KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

Crypto-Agility for IoT

Table of Contents

The State of Cryptography and the Need for Crypto-Agility

Throughout history, cryptography has been used to maintain secrets and protect communications. Today, nearly all the hardware and software we use depend heavily on secure digital cryptography. Static systems are inherently unsecure and this principle applies to cryptography as well. There's no doubt that cryptographic algorithms currently in play will eventually be deemed unreliable. Moore's Law and the pre-dictable evolution of computing power always prevails. As such, many IoT devices will operate well beyond the effec-tiveness of their cryptographic keys.

With the outcome predetermined, readiness becomes a necessity. Not the readiness to respond to broken algorithms or their impact on data and communications - although that is important - but the readiness to respond to crypto risks.

In the world of IoT, the leading method to securely tag a device with a unique identity (and enable authentication, authorization, data encryption and verification of secure code) is the usage of digital certificates and keys.

Digital identity is an additional place where crypto-agility is required. In the world of IoT, the leading method to securely tag a device with a unique identity (and enable authentication, authorization, data encryption and verification of secure code) is the usage of digital certificates and keys. Threats to cryptography affect the foundation of digital identity and all processes built upon it, including message integrity. Therefore, the issuance of unique identities along with the readiness and ability to upgrade are essential to IoT security.

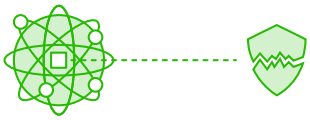
SCENARIOS

Security Response

When considering the need to swap out encryption keys, upgrade crypto libraries, or re-issue digital identities, incidents that draw critical security responses come to mind. Rightfully so, as the consequences of not responding can be significant.

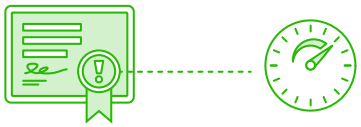
Crypto Library Bug

Discovery of a bug in crypto libraries may result in the need to generate new keys and reissue certificates according to the technology used in patching or replacing it.



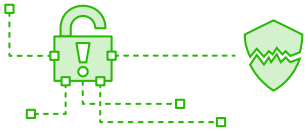
Quantum Computing

In as early as five-to-eight years from now, most public-key algorithms in use today will be susceptible to attack by Quantum computing processors.



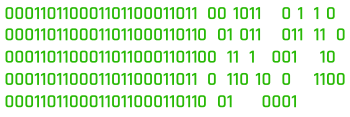
Certificate Expiration

It's common to see organizations extend the validity period of a certificate, sometimes to 25, 50, or even 99 years to avoid any chance of it expiring while in service. Certificate expiration is an important check and balance system to verify legitimacy and authorization, and ensure certificates a re r egularly re-issued. However, experts recommend validity periods of **no more than two to three years**. Maintaining a regular cadence for certificates will enable the management of certificates running like a well-oiled machine.



Compromise Or Breach Of Root

When a Root of Trust (RoT) is breached, all trust is lost. In the case of a certificate authority issuing certificates, it renders the chain of trust and all public and private key pairs moot, or even dangerous, as they can be issued and used maliciously. The immediate replacement of that RoT is required, along with the replacement of all certificates and keys used across all devices, applications, servers and services within the IoT ecosystem.



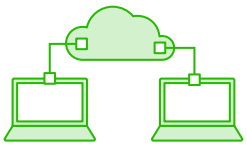
Algorithm Deprecation

Similar to a compromised RoT, a complete replacement is required with an outdated algorithm. Any keys that employ the affected algorithm are no longer secure. It should be assumed that their encryption can be broken by rogue actors, making data accessible and communications no longer secure.

SCENARIOS

Business Continuity

There's another set of scenarios to prepare for through crypto-agility. These incidents relate to operations to ensure that business is not adversely affected or interrupted completely as a result of cryptography.

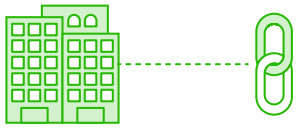


Change Of Device Ownership

IoT devices that you own today may be sold or transferred to another party in the future. Bringing devices back to the manufacturing line for reprogramming is not a viable option, nor is expanding the private chain of trust to include new owners. Regardless, for devices to communicate securely with the proper systems, there is still a requirement to reconfigure the device's identity. This is achieved by generating new keys and issuing new certificates, along with updating the trust stores that define who the device trusts and who trusts it.

Introduction Of New Operators

There are times when a new manager is introduced to support a fleet of devices and handle their maintenance or servicing. There are other situations where a new business partner requires interaction with the device alongside its existing processes and communication. Rather than sharing a private RoT and extending its chain from one organization to another, adding identities to the device, issued from a different RoT, allows all parties to trust it and communicate with it independently.



Mergers And Acquisitions

A change in business ownership or structure may require a modification of access policies within the IoT ecosystem. This includes changing or extending device identities, or the modification of crypto keys and certificates located on servers and appliances within on-premise or cloud-hosted infrastructures. As frequently seen in enterprise IT environments, responding to changes in business structure can take months if not years to complete. This is no different in the realm of IoT, and perhaps made even more challenging by the quantity, diversity, and geographic distribution of IoT devices.

Executing with Crypto-Agility

The above scenarios all have one thing in common: they require that devices holding certificates and keys be reachable and that elements be replaceable. Sending trucks to collect infusion pumps from regional clinics and hospitals and bring them back for reprogramming, could technically be considered crypto-agility. The same is true for requiring all vehicles in a particular line be brought in to the dealer for an update. It's unrealistic to think that there wouldn't be gaps in the process – nor would compliance be at 100%. Such an approach would significantly disrupt operations and negatively impact customer satisfaction.

It's not enough to have the ability to swap out certificates and keys. It is imperative to be non-disruptive to customers, attainable within targeted timeframes, and achievable within ecosystems consisting of hundreds of millions (or more) distributed IoT devices.

It's not enough to have the ability to swap out certificates and keys. It is imperative to be non-disruptive to customers, attainable within targeted timeframes, and achievable within ecosystems consisting of hundreds of millions (or more) distributed IoT devices.

FOUNDATIONS ARE ONLY BUILT ONCE

Digital identity is the foundation of IoT security. Identity lifecycle management for IoT devices is no less a requirement than it is for the user accounts issued for accessing IT networks and applications. As vital as it is to implement a secure, sustainable, and scalable identity foundation, it is equally critical to ensure that it functions through predictable future incidents and that its operations and security assurance level face no degradation.

KEYFACTOR CONTROL

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

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.

Empower your development teams to build it right.

Easily design identity and security into the device.

Secure identity has to be rooted in the design. Keyfactor Control makes it easy to incorporate robust cryptography that will ensure your devices do only what you intend them to do throughout their lifecycle.

Manufacture and deploy anywhere with confidence.

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.

Manage authenticity through the entire lifecycle.

Give your customers confidence your products are built to stay secure.

Keyfactor Control makes it easy to create products that are ready to go the distance—safely. Identity refreshes, access controls, and other essential tasks, ensure everything stays current.

ABOUT

KEYFACTOR

Keyfactor™, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its lifecycle, Keyfactor empowers global enterprises with the freedom to master every digital identity. Our clients are the most innovative brands in the industries where trust and reliability matter most.

CONTACT US

- keyfactor.com
- 216.785.2990

KEYFACTOR