PKI FOR COMPLIANCE WITH U.S. CYBERSECURITY IMPROVEMENT ACT

DigiCert PKI solutions help bring IoT device manufacturers into compliance with the Internet of Things (IoT) Cybersecurity Improvement Act of 2020.

The act

What is in the law?

On December 4, 2020, the IoT Cybersecurity Improvement Act of 2020 was signed into law. This law requires the National Institute of Standards and Technology (NIST) to "develop and publish standards and guidelines for the federal government on the use and management" of any IoT device owned, controlled or connected to any government agency.[1] It also instructs the Office of Management and Budget (OMB) to review security policies and principles set by NIST, and to issue policies and guidelines that address security vulnerabilities within federal information systems.

Why is the law important?

The sponsors of the legislation, Representatives Robin Kelly of Illinois and Will Hurd of Texas, wanted to "ensure that the US government purchases secure devices and closes existing vulnerabilities to protect our national security and the personal information of American families."[2] The goal is to increase IoT security by establishing federal guidelines for private manufacturers, based on NIST-recommended standards for minimum security protocols and practices. From the factory floor to deployment in a government agency, this law ensures devices are secured against cyberattacks. In order to ensure that a broad range of security measures are included in these guidelines, NIST has been collaborating with private sector businesses to develop policies and principles under the IoT Cybersecurity Program.

1. Internet of Things Cybersecurity Improvement Act of 2020, H.R. 1668 § 1 et seq. (2020).

2. Internet of Things Cybersecurity Legislation Clears Congress, Heads to White House. (2020, November 18). Congresswoman Robin Kelly. Retrieved April 14, 2020.

The guidelines

What are the guidelines recommended by NIST?

In January 2020, NIST released guidelines (NISTIR 8259) focusing on six foundational activities that manufacturers need to evaluate when developing and releasing IoT devices. Four of the activities relate to pre-market requirements, and the last two are considered post-market activities.

1. Identify expected customers and use cases
2. Understand customer cybersecurity goals
3. Decide how to address customer goals
4. Plan for adequate support of customer goals
5. Define how to communicate with customer about security
6. Decide what and how to communicate to customer

In May 2020, NIST created additional guidelines to supplement NISTIR 8259, called "IoT Device Cybersecurity Capability Core Baseline" (NISTIR 8259A). The core baseline information outlines customer expectations from IoT manufacturers by defining common device cybersecurity capabilities.

1. Device Identification describes the need for a device to have a unique identifier associated with the device for device authentication, asset management, or part of a network control scheme
2. Device Configuration allows authorized entities to change feature functionality on devices
3. Data Protection requires that stored and transmitted data on the device is secure
4. Logical Access to Interfaces limits access to the IoT device through local interfaces such as touch screen, USB port, or a network
5. Software Updates allows software on the devices to be securely updated by authorized entities
6. Cybersecurity State Awareness is needed to either monitor or audit the IoT device in case of a device breach

To provide further guidance, NIST is in the process of adding additional guidelines, which are currently in the draft phase:

- "IoT Non-Technical Supporting Capability Core Baseline" (NISTIR 8259B)
- "Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline" (NISTIR 8259C)
- "Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government" (NISTIR 8259D)

What does this mean for IoT device manufacturers?

Device manufacturers will need to incorporate all cybersecurity core baseline capabilities into their IoT devices in order to sell them to the US Federal Government. In the future, lawmakers expect that these cybersecurity standards will become standard in the private sector, too. Since private sector consumers are expected to buy products similar to those purchased by the federal government, the law will hopefully promote greater security in all IoT devices.

Public Key Infrastructure brings compliance to IoT devices

PKI delivers security and trust in compliance with Federal law

For decades, PKI has been trusted to secure websites, email and communication. Modern PKI is the same proven foundation but built to secure today's technology.

IoT devices expand attack surfaces, exposing devices and systems to greater vulnerabilities or cyber threats. PKI provides the identity for authentication, and confidentiality via encryption and integrity. This ensures data hasn't been modified from the point of origin or while at rest on the device. PKI is a security solution that addresses the common cyber challenges identified by NIST.

PKI enables multiple security approaches:

- Mutual authentication
- Data encryption
- Secure boot
- Establishing device identity
- Ensuring integrity of firmware updates
- Data integrity
- Secure over the air (OTA) communications
- Multi-factor authentication (MFA)

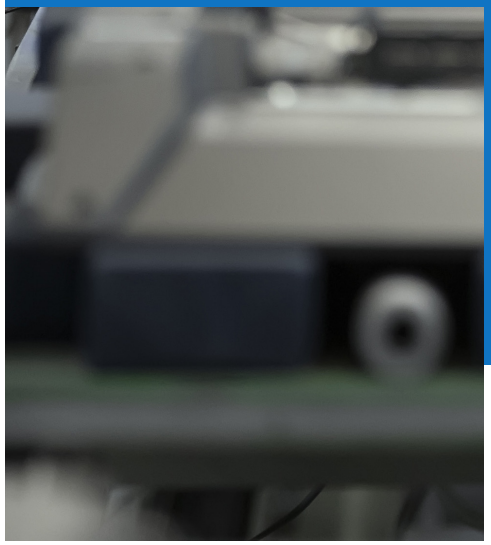
PKI is flexible for unique manufacturing needs

PKI for IoT is built to work easily with different manufacturing environments and processes. Manufacturers choose a PKI deployment configuration that meets their needs, so integration is seamless, and management is simple. Custom deployment options give manufacturers the flexibility to easily deploy, provision and create the PKI certificates at the core of the security solution—all without altering, delaying or reconfiguring their manufacturing ecosystem.

Some manufacturers may need an on-premises solution if there is no network available during manufacturing. Others may want a cloud solution for lower costs and easier set up. This kind of flexibility means that manufacturers can provision components or devices before manufacturing, during manufacturing, or even after the device is active in the field.

PKI provides unique, true device identity

Because every IoT device has a different computational power, communication protocol, field operation and lifespan, manufacturers need a security solution that works just as well on a smart watch as on a telecommunications satellite in orbit. PKI offers the ability to create certificate profiles, templates or protocols, tailored to the individual requirements of the solution or environment. This, in turn, creates an identity as unique as a fingerprint, so the manufacturer or user can verify that the device is, indeed, authentic and not a malicious entity masquerading as the original, true device.



PKI and IoT in the real world—example use cases

Built-in identity

IoT manufacturers need to periodically update software on deployed devices. With PKI, manufacturers can identify their own genuine products through the identity built into the certificate securing the device. Once the identity is confirmed, the manufacturer can send security software updates, patches or configuration changes by secure encryption using PKI. If the code is altered during transmission to the device, the device will see an unexpected change with the encryption, alerting the administrator.

Authentication verification

With PKI, manufacturers can monitor the state of their security by verifying the genuine identity of a device prior to granting access to the cloud service. Only a device with a valid PKI certificate can connect to the cloud, eliminating the possibility that a malicious actor could masquerade as the device to gain unauthorized access. As with the previous use case example, after identity is established and access is granted, PKI secures the in-transit communication, so any data traveling between the device and the cloud is protected against tampering.

Meet compliance with modern PKI solutions from DigiCert

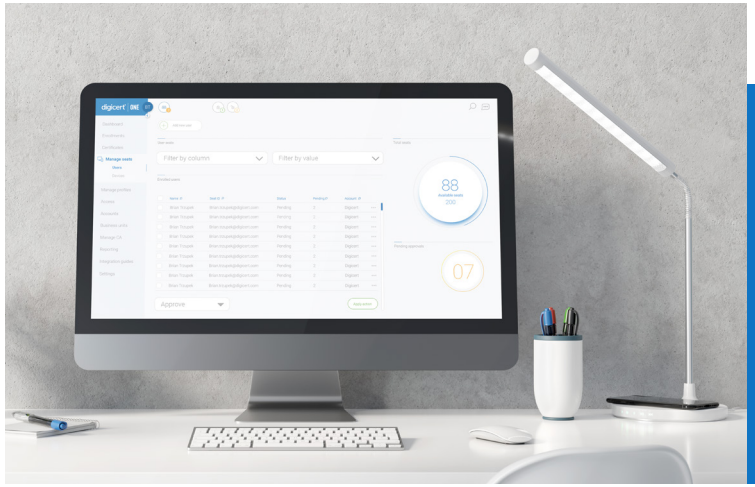
DigiCert® IoT Device Manager and DigiCert® Secure Software Manager help manufacturers meet and remain in compliance with the IoT Cybersecurity Improvement Act of 2020.

DigiCert IoT Device Manager is a PKI management system for provisioning and monitoring the digital certificates that encrypt and give identity to the device.

DigiCert Secure Software Manager ensures the confidentiality and integrity of the software being updated to each device.

Part of DigiCert® ONE

DigiCert IoT Device Manager and DigiCert Secure Software Manager are part of DigiCert ONE, a modern PKI platform built on cloud-native, container-based architecture. DigiCert ONE is fast and flexible, easy to stand up, highly scalable, and ready to meet your needs with multiple deployment options, including cloud, on-premises, hybrid or air-gapped.



Learn more

Interested in finding out more about PKI and IoT security? Talk to one of our experts about a custom solution for your devices. iot@digicert.com

About us

At DigiCert, finding a better way to secure the internet is a concept that goes all the way back to our roots. That's why our certificates are trusted everywhere, millions of times every day, by companies across the globe. It's why our customers consistently award us the most five-star service and support reviews in the industry. And it's why we'll continue to lead the industry toward a more innovative and secure future. In SSL, IoT, PKI, and beyond—DigiCert is the uncommon denominator.