KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

# Five Guiding Tenets for IoT Security

# Table of Contents

# The Promise of IoT and IoT Security

The rise of the Internet of Things (IoT) is like the advent of the Internet all over again. From the perspective of new business models and process transformation, IoT applications are perhaps even greater than what the Information Superhighway brought us a few decades ago. The universal connectivity of devices and ongoing innovation borne from access to real-time data is driving economic efficiency and growth. Impactful results across verticals and markets are already being witnessed - from the introduction of self-driving cars communicating with peers in a connected city, to self-regulating patient care from medical devices at any time and from any location.

In theory, IoT has the promise to be more secure than traditional IT, where humans and manual processes are typically the weakest link in the environment. That said, once a breach occurs within a machine-controlled network, the potential damage is exponentially more powerful, disruptive, and damaging. Not only can IoT devices be misused, but hackers can also compromise or sabotage data, triggering actions that are erroneous and destructive.

While the promise of greater security is present, reflecting on the naiveté of the early Internet should also serve as a warning for today's IoT aspirations. As the Internet became mainstream, developers and users were not focused on the nuances of conducting business online or the potential for malicious actors to hijack the web. The results of those oversights still impact today's web. A continuously evolving threat landscape relentlessly hammers away at the Internet's infrastructure and systems, often capitalizing on those whose foundations are inherently insecure.

The promise of IoT security rests in our willingness to learn important lessons from our experience in IT security and applying them to both the unique requirements and anticipated needs of the IoT. The potential of IoT security hinges on our ability to build a solid foundation across the IoT ecosystem, consisting of devices built with security and the necessary properties to ensure it endures.

The potential of IoT security hinges on our ability to build a solid foundation across the IoT ecosystem, consisting of devices built with security and the necessary properties to ensure it endures.

# The Industrial IoT Ups the Ante

The most enthusiastic sector to embrace the Internet of Things in a transformational way is the industrial sector. The **Industrial IoT (IIoT)** offers immense potential for an array of niches such as automotive, healthcare, energy, and aerospace. However, the cost of a breach in these domains is irrevocably high. It's one thing to have hackers infiltrate your laptop; it's another to have them compromise your medical device, your car, or the airplane you travel on. It's not hard to find evidence that the security risks within the IIoT are real. Two fast-moving verticals, medical devices and connected vehicles, paint an accurate picture of the current and future state of security issues for the IIoT.

## MEDICAL DEVICES

With the benefits real-time data transfer offers patients, physicians and providers, healthcare is one of the fastest moving IoT segments today. In fact, healthcare organizations have an average of 10,000 connected medical devices. Security problems in this sector can easily lead to nightmare scenarios. Medical IoT poses security risks on multiple fronts. First, connected records systems containing personal information are lush targets for identity thieves. Compromising a medical device and using it as a network beachhead could result in a breach of patient records. Secondly, and with more life and death consequences, attackers could exert control over medical equipment with potentially fatal results.

Vulnerabilities in connected medical devices such as pacemakers and infusion pumps have led to recalls and warnings as early as 2011. In 2017, the *US Food and Drug Administration* (FDA) recalled 465,000 pacemakers after discovering security flaws that could allow hackers to drain device batteries or send malicious instructions to modify a patient's heartbeat. The advisory stated that nearby attackers could "gain unauthorized access to a pacemaker and issue commands, change settings, or otherwise interfere with the intended function of the pacemaker." The flaws discovered included an ability to bypass the pacemaker's authentication algorithm, and unencrypted patient information being transmitted to and from home monitoring units.

The *Industrial Control Systems Cyber Emergency Response Team* (ICS-CERT) issued a similar warning in September 2017 for wireless syringe infusion pumps used in acute care settings (i.e. neonatal and intensive care units). When successfully exploited, the flaws can enable "a remote attacker to gain unauthorized access and impact the intended operation of the pump." The critical and high-severity flaws discovered included an ability to bypass the Class-3 implantable device's authentication algorithm, use of hardcoded usernames and passwords to establish wireless connections, lack of authentication for FTP connections, and improper certificate validation and access control.

Medical devices will always be appealing targets for hackers. Not necessarily to impact an individual patient's health, but as a means to breach healthcare system networks where information is collected. This information, susceptible to ransomware attacks, carries a black market value exponentially greater than credit card records.

## CONNECTED VEHICLES

Ironically, one of the most appealing benefits of connected cars is enhanced safety, whether through predictive maintenance of critical components, accident avoidance courtesy of sensors and AI, or precision control of safety features such as airbags and brakes. In reality, though, these connected systems have proven to be vulnerable to hacking, leading them and the entire vehicle to be viewed as a target.

Many of these attacks, witnessed in both controlled tests and real usage scenarios, target the *Controller Area Network* (CAN). and through it can reach all vehicle components, ranging from parking sensors to safety systems and infotainment units.

In 2015, cyber security researchers Charlie Miller and Chris Valasek made headlines after remotely hijacking a *Jeep Cherokee* while it was driving, turning off the transmission while the vehicle was on the freeway. Security measures missing included the lack of code signing and firmware validation when updating ECUs, as well as weak or no authentication required to gain system access. The duo recently stated they had expanded their bag of tricks, and could cause unintended acceleration or tamper with the car's steering wheel or brakes when the car is traveling at any speed.

In a 2016 proof-of-concept hack, Chinese researchers from Keen Security Lab were able to compromise the electronic systems of a *Tesla Model S* vehicle from 12 miles away. The "white hat" hackers succeeded in meddling with the vehicle's brakes, dashboard computer screen, door locks and other systems. The hack targeted the controller area network (CAN bus), a collection of connected computers found inside modern vehicles that control everything from indicators to brakes. Tesla released an update following notification of the hack, requiring all new firmware to be digitally signed with a cryptographic key. This code signing update was pushed out wirelessly in a software update to all *Tesla S* cars and Tesla X SUVs. One year later, the Chinese researches were at it again, successfully hacking a Tesla Model X.

As more connected car models are being designed, manufactured and brought to market, the potential target pool for such attacks will naturally increase.

In these examples and others being witnessed across other verticals, a proper security foundation was not in place. Some basic and well-versed security measures could have prevented negative outcomes. With an industry shift to facilitate over-the-air updates, whether to fine-tune an existing component or upgrade functionality and enhance the driving experience, connected vehicles and their components require security to be a core element built into its foundation.

# Lead with Experience and Vision

The **Industrial Internet Consortium (IIC)**, and the **IoT Security Foundation (IoTSF)** have developed security frameworks to help address many foreseeable problems. Their work is taking place in-tandem with industry-specific projects whose comprehensiveness and maturity vary greatly by vertical and region. These efforts continue to evolve, with enforcement of tangible policy coming through after lengthy review processes at both government and industry levels. Not to mention lead time for vendors to formalize compliant hardware and software offerings and prove compatibility.

Polished standards or not, the IoT train has left the station. Manufacturers can no longer design today and deploy with the hopes of securing equipment & devices later. Unlike our experience in the world of IT and the Internet, some characteristics of the IoT mean such an approach would be costly, ineffective, and often impossible. Those factors include the sheer magnitude of IoT deployments, where 100,000 devices can be a modest starting point. The diversity of hardware, software and protocols is another factor, as is the reality that most IoT devices are headless, deployed broadly, and never touched again (unless an automated process is in place).

Moving forward with IoT requires leading with experience, collaboration, and vision.

The IoT train has left the station. Manufacturers can no longer design today and deploy with the hopes of securing equipment and devices later. Such an approach would be costly, ineffective, and often impossible.

# 5 Guiding Tenets for IoT Security

The following tenets of IoT security help establish a secure foundation. All of which can be adopted and fully executed today.

01

### UNIQUE CREDENTIALS FOR EACH DEVICE

Using unique digital certificates for every device allows an organization to validate that a device is authentic and assert with high assurance that its messages are genuine. It also allows IoT platforms and applications to validate the integrity of messages sent to and from each device, ensuring that valuable data is sent from and received by only the intended recipients. The impacts of a compromised device are minimized as a result of each device carrying its own unique identity and encrypting its data with keys associated to that unique identity.

Common alternatives within the IoT include static passwords and shared keys, neither of which provide the required level of security or control. Compromising a static password allows access to or impersonation of, any and all devices utilizing that password. Should that password be stored in clear text, the task is unfortunately quite simple. Updating the compromised password across all deployed devices is challenging and sometimes impossible due to being embedded within code. While shared keys are a stronger method than text-based passwords, they do not allow for absolute differentiation between devices in the IoT ecosystem. This is because multiple devices authenticate with the same key and any subsequent identifying information cannot be validated with any credibility. Ensuring that specific instructions only reach a particular device, or validating that that specific data came from a particular device, are both out of reach unless each device carries its own unique and strong credentials.

02

### PRIVATE KEY STORAGE IN HARDWARE WHEREVER FEASIBLE

**Trusted Platform Module (TPM)** technology or Secure Storage hardware are designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that carries out cryptographic operations. It allows a hardware-enabled way to secure your cryptographic keys and certificates.

03

### VERIFICATION OF DIGITALLY-SIGNED FIRMWARE AND SOFTWARE UPDATES

Executables and scripts can cause potential damage to a device. Therefore, it's important that devices verify the authenticity of any new software or firmware prior to their installation. Code signing is the method of using a certificate-based digital signature to sign executables and scripts in order to verify the author's identity and ensure the code has not been changed or corrupted since it was signed by the author.

04

### ESTABLISHING AN ORGANIZATION-SPECIFIC ROOT OF TRUST (RoT)

When you manage your own **Root of Trust (RoT)**, you have complete control over the identity validation of every device or person you are issuing a key to. Once the accompanying digital certificate is issued, anyone can verify the identity of the key holder.

Sharing a RoT with other parties, whether partners, competitors, or complete strangers, results in sharing risk. The compromised root of another party should not impact your security. By maintaining your own private RoT you are ensuring a chain of trust that contains only constituents you authorize.

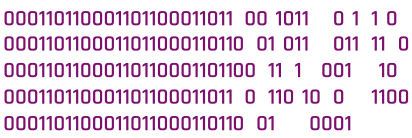
With the value of **Public Key Infrastructure (PKI)** for IoT more broadly understood and leveraged, we're seeing more and more device manufacturers shipping their hardware with keys and certificates pre-loaded. Chip manufacturers and suppliers of other subcomponents are doing the same. Rather than blindly accepting their trust model and its operations and subsequently sharing their RoT with the rest of their customers, these certificates and keys can be used to validate the authenticity of the new hardware when it first arrives, followed by bootstrapping over to credentials issued from your own private RoT.

## 05

## CONTINUAL LIFECYCLE MANAGEMENT FOR CERTIFICATES, KEYS, AND RoT

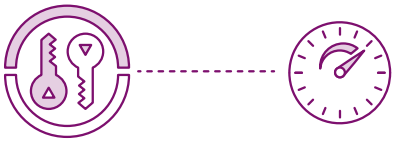
Renewable, replaceable and revocable credentials, along with an updatable RoT, are non-negotiable requirements. Static systems are inherently insecure and this principal applies to cryptography as well. It is inevitable that cryptographic algorithms weaken over time and many IoT devices will be deployed for durations that extend well beyond the effectiveness of their cryptographic keys. As a result, one must be able to perform complete lifecycle management for certificates, keys, and RoT that are stored on devices (and within IoT ecosystem gateways, servers, and applications).

**Security response cases that require the management of certificates and keys include:**



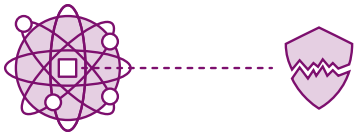
### DEPRECIATION OF ORIGINAL CRYPTOGRAPHY

As per Moore's Law and ongoing advances in computing resources, encryption algorithms used today will not be effective or secure in the future. As cryptography algorithms evolve, new Roots of Trust, certificates and keys will need to be installed on all devices and ecosystem participants, including those already deployed.



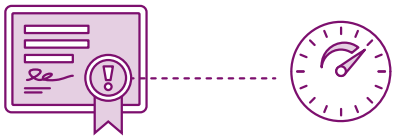
### CERTIFICATE AUTHORITY COMPROMISE OR DEPRECIATION

A recent example includes a wave of customers reacting to Google's depreciation of Symantec certificates, and replacing certificates and keys following their issuance from a different CA.



### QUANTUM COMPUTING ADVANCES

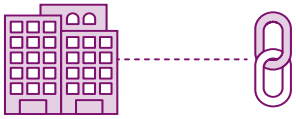
In the near future, most public-key algorithms may be broken by available computing power. Existing devices will require immediate removal of their certificates, keys, and trust stores, along with the installation of replacements from a post-quantum resistant RoT.



### EXPIRATION

Best practices for certificate issuance is to set an expiration of 1 or 2 years (dependent upon specific use case) and not 50 or 99 years as commonly seen in an effort to avoid this lifecycle management step. Given that devices will have longer life spans, tracking of certificate expirations and enrollment for replacement credentials is not a nice-to-have—it's a mandate.

**In addition to these security influencers for the management of certificates and keys, there are also predictable business triggers, including:**



### CHANGE OF OWNERSHIP

Devices that you own today may be sold or transferred to another party in the future—especially in the case of more expensive devices and those with long deployment life spans. While bringing the devices back to the manufacturing line for reprogramming is not an option, there will still be a requirement to reconfigure the device's identity along with who trusts it, and who it trusts.

### INTRODUCTION OF NEW OPERATORS

In addition to transferring a device's ownership, there may also be cases when a new entity is introduced to support that device and handle its maintenance or servicing. Rather than extending your RoT from one organization to the other so both can communicate with the device, adding an additional identity to the device from a different RoT would allow both parties to trust it and communicate with it.

# Public Key Infrastructure (PKI) for IoT

PKI is a trust framework composed of hardware, software, policies, and procedures needed to manage trusted digital certificates and public key encryption. PKI offers an effective and secure identity layer that is scalable and capable of accommodating millions of device identities. Usage of PKI enables the critical security elements of authentication, encryption and code signing.

When compared to identification alternatives, PKI offers the richest capabilities and highest security assurance level possible. Shared passwords and tokens can be compromised. Unauthorized devices can use them to attempt to access your IoT systems. These passwords and tokens are difficult to update and having a shared key limits the ability to control the identity and access of particular devices within the overall fleet.

In broad use for several decades and widely trusted by most large IT organizations, PKI offers non-exportable digital identities, individually controlled at a per-device level, and enforced within all authentication and encryption functions.

While PKI can secure an IoT system, the cost, time, and expertise needed to manage a robust PKI can be staggering. From services to resource salaries and hardware, annual in-house PKI maintenance can cost from $300,000 to more than $1 million.

Strong PKI operations also tend to deteriorate over time, requiring further maintenance. As projects expand and new initiatives arise, organizations find themselves enabling PKI in new workloads without factoring those demands into their original PKI design or operations model. This results in widening security gaps and increased stress on management teams. Continued operational oversight and built-in scalability are mandatory for a PKI to continue supporting original requirements while taking on new initiatives, all while maintaining its security assurance level.

One popular method to ensure the ongoing efficiency and security assurance of a PKI is through a SaaS model. Consuming PKI through a managed service eliminates the direct responsibility of maintaining the system including functionality, performance, scaling, and security assurance levels.

# KEYFACTOR CONTROL

THE END-TO-END SECURE IDENTITY PLATFORM FOR CONNECTED DEVICES

IoT security begins with building a foundation of unique identity and trust. It is maintained by the ability to securely update devices throughout their operations. Keyfactor™ Control establishes trusted identity for your devices and provides complete identity lifecycle management for your IoT ecosystem. Keyfactor Control makes it easy and affordable to embed the high-assurance secure identity in every step of IoT device lifecycle. Through design, manufacturing, deployment, and ongoing management, Keyfactor Control provides the identity foundation you need to produce and sustain the most secure devices on the market.

## Keyfactor Control delivers the following core functions:

- **Unique Identity Provisioning—**In establishing unique identity for every device, the most common questions include how to get a digital certificate onto devices and what should happen when the device first connects. These elements are also the most pivotal in establishing a foundation for IoT security. Keyfactor Control ensures that every device has a unique identity assigned, a proper RoT is established, and a secure identity is provisioned during the device activation process. This configurable process includes setting up the device for unique identity provisioning, authentication of the device when it comes online, and registration of the unique device and its role within a central directory.
- **Secure Update & Management—**Devices cannot be deployed into the wild without the ability to stay on top of the fleet, and make updates. Knowing what devices are active, where they are operating, and having the ability to securely update them is a critical step to ensure ongoing IoT security. Keyfactor Control maintains a secure connection with each device, managing device identity centrally and remotely. This permits replacement of device certificates as well as modification of trust and key stores. This inventory management with identity refreshes, access controls, and other essential tasks, ensures everything stays current. These occur without recalling or replacing devices or waiting for a maintenance window when devices are taken offline.
- **Ecosystem Integration & Workflow—**With a RoT established and unique device identity in place, it becomes possible to authenticate all connections to and from the device. It's also possible to encrypt data communication between devices and the IoT gateways, platforms and applications they communicate with. The RoT established by Keyfactor Control can be leveraged by all IoT ecosystem elements capable of encryption and authentication. Certificate-based authentication, along with granular access control based on customizable extended attributes for each device is easily integrated into common IoT hardware, platforms and applications. Plugins, agents, and APIs are available for popular IoT platforms such as *ThingWorx, Azure IoT Hub, AWS IoT, SAP Leonardo*, and others.
- **Secure Code Signing Enablement—**Signing firmware and software updates are a critical best practice to ensure that the software installed in your devices is genuine. Keyfactor Control ensures that code signing keys are properly requested, approved, and generated—all critical steps in avoiding their misuse and malicious code being signed using a legitimate certificate.
- **Secure Worldwide Manufacturing—**Keyfactor Control works in conjunction with common ERP and MRP systems to establish "bootstrap" identities with information only known to the manufacturer. Your controls are reliably and securely accessible worldwide. The options are limitless. Be free to consider the best and most cost-effective ways to get things done knowing you can ensure authenticity and security during the build and deployment of your products.

### PRIVATE & PUBLIC CERTIFICATE AUTHORITIES

In addition to providing a private RoT together with a fully managed PKI, Keyfactor Control also includes a fully managed private PKI, and supports both internal certificate authorities as well as public issuers such as; *Microsoft™Certificates Services, Entrust™, Symantec™, DigiCert™, Certicom™, Verisign™, Thawte™, Comodo™ and GlobalSign™.*

### SCALABILITY

Proven in environments of 500 million devices, Keyfactor Control is designed for the mass scalability required by IoT. Keyfactor Control can run in the cloud or on-premise.

KEYFACTOR

# Conclusion

As the IoT landscape and security requirements evolve, an IoT system must be equipped with a solid identity framework from its inception. Secure devices are at the forefront of these efforts. PKI and a RoT provide a secure foundation for IoT devices, platforms, applications, and data analytics. A method to securely update device identity and trust ensures this foundation will stand the test of time and properly mitigate foreseeable obstacles that lie ahead.

Adherence to the five tenets for IoT security results in secured IoT devices and validated IoT data. Keyfactor has a rich history of partnering with businesses to secure IoT systems using software and managed services. Our PKI experts become an extension of your team, addressing IoT security challenges with the knowledge, experience, and operational efficiency to meet the needs of any business. As your organization moves forward with enhanced security, we invite you to explore additional information detailing Keyfactor Control functionality and use cases. We can provide best practices for planning, implementing, and managing a trusted and efficient IoT security solution.

Keyfactor Control makes it easy and affordable to embed high-assurance secure identity in every step of IoT device lifecycle. Through design, manufacturing, deployment, and ongoing management, Keyfactor Control provides the identity foundation you need to produce and sustain the most secure devices on the market—giving you the freedom to design great products with the confidence that they'll deploy and remain secure throughout their use.

## ADDITIONAL READING

**How to Navigate Complex Supply Chains to Build Trusted IoT Devices**

In this whitepaper, learn how a "zero trust" approach—designing security into devices while maintaining effective security controls throughout the process and product life cycle—ensures the safety of your devices from the production floor to the end-user.

DOWNLOAD WHITE PAPER

KEYFACTOR

Keyfactor is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate any key, any certificate, anywhere across the entire enterprise.

We help our customers apply cryptography in the right way from modern, multi-cloud enterprises to complex IoT supply chains.

With decades of cybersecurity experience, Keyfactor is trusted by more than 500 enterprises across the globe.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook.

CONTACT US

- www.keyfactor.com
- +1.216.785.2990