Public Key Infrastructure: A Trusted Security Solution for Connected Medical Devices

DigiCert | MDISS

digicert® | MDISS

Table of Contents

1 Introduction
2 Security Risks in IoT Devices
3 Public Key Infrastructure (PKI): A Proven Solution
6 PKI Deployment Considerations
7 PKI Uses for Connected Medical Devices
8 PKI Use Case: Wireless Infusion Pumps & Pump Servers
11 Summary
12 Contributing Authors

Introduction

In today's healthcare environment practitioners are using state-of-the-art, high-tech equipment that delivers specialty services with better efficiency, accuracy, and overall quality. Using this technology, patients and doctors are also able to generate meaningful data that improves clinical outcomes and, ultimately, the patient's quality of life.

Despite these improvements in the delivery of care, many healthcare experts are not aware of the vulnerabilities present in connected medical devices. Numerous devices lack proper authentication—the process of validating identities to ensure only trusted users, messages, or other types of services have access to the device. This allows untrusted users to gain access and potentially manipulate the device. Other devices lack basic encryption of the sensitive data being stored in or transferred from the device. These cybersecurity oversights can result in direct harm to the patients and healthcare providers using the devices.

According to security research conducted in 2014 by Scott Erven, head of information security for Essentia, thousands of medical devices in use in healthcare environments are vulnerable to hacking, exposing patients and practitioners to malicious attacks. Erven, among other tactics, used the search engine Shodan to find medical devices connected to the public Internet. What Erven discovered was shocking:

"His team found drug infusion pumps–for delivering morphine drips, chemotherapy and antibiotics–that can be remotely manipulated to change the dosage doled out to patients; Bluetooth-enabled ICDs (implantable cardiovascular defibrillators) that can be manipulated to deliver random shocks to a patient's heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital's network; temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage; and digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs, or administer unwarranted care."[1]

Erven's findings, coupled with similar reports from other medical device security researchers, have raised awareness about the massive vulnerabilities present in connected medical devices. If these vulnerabilities are left unsecured, they put patients in harm's way and can expose confidential data or compromise an entire hospital network.

Medical device manufacturers need to adopt strong security practices to secure connected devices so patients receiving treatment from them have peace of mind and do not have to worry about malfunctions due to malicious attacks.

Public Key Infrastructure (PKI) is a fundamental aspect of securing IoT devices. As an accepted and well-established standard, PKI is a core component of authentication, data confidentiality, and data and system integrity.

This white paper discusses security risks inherent in IoT devices, and articulates how PKI can be used to mitigate these vulnerabilities and improve the security posture of connected medical devices.

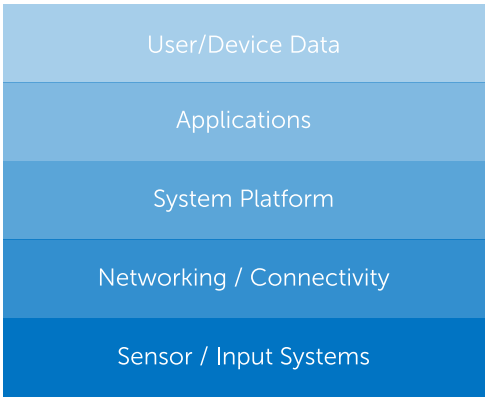
[1] Zetter, K. Wired Magazine. "It's Insanely Easy to Hack Hospital Equipment." Accessed 6 August 2016. https://www.wired.com/2014/04/hospital-equipment-vulnerable/

Security Risks in IoT Devices

While delivering on the promise of streamlined efficiencies and operational insights, smart devices in healthcare also present a new and more widespread threat to users and personal data. Current threats to IoT devices have moved beyond simple proof-of-concepts, and it is expected attackers will continue to explore the developments in technology; the ways potential threats can be realistically exploited will accelerate.

Each IoT device is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Securing these Internet-connected devices and platforms requires a thorough understanding of the makeup of the IoT information stack, its various elements, and the specific security requirements and impact to IoT devices.

IOT INFORMATION STACK



For example, an IoT application that collects data from multiple connected devices may have entirely different security requirements than the actual device itself. Security must be considered and addressed throughout each part of a device's information architecture in the IoT.

OWASP LIST OF TOP IOT VULNERABILITIES

The Open Web Application Security Project's (OWASP) list of top IoT vulnerabilities demonstrates the critical concern that proper data security, identity, and trust play in developing solutions for the IoT.

The list includes the following as the most critical existing attack vectors for IoT and connected devices:

- Unsecure web interfaces
- Data privacy concerns
- Unsecure device software/firmware
- Insufficient device identity
- User and device identity and authentication
- Unsecure cloud backend systems
- Poor transport encryption
- Implementation
- Unsecure network services
- Unsecure mobile connections
- Poor physical device security

Security implementations are not simply about encrypting data; they also ensure the proper deployment and configuration of security across the various layers of communication within individual devices and across integrated systems.

Security in IoT implementations must be a critical component during the device design and manufacturing phase, or during the initialization phase of a product update. Correctly implemented, secure IoT deployments should ensure that the basic security requirements needed for data confidentiality, data integrity, and data accessibility are properly configured as part of the solution, which is where PKI comes into the picture.

Public Key Infrastructure (PKI): A Proven Solution

Public Key Infrastructure (PKI) is a concept broadly misunderstood in the security world. Many security professionals understand the common uses for PKI—such as authentication, encryption, and signing services—but many fall short in their understanding of how it actually works and is implemented.

PKI FRAMEWORK

PKI is a framework that contains the set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.[2] Digital certificates are issued by a Certificate Authority (CA) who acts as a trusted third party. When issued, the certificate is associated with a key pair linked to a user (server, computer, or device) and has an identity that is already verified. Once this identity has been verified, other users can trust the legitimacy of the key holder's identity.

An example of this concept is a standard-issue U.S. driver's license. Before issuing the license the state verifies the individual is who he claims to be and that he is fit for driving. If a driver's license is presented as a form of identification, most parties accept and trust it without question.

A strong PKI framework consists of the following components.[3]

1. Certificate Authority (CA) – The entity that stores, issues, and signs digital certificates.
2. Registration Authority (RA) – The entity that verifies the identity of other entitites.
3. Certificate Policies – Policies created to govern the operation of the PKI.
4. Central Directory – A secure location where keys are stored and indexed.
5. Certificate Management System – A system that automates digital certificate management.

[2] Shinder, D. "Understanding the Role of the PKI." Accessed 5 April 2016. http://www.windowsecurity .com/articles-tutorials/authentication_and_encryption/Understanding_the_Role_of_the_PKI.html.

[3] Cobb, M., Brayton, J., Finneman, A., Turajski, N., & Wiltsey, S. "PKI (public key infrastructure)." Accessed 5 April 2016. http://searchsecurity.techtarget.com/definition/PKI

TRANSPORT LAYER SECURITY (TLS) USE CASE

A common use for PKI is Transport Layer Security (TLS)* communications, which is the standard security technology for establishing an encrypted link between a web server and a browser. This secure link ensures all data between the web server and browser remains private. (See graphic.) With the expansion of e-commerce and online banking, and the associated need to securely verify identities, TLS has become a hardened and relied upon security solution.

MOVING BEYOND TLS

PKI has applications well beyond this TLS use case. For example, digital certificates can be provisioned to IoT devices to provide the highest levels of authentication, encryption, and data and system integrity. With no set IoT industry security standards, many experts recommend and rely on PKI for device authentication because of its interoperability.[4]

PKI is a fundamental aspect of security for IoT devices. PKI-based solutions are accepted as a standard for secure communications between users and devices, and have been used to secure servers, fax machines, and other connected devices for decades. PKI offers core security for comprehensive authentication, encryption of sensitive data, and the assurance of data and system integrity. A PKI framework should be the starting point for securing any connected device.

HOW PKI IS USED WITH TLS CERTIFICATES (OVERVIEW)

Web Broswer

Web Server

1. Server sends a copy of its asymmetric public key to browser.
2. Browser creates a symmetric session key and encrypts it with the server's asymmetric public key then sends it to the server.
3. Server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key.
4. Server and browser now encrypt and decrypt all transmitted data with the symmetric session key. This allows for a secure channel because only the browser and the server know the symmetric session key, and the session key is only used for that specific session. If the browser was to connect to the same server the next day, a new session key would be created.

*Note: Transport Layer Security (TLS) is the updated cryptographic protocol used to secure web communications. Secure Sockets Layer (SSL) is the predecessor for TLS and is being phased out. Both SSL and TLS are often used interchangeably or referred to as SSL. In this paper, we will use TLS for better accuracy.

[4]Anderson, M. "Looking for the Key to Security in the Internet of Things." Accessed 6 August 2016. http://spectrum.ieee.org/riskfactor/consumer-electronics/standards/looking-for-the-key-to-security-in-the-internet-of-things

digicert® | MDISS

PKI IS FLEXIBLE

While traditional PKI implementations share common threads, like issuing certificates for devices, servers, and clients for authentication and encryption, every IoT implementation can vary in its security requirements. Device manufacturers need to consider the availability of connectivity, internal device resources, and how these interact with PKI. Some devices will have technical resource constraints or limited availability for regular maintenance and updates.

There are many options for a PKI trust model, which is the security architecture of how trust is established within a deployment. This allows for a variety of approaches for security implementations, making PKI the most flexible solution for securing connected devices. Whether you are working with public or private networks, PKI offers alternative solutions to enable the deployment of the critical authentication and encryption capabilities that ensure privacy and trust.

Historically, TLS X.509 certificates have been the standard—that has not changed. However, with IoT-specific PKI, digital certificates are not under the same restrictions, offering flexible, custom advantages for IoT device manufacturers including the following:

- Custom certificate profiles and key usage fields
- Custom certificate subject fields
- Flexible trusted roots and revocation options
- Shorter and longer validity certificates
- Stronger cryptographic hashes and algorithms
- Direct-to-root chained certificates

Additionally, PKI can be flexible in the way the certificates are provisioned to devices. PKI certificates can be deployed during manufacturing when the manufacturer or CA provisions the certificate to the device. PKI certificates can also be deployed remotely to legacy devices in use by customers through software updates that provision the certificates to enable secure communications between the device and back-end systems.

PKI IS SCALABLE

PKI-based systems have the advantage of broad project application, cross-platform support, and certificate deployment capabilities for projects of various sizes. PKI enables identity authentication, data encryption, digital signing, and device access control, typically out-of-the-box with little internal development by those implementing PKI services. These critical functions are often available in on-prem and hybrid cloud-based platforms to ensure maximum scalability as IoT projects grow in size.

Although unique cryptographic algorithms and flexible certificate options are important functions of PKI systems, IoT implementations need scalable PKI platforms to handle the increased volume and speed of certificate deployments in IoT projects. To meet the critical needs of connected devices, projects must be able to rely on effective, simple, and scalable APIs and systems that can issue not thousands, but millions, of certificates. Performance and availability of these systems vary greatly between available CA software and a commercial CA's hosted services.

PKI Deployment Considerations

Deploying, managing, and maintaining an enterprise-level PKI security solution can be a complicated task. Organizations that seek to implement and maintain an on-premise or in-house PKI security solution should consider the following challenges and complications before making the decision to act as their own internal CA.

PKI EXPERTISE

Understanding PKI is complex and typically isn't an IoT manufacturer's full-time role. PKI expertise is needed to help clarify and comprehend data security requirements, such as FIPS 140-2 level 2, ECDHE cipher suites, PKCS #11 cryptographic interfaces, root ubiquity compliance, and X.509 OIDs.

CRYPTOGRAPHIC AGILITY

Cryptography is constantly changing. What was considered completely secure and safe to use three or four years ago is now deprecated. There are aspects of certificates which may require an even quicker turn-around of switching substantial infrastructure to new or different cryptographic properties. Most PKI implementations are built to enable IoT projects to take advantage of updates to curves, algorithms, and hashes as these technological capabilities become available. When vulnerabilities are found or deprecation occurs, the CA must have the ability to immediately switch to a secure alternative. This advantage is typically not found with new security standards or security alternatives being developed.

SYSTEM AVAILABILITY

Core IoT services require exceptional uptime and availability. When dealing with globally disparate certificate provisioning, verification, and revocation, deploying a brand new infrastructure to support the many needs of such systems is not logistically feasible for most organizations and is almost never economically feasible when compared to using systems already in place.

INFRASTRUCTURE SCALABILITY

Certificates are used to secure sensitive and valuable information. Investing in servers and infrastructure needed to handle mass issuance, reissuance, and/or revocation events is necessary to ensure integrity of the PKI systems. Those events are rare, but the cost involved in such an investment can be large, especially when dealing with tens of thousands or hundreds of millions of certificates.

SECURITY

The security requirements of running a CA are substantial. Your Root CA needs to be secured to the absolute highest level, which requires investment in hardware, CA software, infrastructure, PKI architects, consulting services, and training.

COST

While using an internal or private CA might seem ideal and even a more cost-effective solution at first, it is important to understand the underlying costs of hosting, deploying, and maintaining on-going CA infrastructure systems. Hosted CA infrastructure with a commercial Certificate Authority can deliver competitive pricing for critical services which can automatically scale with certificate issuance. This allows your investment to start at an already financially viable position and grow to more affordable levels as your IoT certificate issuance increases.

LIABILITY

If an internal CA is compromised and enables access to privileged data, the damage to a company's reputation is often detrimental, not to mention the resulting monetary loss can be significant. Separating management of some parts of an organization's security solution can not only increase the overall security of that solution, but also help to minimize damages in worst-case scenarios.

COMPLIANCE AND DATA CONTROL

Hosted, cloud-based PKI services also come with their own set of internal compliance and data control concerns, especially for devices or systems dealing with medical or patient data. Effectively implementing and managing a PKI solution requires adherence to PKI standards, industry requirements, potential government mandates, data storage requirements, certificate management policies, training personnel, and data recovery policies. Additional considerations should be made for often hidden requirements of security deployments.

PUBLIC TRUST

While private PKI may be used by some IoT providers, having the ability to also flexibly issue publicly trusted certificates is incredibly valuable. An internal CA may never be able to be used in a way that is trusted automatically by external services or relying parties, leading to certificate-related errors for users engaging with IoT devices or with devices attempting to establish connections with back-end systems and services.

PKI Uses for Connected Medical Devices

Before digital certificates are deployed to a medical device, the right infrastructure for overseeing certificates needs to be in place. A certificate management platform that streamlines critical aspects of a certificate lifecycle (provision, issue, renew, revoke) allows manufacturers to be dedicated to security without additional hassle or error. Platforms should be flexible, reliable, and enable the manufacturer to scale.

IoT manufacturers will benefit from using a platform that allows them to:

- Provision, issue, renew, and revoke certificates
- Create custom certificate profiles
- Deploy a high volume of certificates
- Scan and remediate TLS vulnerabilities
- Review analytics and reports
- Securely store and manage certificate keys

Once a manufacturer has a certificate management platform in place, they can then deploy certificates for authentication, encryption, and signing services.

AUTHENTICATION SERVICES

PKI enables the safe authentication of users, systems, and devices without the need for tokens, password policies, or other cumbersome user-initiated factors. With PKI, IoT solutions can enable direct authentication across systems. PKI also offers the highest levels of identify assurance, providing a measure of confidence that the entities at both ends of a data transaction or authentication event are who they claim to be. Effective identity verification is a fundamental element for effective security and connected device trust. PKI certificates provide evidence that the identity of organizations, domains, and devices was properly established because certificates cryptographically bind public keys to such identities.

ENCRYPTION SERVICES

PKI affords the capability to address the security needs of data in transit. While not vulnerable to common brute-force or user-deception attacks, PKI facilitates the secure transmission of sensitive information. When a connected device transmits or receives sensitive personal health information (PHI) over the Internet, the data must be encrypted. Digital certificates can be used to ensure the highest level of HIPAA-compliant encryption is used to secure this data.

SIGNING SERVICES

Signing services ensure data and device integrity by making sure any messages sent to a device from sensors or other intelligent systems are not intercepted and remain unaltered. PKI also facilitates the verification of availability and access for protocol configurations, applications, or interaction with data stored in the device. This ensures the complete coverage of data and system confidentiality, integrity, and availability.

PKI can be used to provide secure signing services in the following ways:

Data Integrity: Certificates can be used to ensure data being sent to and from a connected device has not been intercepted and modified in transition.

Secure Device Boot: When a device is started, certificates are used to ensure the configuration settings, software, firmware, or other components of the device have not been modified from the desired settings.

Firmware Authentication: When a firmware update is sent to a connected device, certificates can be used to ensure the update is coming from a trusted source and signed by a trusted and/or pinned certificate.

Software Code Signing: When manufacturers put software on a connected device, certificates can be used to sign the code, ensuring it hasn't been modified.

PKI Use Case: Wireless Infusion Pumps & Pump Servers

This use case shows how PKI can be used with wireless infusion pumps and servers to securely authenticate and encrypt any communication coming to and from the devices. The workflow of a wireless infusion pump includes connecting to a wireless pump server to receive drug dosage information. The pump server then connects with multiple outside sources such as the electronic medical record (EMR) system, e-prescribing system, and even pharmacies to send and receive drug data. This use case will focus on authentication between the pump and the pump server. Similar authentication and encryption should also be in place for the pump server and other outside connections.

Each of these connections requires a method to identify one another and a securely encrypted transfer of data that can be checked for authenticity. Without the ability to identify one another and properly encrypt the data, the wireless infusion pumps could receive data from non-trusted sources that contain malware or counterfeit drug dosage information. The data being sent could also be intercepted by a perpetrator, the drug dosage amounts could be manipulated to lethal levels, and the counterfeit drug data could arrive at the wireless pump and be administered to the patient.

PUBLIC/PRIVATE KEY CREATION AND PROVISIONING

Mutual authentication using public/private key pairs must be performed in order to secure the different connection points between wireless infusion pumps and pump servers. To do this, a public/private key pair is created based on strong cryptographic technology that cannot be counterfeited. A CA then combines the public key with the information used to uniquely identify the private key (such as the serial number of the pump) and signs the resulting certificate file. When this is complete the private key and certificate are imported to each pump and server through a secure process. (See graphic.) Once the private key is contained on the device it cannot be tampered with or exported from the device. The private key and certificate are unique for each device.

AUTHENTICATION

Mutual authentication using public/private key pairs is performed each time the wireless infusion pump connects with the pump server. Each time a connection is initiated a secure "handshake" takes place, validating both the server and pump as trusted sources. The server uses its private key to sign an authentication then passes the signed authentication and its certificate to the pump. The pump inspects the certificate provided by the server to ensure it can be trusted. The pump uses its private key to sign an authentication then passes the signed authentication and its certificate to the server. The server inspects the certificate provided by the pump to ensure it can be trusted. During this process if the certificate used by the pump and server are trusted, the session continues, otherwise the connection is terminated.

ENCRYPTION

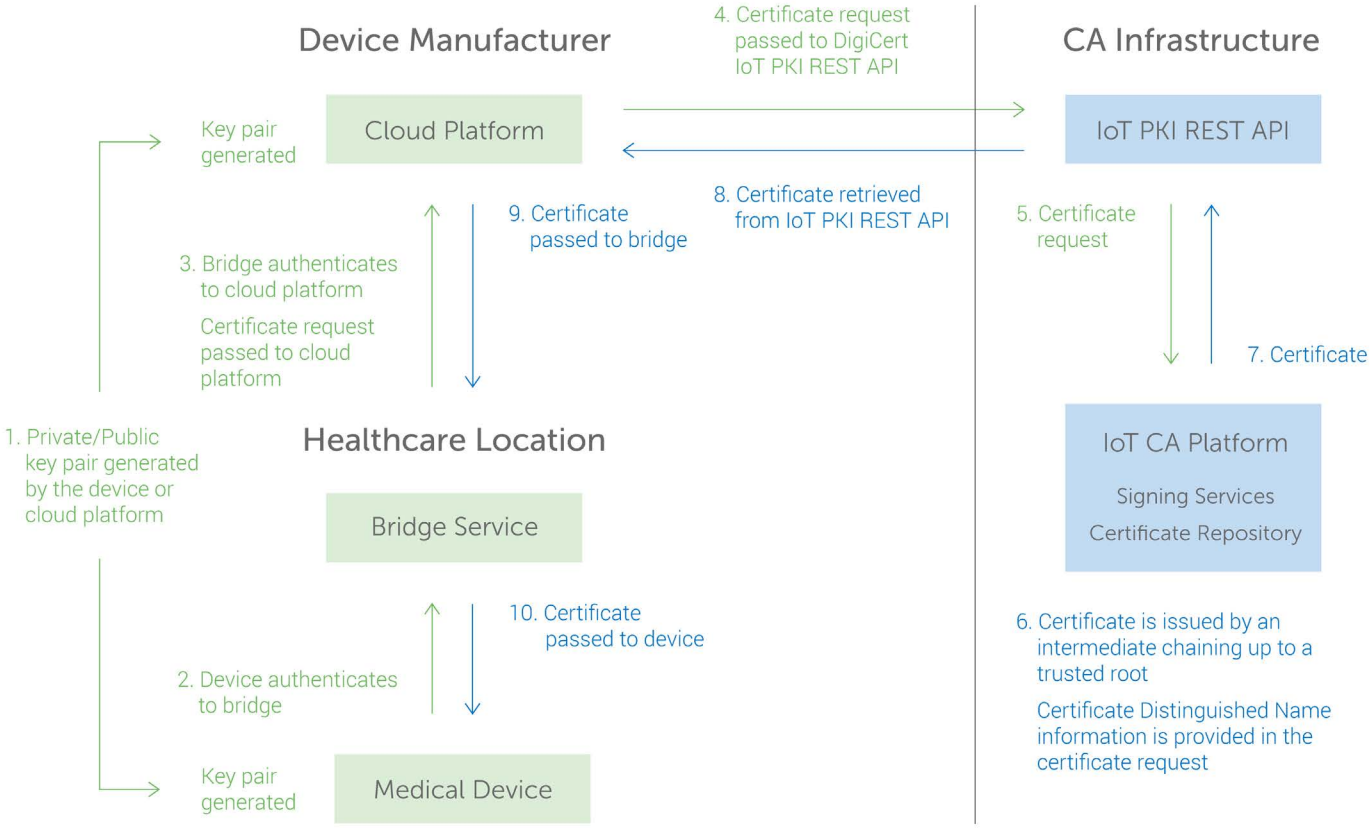
Once the pump and server have completed their mutual authentication, the server continues the process of establishing an encrypted session with the pump. An ephemeral symmetric session key is generated and shared between the pump and the server. The session key is used to encrypt any data transferred between the pump and the server. A new session key is created each time the pump makes a connection with the server. The encrypted session ensures the integrity of the data in transit between the pump and server.

SIGNING

In this use case, the manufacturer's process passes the pump configuration parameters to the pump using a signed configuration file. The pump configuration file must be signed by the server and the pump must check the signature of the file before applying the configuration which will set the parameters it uses to deliver substances to patients.

The proper use and configuration of public/private key pairs have shown to reliably prove authenticity and prevent the introduction of counterfeit devices, as well as protect data sent between pumps and servers using encryption.

DIGICERT IOT CERTIFICATE ISSUANCE (OVERVIEW)



Summary

PKI is the foundation for securing the growing number of connected devices within the healthcare industry. Its existing technologies, when correctly implemented, can mitigate the security risks associated with large-scale device deployments.

IoT ecosystems that use PKI are able to properly apply encryption, authentication, and signing services. Additionally, a PKI-based IoT security solution ensures strong identity and message integrity for data exchange between systems, devices, applications, and users.

To achieve a comprehensive PKI solution, IoT providers should consider the hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, as well as manage the encryption process. Using a high-volume issuance platform complements PKI and provides the scalability and flexibility that many IoT manufacturers require.

As technical innovation continues to push the market forward, organizations are adopting this scalable and flexible solution to deliver the highest levels of security for their connected devices.

Contributing Authors

Mike Nelson
DigiCert
VP of Healthcare Solutions
mike.nelson@digicert.com

Mike Nelson is the VP of Healthcare Solutions at DigiCert, a leader in digital security. Mike oversees the company's healthcare strategy working with healthcare providers, medical device manufacturers, and insurance companies to strengthen their cybersecurity posture. He has deep understanding of the healthcare industry, and specifically around how technology can be used to improve clinical outcomes.

Before joining DigiCert, Mike started up and led a consulting practice focused on using collaboration to solve complex healthcare problems at Leavitt Partners, a health intelligence company founded by Mike Leavitt, the former Secretary of the US Department of Health and Human Services. Before joining Leavitt Partners, Nelson served as a senior manager for GE Healthcare where his team developed advanced IT solutions aimed at enhancing patient outcomes while reducing costs. Nelson began his career in healthcare at the U.S. Department of Health and Human Services where he ultimately served as the Director of the National Electronic Health Record Initiative, a Medicare demonstration project focused on using HIT in meaningful ways to improve quality and lower costs for Medicare patients.

Dale Nordenberg
MDISS
Executive Director
dalenordenberg@mdiss.org

Dr. Nordenberg is the co-founder and Executive Director for the Medical Device Innovation, Safety, and Security Consortium (MDISS), a public-private partnership that works closely with leading device manufacturers, healthcare systems, government agencies, and other stakeholders to improve the security and safety of medical devices from design through retirement.

Dr. Nordenberg is a member of the Health Information Technology Standards Federal Advisory Committee, Office of the National Coordinator, HHS; a member of the FDA's National Evaluation System for Technology (NEST) Planning Board; and co-chairs the Medical Device Security Information Sharing Council for the National Health Information Sharing and Analysis Center (NHISAC). Dr. Nordenberg is also CEO of Novasano Health and Science, a company that delivers information technology services and products to accelerate innovation in healthcare and life sciences. He has extensive experience in the domains of healthcare strategy and operations, health information technology, FDA regulated industries, research network development, public-private partnership development, and emergency preparedness.

digicert® | MDISS