the initial pre-market guidance was published, we’ve seen an unprecedented rise in cybersecurity risk across the healthcare industry – from the WannaCry ransomware that nearly shutdown the National Health System (NHS) to numerous vulnerabilities revealed in medical IoT devices.

In response to these emerging risks, the FDA released an updated draft of the pre-market guide for cybersecurity in medical devices. Over 40 stakeholders – including federal agencies, researchers, manufacturers, and leaders in cybersecurity like Keyfactor – provided feedback during the comment period. Once finalized, this guidance will supersede the pre-market guidance released in 2014.

2005

FDA outlined requirements to address cybersecurity vulnerabilities for networked medical devices that include ‘off-the-shelf’ software.

2014

Pre-market guidance released to assist manufacturers with identifying issues related to cybersecurity in the design and development of their medical devices.

2016

Post-market guidance provided recommendations to the industry for management of post-market cybersecurity vulnerabilities throughout the product lifecycle.

2018

FDA updated recommendations on cybersecurity considerations for device design, labeling and documentation to be included in pre-market submissions.

SECURITY CAN'T WAIT

Hackers don’t wait for standards – they aim to stay ahead of them. It will take several months until the final guidance is published, but certain security measures including encryption and authentication will undoubtedly remain as a core component. Unless adequate security controls are implemented, weaknesses will continue to be exploited by hackers and researchers.

Device manufacturers should incorporate cybersecurity provisions from the draft guidance into their medical devices today to ensure an efficient pre-market review, prevent undue costs or delays in time to market, and to protect investments in next-gen devices.

> “Now, because of the rapidly evolving nature of cyber threats, we're updating our guidance to make sure it reflects the current threat landscape ...”[5]

Sources:
4. https://cdn2.hubspot.net/hubfs/3821841/docs/Chertoff_Abbott_WhitePaper_Final.pdf
5. https://www.fda.gov/news-events/fda-brief/fda-brief-fda-proposes-updated-cybersecurity-recommendations-help-ensure-device-manufacturers-are

The Role of PKI in the Emerging IoMT

Public key infrastructure (PKI) is recognized by industry experts as a reputable and proven solution to secure emerging IoMT and next-gen connected medical devices.

TAKING ACTION

As the first line of defense, everyone from patients to providers count on manufacturers to build devices that can be trusted from out-of-the-box to end-of-life. The challenge for device manufacturers and software developers is that the limited resources (i.e. CPU, memory, etc.) available to work with can make it difficult to implement the required cybersecurity best practices into device design.

This is where public key infrastructure (PKI) brings real value. PKI is a comprehensive set of processes, policies, and technologies that enable the use of public key encryption and digital certificates (or 'digital identities') for device authentication, data encryption, and code signing services. The real advantage of PKI is that manufacturers can implement these safeguards with minimal footprint on the device and at massive scale.

PKI is a proven and practical technology that enables manufacturers to embed trust into every device pushed from the production line – from design and development through the entire device lifecycle. Common vulnerabilities including code compromise, weak passwords, and man-in-the-middle attacks can easily be thwarted with a single solution.

ADVANTAGES OF PKI

IDENTITY AT SCALE

Introducing a new fleet of connected medical devices comes with many security challenges. Number one is how to establish trust in each device you build. PKI enables manufacturers to embed a unique digital certificate into every device to build trust across the supply chain and track devices throughout their lifecycle.

SECURE UPDATES

The biggest challenge in maintaining device integrity after deployment is the ability to securely update them without inconvenience or risk to the patient. PKI allows manufacturers to securely update devices deployed in the field by digitally signing software and firmware updates.

AUTHENTICATION

Unique device identities provide mutual authentication as the device attempts to connect to gateways, update servers, or other devices – without the need for static passwords or tokens. Digital certificates provide manufacturers with a method to communicate securely with devices even after they've been deployed into the 'wild'.

CRYPTO-AGILITY

Security isn't static. Manufacturers must be able to update not just the software on the device, but the security measures used on that device as well. PKI makes this process easy, as manufacturers can quickly replace digital certificates on devices as algorithms evolve, keys lose strength, or trust is compromised.

How to Build Trusted & Secure IoMT Devices

The following best practices will help to support an efficient pre-market review and improve time to market by integrating security into device design and development.

01 | SECURELY PROVISION UNIQUE KEYS

By binding a digital identity to each device before it goes out into the world, you can be confident that every device you manufacture is secure, and will remain that way for as long as it is in use. It also allows connected platforms and applications to validate the integrity of data sent to and from each device.

The FDA draft guidance advises manufacturers to "use unique per-device cryptographically secure communication keys to prevent leveraging the knowledge of one key to access a multitude of devices." But provisioning a unique key for each device at the scale of thousands or even millions is no simple task. Even where build processes can be adapted to generate unique credentials during production, there are still concerns about the security of manufacturing facilities and the ability to keep credentials confidential.

How to Securely Provision Unique Keys

- Generate keys on the device itself upon activation. Even if an attacker is able to intercept and decrypt communications between the device and backend systems, the key cannot be compromised or extracted.
- Use strong asymmetric cryptography – such as Elliptic Curve Cryptography or larger RSA keys – to ensure that credentials cannot be "guessed" or reverse-engineered.
- Where feasible, store keys in a Trusted Platform Module (TPM) or other embedded technology to prevent compromise, even if an attacker gains physical access to the device.

RELATED GUIDELINES

LINES	GUIDANCE
467-469	Use unique per device cryptographically secure communication keys to prevent leveraging knowledge of one key to access a multitude of devices.

> "IoT Solutions often have no security, and from a cryptographic perspective, they often share the same key or use default passwords."[6]

THE KEYFACTOR SOLUTION

The Keyfactor Control platform provides end-to-end secure identity for connected medical devices, making it easy and affordable to build in high-assurance, unique identity into each device.

The Keyfactor Control Native Agent allows unique keys to be generated on each device upon activation, even at a scale of up to 100 million devices. You also have the flexibility to store keys in embedded hardware security solutions for additional protection against physical attacks.

Sources:
6. Gartner, The Resurgence of PKI in Certificate Management, the IoT and DevOps, October 23, 2018

02 | AUTHENTICATE FIRMWARE & SOFTWARE

You can't secure what you can't update. Anything that you're building into the firmware of devices today will eventually need to be modified. The challenge is to ensure that your updates have not been tampered with in-transit to the device, and that the update originates from the expected source (i.e. the manufacturer's update servers).

Each firmware or software update must be digitally signed by the manufacturer, and the digital signature must be verified by the connected medical device prior to installation. By allowing devices to only accept digitally signed firmware and software updates, trust can be assured both in the operation of the device and in the data it collects and shares. This process is called code signing.

But code signing is not enough on its own. Manufacturers must take extreme caution in protecting private keys linked to code signing certificates. Hackers intentionally target these valuable keys to digitally sign and distribute malware disguised as a trusted update or patch.

How to Authenticate Firmware and Software

- Sign bootloader firmware and implement a Secure Boot workflow to prevent malicious code from loading during device start-up.
- Always sign over-the-air (OTA) updates, firmware, and software to prevent device compromise.
- Ensure that devices only accept updates that have been digitally signed by the manufacturer or a trusted third-party.
- Store code signing keys in a Hardware Security Module (HSM) to prevent key compromise.

THE RISK OF CODE COMPROMISE

In 2019, Kaspersky Labs discovered a software supply chain attack against Taiwan-based tech giant ASUS. Attackers compromised the company's live update tool to distribute malware to nearly 1 million ASUS machines. These machines accepted the update, because the tainted software was signed with legitimate ASUS code signing keys, making it appear valid.[7]

THE KEYFACTOR SOLUTION

Keyfactor Control ensures that code signing operations are properly requested and approved from a centralized portal, all the while keeping private keys secure in an HSM-protected vault.

When the signed software is delivered to in-field devices, the Keyfactor Control Native Agent verifies the digital signature, only accepting updates for installation if the signature is successfully verified.

RELATED GUIDELINES

LINES	GUIDANCE
421-427	Authenticate firmware and software. Verify authentication tags (e.g., signatures, message authentication codes (MACs) of software/firmware content, version numbers, and other metadata. The version numbers intended to be installed should themselves be signed/have MACs. Devices should be electronically identifiable (e.g., model number, serial number) to authorized users.
445-448	Only allow installation of cryptographically verified firmware/software updates. Use cryptographically signed updates to help prevent unauthorized reduction in the level of protection.
451-453	Where feasible, ensure that the integrity of software is validated prior to execution, e.g., 'whitelisting' based on digital signatures.
471-473	Where feasible, use industry-accepted best practices to maintain/verify integrity of code while it is being executed on the device.
534-535	The device should be designed to facilitate the rapid verification, validation, and testing of patches and updates.
685-687	[Submit] A summary describing the design features that permit validated software updates and patches as needed throughout the life cycle of the medical device to continue to ensure its safety and effectiveness.

Sources:

7. https://blog.keyfactor.com/hackers-hijacked-asus-software-updates-to-install-the-need-for-code-signing

03 | ENFORCE STRONG AUTHENTICATION

Many IoT devices in healthcare lack proper authentication – the method of allowing access to only trusted apps, users, and systems. Untrusted entities can gain access and compromise the end user's network, data, or the device itself, causing direct harm to the patients and healthcare providers that use your devices every day.

With no set of IoT industry security standards, industry experts recommend using PKI and digital certificates as one of the most effective ways to securely authenticate devices without compromising interoperability.

Most connected medical devices communicate over common protocols that can be secured with Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Digital certificates establish mutual authentication between any two entities or devices – ensuring secure data exchange across open networks.

How to Enforce Strong Authentication

- Establish and manage your own Root of Trust (RoT) from which all keys and certificates are issued – providing you with complete control.
- Install a digital certificate on each device to establish mutual authentication and encrypt all communications to and from other entities.

THE KEYFACTOR SOLUTION

Keyfactor Control enables you to establish and manage your own private Root of Trust (RoT) to ensure complete control over device authenticity across the supply chain.

The Keyfactor Control Native Agent can then be used to securely install a digital certificate on each device to support mutual authentication and encrypted communications.

RELATED GUIDELINES

LINES	GUIDANCE
414-416	Use cryptographically strong authentication resident on the device to authenticate personnel, messages, commands and as applicable, all other communication pathways.
417-419	Authenticate all external connections. For example, if a device connects to an offsite server, then it and the server should mutually authenticate, even if the connection is initiated over one or more existing channels.
428-434	Perform authorization check based on authentication credentials or other irrefutable evidence. For example, a medical device programmer should have elevate privileges that are granted based on cryptographic authentication or a signal of intent that cannot be physically be produced by another device, e.g. a home monitor, with a software-based attack.
458-461	Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption and authentication of the end points with which data is being transferred.
674-676	[System diagrams should include] Authentication mechanisms and controls for each communicating asset or component of the system including web sites, servers, interoperable systems, cloud stores, etc.

04 | PROTECT DATA CONFIDENTIALITY

While patient safety is priority one, securing patient data runs a close second. Of course, pacemakers or insulin pumps can have life-threatening vulnerabilities, but the need to secure HIPAA-covered protected health information (PHI) extends to virtually every device that collects data across the entire IoMT ecosystem – from wearable devices to connected smartphones and mobile apps.

Mutual authentication ensures that sensitive data is protected in-transit between the device and other apps or systems. However, many times data is generated by the device before it is uploaded to another location, and must be stored temporarily for some period of time. This can lead to a vulnerability whereby an attacker can obtain patients' PHI by accessing the device either physically or through remote connectivity.

Requirements to protect PHI are outside the scope of the FDA guidance, but manufacturers have strict obligations under other regulations, including HIPAA, to prevent unauthorized access or disclosure of patient data.

How to Protect Data Confidentiality

- Protect data-in-transit with SSL/TLS mutual authentication and encryption (See 'Step 3: Enforce Strong Authentication).
- Where feasible, protect data-at-rest by using the public key of the server where that data will be transmitted. Even if an attacker gains full access to the device and all keys on the device, they will not be able to decrypt the data.

> "Over 90% of data transaction on IoT devices are unencrypted."[8]

THE KEYFACTOR SOLUTION

The Keyfactor Control Native Agent has the ability to encrypt a given piece of data with the public key of any digital certificate, providing the flexibility to secure data-at-rest when required.

RELATED GUIDELINES

LINES	GUIDANCE
381-382	Encryption should be used as appropriate, since it protects sensitive information from unauthorized disclosure.
476-480	Manufacturers should ensure the confidentiality of any/all data whose disclosure could lead to patient harm (e.g., through use of credentials, encryption). Loss of confidentiality of credentials could be used by a threat to effect multi-patient harm. Lack of encryption to protect sensitive information "at rest" and "in transit" can expose this information to misuse that can lead to patient harm.
458-461	Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption and authentication of the end points with which data is being transferred.
714-716	[Submit] A list of verifiable function/subsystem requirements related to access control, encryption/decryption, firewalls, intrusion detection/prevention, antivirus packages, etc.

Sources:
8. https://www.csoonline.com/article/3397044/over-90-of-data-transactions-on-iot-devices-are-unencrypted.html

05 | PREPARE FOR REMEDIATION

Despite every precaution, devices are rarely impervious to threats. If a device is compromised, the risk to patients and providers grows by the minute, as hackers seek to hide in the network, sniff or steal data, or inject malware into other devices. In this case, the FDA states that the potential impact of "multi-patient" harm must be contained.

When an attack or vulnerability is detected on a device that communicates using a digital certificate, the natural response is often to revoke the certificate through the Certificate Authority (CA) from which it was issued. But this method can often create more problems than it solves:

01. Revoking the certificate may not immediately disable connectivity, since other systems and devices may cache revocation status for some time.

02. If the certificate is revoked, and the cybersecurity incident is then remediated, a new certificate must be issued and installed before each device can resume communication, since there is no mechanism to "unrevoke" a certificate.

03. In deployments with a large number of devices, mass revocation of certificates can cause significant bandwidth and performance issues.

How to Prepare for Remediation

- Manage the lifecycle of every digital certificate to ensure quick response and remediation when security incidents occur.
- Avoid revoking certificates to disconnect compromised devices, which can cause significant disruption to operations and healthcare delivery.

RELATED GUIDELINES

LINES	GUIDANCE
491-494	Proper device design can significantly reduce cybersecurity risk while it is marketed and deployed in its use environment. Therefore, appropriate design should anticipate the need to detect and respond to dynamic cybersecurity risks, including the need for deployment of cybersecurity routine updates and patches as well as emergency workarounds.

THE KEYFACTOR SOLUTION

With Keyfactor Control, devices can be immediately disconnected without any of the downsides of revocation. This is done by simply using certificate metadata – custom data fields such as device type or serial number – to find certificates on affected devices and disconnect them. Affected devices can later be restored to service without any need to re-issue and install a new certificate.

06 | DESIGN FOR CRYPTO-AGILITY

When cybersecurity incidents arise, manufacturers must respond to address immediate issues and longer-term threats. This is where crypto-agility comes into play.

In certain types of incidents, it isn't sufficient to temporarily disable access for a given client certificate. This includes cases where private keys have been breached or when the Certificate Authority (CA) can no longer be trusted. These events require manufacturers to quickly re-issue the identity of each device, and update the Root of Trust for each system that relies on it.

FDA guidance defines "cryptographically strong" as "cryptographic algorithms, protocols, and implementations that authoritative sources in cryptography would consider sufficiently secure." But what is considered "cryptographically strong" today may not be considered as such tomorrow.

The practical use of quantum computing may be years away, but devices expected to stay secure beyond this point should be manufactured with the assumption that the cryptography used today will not be effective over its entire lifespan. This applies to all cryptography used in the connected IoMT ecosystem – from client authentication and server certificates to CA and Root of Trust certificates.

How to Design for Crypto-Agility

- Engage the product team that owns the vision to understand where the device will be two, five, ten years from activation.
- Stay ahead of expired certificates and outdated keys or algorithms that could put the security of your devices and safety of patients at risk.
- Create a plan on how these devices will migrate to new keys and algorithms as they become available, and within a reasonable timeframe.

> "The biggest threat against IoT devices is the lack of life cycle management of the credentials they use."[9]

THE KEYFACTOR SOLUTION

The Keyfactor Control Native Agent can securely generate new unique cryptographic keys for each device, obtain a new client authentication certificate, remove the outdated RoT from subsystems, and install a new RoT and encryption certificate – all with just a few kilobytes of data.

RELATED GUIDELINES

LINES	GUIDANCE
164-165	Cryptographically strong – cryptographic algorithms, protocols and implementations that authoritative sources in cryptography would consider sufficiently secure.
414-416	Use cryptographically strong authentication resident on the device to authenticate personnel, messages, commands and as applicable, all other communication pathways.

Sources:
9. Gartner, The Resurgence of PKI in Certificate Management, the IoT and DevOps, October 23, 2018

Conclusion

No device is hack-proof, but adoption of cybersecurity best practices in design and development enables manufacturers to drive innovation while mitigating the risk of emerging threats.

Medical devices should compete on the health benefits they deliver, never on critical matters of patient safety and security. Even so, by integrating key principles in the updated FDA pre-market guidance, manufacturers can make inherent security a product differentiator:

ACCELERATE TIME-TO-MARKET

As the FDA becomes more vigilant about cybersecurity, manufacturers can accelerate approval and time-to-market by including recommendations on device design, labeling, and documentation in pre-market submissions.

MINIMIZE RISK & REPUTATIONAL DAMAGE

Hackers and security researchers are becoming more adept to vulnerabilities in IoMT devices. Prevent device recalls and safety communications from the FDA that can cause serious damage to your reputation, equity, and bottom line.

ESTABLISH TRUST & MARKET LEADERSHIP

In the IoMT – security isn't just critical, it's personal. Become a trusted market leader by implementing 'security by design' principles and providing high assurance to users that hackers cannot access devices in their body or on their skin.

KEYFACTOR

Keyfactor works with the world's leading medical device manufacturers to build and deliver the most secure and innovative medical devices on the market. From design to deployment, our leading secure identity platform for IoT devices – Keyfactor Control – gives manufacturers high-assurance secure identity at each step of the device lifecycle.

Learn more about how Keyfactor can work with you to design a framework that aligns to your specific needs and objectives – to meet your timelines and ensure easy implementation.

▶ CONTACT US TODAY

ABOUT

KEYFACTOR

Keyfactor™, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its life cycle, Keyfactor™ empowers global enterprises with the freedom to master every digital identity. Its clients are the most innovative brands in the industries where trust and reliability matter most.

CONTACT US

▶ www.keyfactor.com
▶ 216.785.2990