Advantages of Using PKI to Secure Medical Devices

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]

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]

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

- Unsecure web interfaces
- +PUWH'EKGPV U[UVGO QT WUGT CWVJGPVKECVKQP
- Unsecure mobile connections
- 7PUGEWTG FGXKEG UQHVYCTG 'TOYCTG
- 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.

devices through software updates. DigiCert has experience working with
RTQXKFGTU VQ 'PF CP QRVKOCN UQNWVKQP DCUGF QP FGXKEG GPXKTQPOC