Advantages of Using PKI to Secure Medical Devices

digicert®

The challenge with networked medical devices

According to Forbes, the healthcare device market will hit $117 billion by 2020. The debate about how to secure healthcare technology is becoming increasingly urgent in today's healthcare market.

On the one hand, networked medical devices are revolutionizing the way patients engage with healthcare. On the other hand, these devices are exposing millions of patients and healthcare providers to safety and security risks.

While in the past the healthcare industry has focused largely on patient privacy, it is important to note that security is not the same as privacy. Privacy focuses more on access control, while security is about protecting the systems and sensitive data from intruders.

Many healthcare records and devices in use today are vulnerable to attack, and the number of networked medical devices is rapidly growing. An estimated 1.8 million people will use a wireless, remote-monitoring healthcare device by 2017.[1]

As more connected devices come to market the following security risks must be addressed:

- Unsecure web interfaces
- Insufficient system or user authentication
- Unsecure mobile connections
- Unsecure device software/firmware
- Poor transport encryption implementation
- Poor physical device security

Private Key Infrastructure (PKI) is a trusted security solution that can be used to secure the millions of connected devices in the market.

In a 2015 study, the Ponemon Institute found that heathcare records are the most expensive to remediate, with each record costing nearly $400.[2]

On the black market, a heathcare record is worth 10 to 20 times more than a credit card number.[3]

Industry standards & PKI security

Numerous industry working groups have convened to discuss and create standards, guidelines, and best practices for securing networked medical devices across the healthcare industry. This work is essential and will move the industry in the right direction, but there are security decisions that can be made today to protect devices and the sensitive data they transmit. Certain security approaches, such as encryption and authentication, will be part of whatever standard emerges from the working groups.

PKI is a proven security solution that provides encryption and authentication to any type of connected device, and offers numerous advantages.

Advantages of PKI & the DigiCert solution

PKI for identity, authentication, & encryption

Identity assurance is the most effective way to reduce risks associated with exchanging information between devices. As such, identity verification is a central element of strong security. PKI's organization inherently provides identity vetting; certificates offer evidence of an identity on an organizational, domain, or device level. DigiCert's PKI platform allows one-time pre-verification or real-time verification to provide identity assurance needed by the systems in IoT deployments.

PKI enables for 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 in a decentralized handling of authentication. While not vulnerable to common brute force or user deception attacks, PKI facilitates the encryption of sensitive information protecting it from malicious actors even in the event of a data stream or data source being captured or compromised.

PKI is uniquely positioned to scale

PKI can be scaled to fit connected medical device environments, which often vary in size, complexity, and security needs. DigiCert's PKI Platform can handle increased volume and speed of certificate deployments for millions of devices.

Scalability also plays are a large role in application. PKI can be implemented during the manufacturing process or can be deployed remotely to existing devices through software updates. DigiCert has experience working with providers to find an optimal solution based on device environments and has PKI implementations in use for both models.

Cyber criminals are zeroing in on the healthcare industry. Attacks have increased 125% since 2010.[4]

The healthcare industry, as a whole, is paying $6 billion dollars annually as a result of the increased attacks.[5]

PKI is flexible

Flexibility in PKI goes beyond scale. The DigiCert PKI Platform uses a hybrid model of deployments that are more flexible than traditional PKI implementations. PKI trust models allow varying approaches for security implementation for connected medical devices.

PKI for connected medical devices can be an open system for users to decide to join on-demand or a closed system. In a closed system, healthcare device providers control the deployment.

DigiCert's PKI platform is the future of medical device security

It is critical for deployment success that the PKI implementation is a viable and secure solution. DigiCert's platform can integrate into all major devices, system enrollment, and deployment processes.

PKI has been a go-to standard for Internet security for decades and is the best option for networked medical devices. PKI enables safe authentication of users, systems, and devices. When it is correctly implemented, it builds and supports security and trust for an entire environment. PKI is a solution that can scale to meet the unique needs of existing—as well as to-be-created—technology landscapes in the healthcare industry.

To talk to an expert about our healthcare security solutions call 1.801.701.9695 or email healthcareiot@digicert.com.

Trusted by Leading Enterprises

nextgen healthcare
surescripts
PLEX
eClinicalWorks
PayPal
FRESENIUS MEDICAL CARE
IBM
Microsoft

[1] http://www.computerworld.com/article/2494451/healthcare-it/in-home-health-monitoring-to-leap-six-fold- by-2017.html

[2] http://www.modernhealthcare.com/article/20150528/NEWS/150529899

[3] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[4] http://lpa.idexpertscorp.com/acton/attachment/6200/f-037a/1/-/-/-/-/Fifth%20Annual%20Privacy%20and%20 Security%20of%20Healthcare%20Data%20Report.pdf

[5] http://lpa.idexpertscorp.com/acton/attachment/6200/f-037a/1/-/-/-/-/Fifth%20Annual%20Privacy%20and%20 Security%20of%20Healthcare%20Data%20Report.pdf