EBOOK

Crypto-Agile PKI for the Future

KEYFACTOR

Table of Contents

The Need for Crypto-Agility: How to Know When Your Cyber Security Is Past Its Expiration Date

In an evolving cyber security landscape, defenses must continually evolve. Static systems are not only inherently insecure, they actually become less secure with every passing day. This principle applies to cryptography as much as to other types of cyber-defenses. And with the advent of quantum computing, most analysts agree that common cryptographic algorothims will eventually become ineffective.

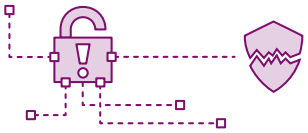
For nearly all hardware and software used in traditional IT environments and burgeoning Internet of Things ecosystems, the scale of potential threat is immense. It's very likely that many IoT devices' lifespans will extend well beyond the effectiveness of their cryptographic keys.

One strategy to counter these threats is to make it difficult for cyber criminals to crack cryptography through whatever computing resources are accessible. However, the predictable evolution of computing power will ultimately erode the defenses of cryptography.

To be even more proactive, organizations must become agile in their readiness to respond to high-level crypto risk. The ability to act before threats become serious becomes an innate part of the lifecycle, resulting in a condition where crypto-agility is fundamental.

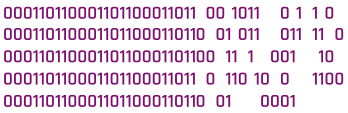
Staying Ahead of the Curve

If you're contemplating swapping out encryption keys, upgrading crypto libraries, or re-issuing digital identities, it's likely you are responding to a critical security threat. You'd be right to respond swiftly for the ramifications of not responding can be grave. The consequences of not reacting to the evolving threat landscape through crypto-agility are equally severe.



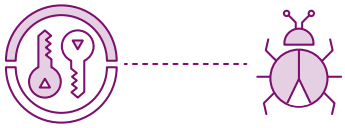
COMPROMISE OR BREACH OF ROOT

When a Root of Trust (RoT) is breached, all trust is lost. In the case of a certificate authority issuing certificates, a breach renders the chain of trust and all public and private keypairs moot, or even dangerous, as they can be issued and used maliciously. The immediate replacement of that RoT is required, along with the updating of all certificates and keys used by devices.



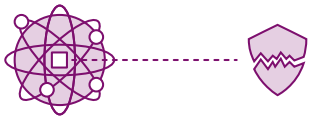
ALGORITHM DEPRECIATION

Similar to a compromised RoT, a complete replacement is required. Any keys using the affected algorithm are insecure. Rogue actors can break their encryption easily, rendering communication insecure while making data readily accessible.



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.

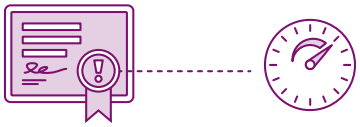


QUANTUM COMPUTING

According to Gartner analysts Mark Horvath and David Anthony Mahdi, most public-key algorithms in use today will be susceptible to attack by quantum computing processors within the next five to eight years.

This looming expiration date for trusted cryptography algorithms will require the immediate removal of certificates, keys and trust stores, along with the swift installation of replacements from a quantum-resistant cryptography root. In their 2016 Post-Quantum Cryptography report, The National Institute of Standards and Technology (NIST) described in no uncertain terms, the projected effects of inaction:

> This would severely compromise the confidentiality and integrity of digital communications on the Internet and elsewhere.
>
> –
>
> NISTIR 8105 – REPORT ON POST-QUANTUM CRYPTOGRAPHY, PUBLISHED: APRIL 2016

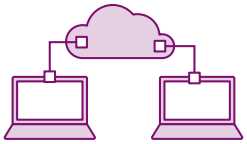


CERTIFICATE EXPIRATION

When certificates are used past their shelf life, they can fail at authentication or establishing secure communication tunnels. Certificate expiry on its own is not necessarily a security response incident like the scenarios mentioned above. However, the method used to avoid such interruption of service is such a case. It is common to see organizations extend the validity period of a certificate to 25, 50, or even 99 years to avoid any chance of it expiring while in service and requiring replacement. Certificate expiration is an important mechanism to ensure certificates are regularly re-issued. It offers a check and balance system, in the form of workflow and approvals, to verify current legitimacy and authorization. Experts recommend applying validity periods of two to three years for this reason.

Ensuring Business Continuity

Maintaining crypto-agility is also vital for operations to ensure that the business is not adversely affected or interrupted completely, as a result of cryptography-based disruptions. Here are three scenarios requiring special consideration:

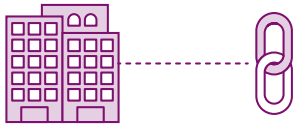


CHANGE OF DEVICE OWNERSHIP

Devices that you own today may be sold or transferred to another party in the future. This is especially common with devices that have long lifespans and high price tags in industrial environments. Sending such devices back to the manufacturer for reprogramming is not an option, nor is expanding the private chain of trust to include new owners. Regardless, for devices to communicate with the proper systems, there is a need 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

In addition to transferring a device's ownership, there are cases when a new entity is introduced to support a fleet of devices and handle their maintenance or servicing. There are also situations where a new business partner requires interaction with the device alongside its existing processes and communication. It's not advisable to share a private RoT, extending its chain from one organization to another as relationships are formed as it presents a future threat if/when relationships disband. A better practice is to adjoin additional identities to the device issued from a different RoT, allowing all parties to trust and communicate with it independently.



MERGERS AND ACQUISITIONS

Any change in business ownership or structure may result in the need to modify access policies within the IoT ecosystem. Such scenarios require modifying device identities, similar to the cases mentioned above, as well as modifying crypto keys and certificates located on servers and appliances within on-premise or cloud-hosted infrastructures.

Frequently in enterprise IT environments, responding to changes in business structure can take months if not years to complete. The same principle applies to IoT, where the quantity, diversity, and geographic distribution of connected devices poses additional potential hurdles. In both cases, it is vital that crypto-agility be a priority, even when business changes occur at a slow pace.

Executing with Crypto-Agility

The above scenarios all have one thing in common: they require that all devices holding certificates and keys be reachable, and those elements be replaceable. It is not enough to simply swap out certificates and keys. Instead, it is imperative to have the ability to do so in a manner that is:

01 →

NON-DISRUPTIVE TO CUSTOMERS AND BUSINESSES

02 →

ATTAINABLE WITHIN MISSION COMMENSURATE TIMEFRAMES

03 →

ACHIEVABLE WITHIN ECOSYSTEMS CONSISTING OF HUNDREDS OF MILLIONS (OR MORE) DISTRIBUTED DEVICES

Knowing What You Have Before It's Gone

The basic principle of having a crypto-agile digital certificate/PKI management solution is knowing what you have and how to deliver secure updates at scale. The following questions can help drive priorities:

01

How many digital certificates do you have?

02

Where are they?

03

What are they used for?

04

What hash algorithm are they using and what is their overall health?

05

When will they expire?

06

Who owns them?

07

How are you protecting valuable code-signing certificates?

08

Do you have a centralized method to securely update each one?

Every Certificate Matters

Don't create blind spots in your IT networks. You must ensure that you are monitoring every certificate, wherever it may reside, and from wherever it may have been issued.

What you can see doesn't always amount to what you have. Network discovery is a basic means to assemble a collection of certificates after they've been issued and deployed - but is often too little and too late. With the ability for individual application and networking teams to issue, purchase, and deploy their own certificates, control over certificate policies is easily lost. The result is certificates deployed on the internal network — and often on the public Internet — that do not conform to security policy, and whose configuration and expiration can lead to costly downtime or security breaches.

Additionally, without any centralized database of these troublesome certificates, tracking them down, replacing them, and mitigating the risk they pose becomes a significant time-consuming challenge. Only direct synchronization with your Certificate Authorities (CAs) results in a complete view of your certificate inventory, comprehensive certificate lifecycle management capabilities, and infrastructure-wide enforcement of security policy. When you are in control of certificate issuance processes, and are aware of all new certificates as they are issued and deployed, you can successfully build a digital identity foundation that is manageable, scalable, and secure.

KEYFACTOR COMMAND CA

Gateways allow for direct integration with your certificate authority, or multiple CAs in parallel. This capability enables you to ascertain every issued certificate, and coordinate every lifecycle management action taken. Certificates issued by these CAs are automatically synchronized, allowing you to inventory, renew, reissue, and re-enroll with one-step automation from within your single Keyfactor Command console.

KEYFACTOR ECOSYSTEM INTEGRATION

Built to support widespread adoption of PKI, our modular certificate lifecycle automation platform is easily extensible to enable crypto-agility in the cloud and DevOps toolchain.

Complete Visibility

After a complete inventory is in place and issuance workflow is synchronized with the certificate authorities, network discovery can be used to monitor the deployment and presence of certificates, setting the stage for proper evaluation of policy compliance and alerting of all anomalies.

- FLEXIBLE
- INTEROPERABLE
- EXTENDABLE
- CUSTOMIZABLE

Code Signing Certificates

The demand for trust in today's uber-connected digital society is unprecedented. Consumers of software require proof that the application they are using is legitimate. Secure code signing validates the author of the software and proves that the code has not been altered or tampered with after it was signed. Trusted code signing certificates are used to verify authenticity, but what is preserving the integrity of those certificates?

Code signing certificates can be sold or used to create signed malware. Developers must take extreme care in protecting private keys mapped to code signing certificates to avoid complications. A streamlined, secure code signing process safeguards your business and provides inherent trust to your software consumers.

KEYFACTOR COMMAND SECURE CODE SIGNING MODULE

The Keyfactor Command secure code signing module locates and transfers all code signing certificates from enterprise network locations (including all networked PC, storage, and thumb drives) to a secure vault. Once inside, the certificates never leave the vault. A user with appropriate access presents the code to be signed to the module where it's signed and returned to the user. Access controls are in place to ensure that only those with the right privileges can sign software and firmware.

Certificate Lifecycle Automation at Scale

Removing the manual and error-prone elements of common certificate management actions such as enrollment, re-issuance, renewal, renovation and inventory, Keyfactor Command provides a central console responsible for all certificate management tasks. Manual processes, spreadsheets and advanced monitoring tools may work well for small certificate counts and environments with limited issuance capabilities, but most large organizations have come to recognize that there are more certificates deployed than they can track or even know about. The result is an increase in efforts and costs to stay on top of them, with the risk of security degradation from error and omission.

Keyfactor Command reporting, bolstered by configurable certificate metadata, provides comprehensive reporting from a single-pane-of-glass. Reports include granular insight into certificate status, deployment and usage. This data can be leveraged for customizable alerts including workflows that integrate via open APIs to business applications such as Splunk, ServiceNow, and Remedy.

KEYFACTOR COMMAND ONE-STEP AUTOMATION

Alleviates the costs and burdens of manual, partial, and decentralized certificate tracking, elevating security to required levels. Leveraging agents for device, server and network appliance endpoints and CA gateways for direct synchronization with a range of certificate authorities, one-step automation provides a platform for comprehensive monitoring and full lifecycle management of all enterprise certificates.

Keyfactor Command removes the manual and error-prone elements of common certificate management actions such as enrollment, re-issuance, renewal, revocation, and inventory, providing a central console responsible for all certificate management tasks, along with direct connectivity to network endpoints including: devices, computers, servers, and network appliances. The platform allows execution of routine tasks remotely on either individual certificates or custom-defined collections of certificates to establish crypto-agility.

Custom metadata and extended attributes, bound to certificates but without requiring certificate modification, allow for custom collections. Such collections can be defined by variables such as certificate types, expiration date ranges, encryption strength, device types, location, owner, or any other variable that leads to action being taken on a group of certificates jointly.

Whether it is finding and replacing all SHA-1 SSL certificates in one action, or updating the trusted root stores of all network firewalls and load balancers in one shot, Keyfactor Command one-step automation reduces the time and effort required while ensuring uniform, successful and secure results across the infrastructure with the confidence of a futureproof, crypto-agile PKI and digital certificate management solution.

Preparing Cryptography for a Post-Quantum Era

Post-Quantum Cryptography. In another example of crypto-agility, Keyfactor and our partner ISARA announced the release of *the world's first quantum-safe, full-stack public key infrastructure solution.* With the new PKI technology, devices deployed today and updated in the future, are secure against conventional attacks and potential attacks leveraging quantum computers.

Many experts believe that quantum computing will pose a legitimate threat somewhere between 2025 and 2035. When it does, today's cryptographic algorithms such as RSA and ECC will become easily breakable. While 2025 may seem like a long way off, many systems being designed and deployed today will still be around then — especially "long-life" cryptographic systems such as industrial-focused IoT devices, cryptocurrencies, and PKIs. Savvy product engineers have already begun to plan for this event by designing crypto-agility directly into their products, with the help of the Keyfactor platform.

ISARA is preparing for a "post-quantum" world by creating crypto algorithms designed to withstand the coming onslaught of quantum computers. ISARA has been refining these quantum-resistant algorithms and working with standards bodies such as the International Telecommunication Union and Cisco to ensure that tomorrow's protocols and data formats can accommodate the new algorithms.

KEYFACTOR

ISARA

PARTNERSHIP

Keyfactor and ISARA have joined forces to make this technology usable today. By combining the power and flexibility of our Keyfactor platform with ISARA's cryptographic know-how, we've created an easy way to generate and manage certificates at massive scale, which are dual-signed—once with a conventional signature, and once with a quantum-resistant algorithm.

This combination provides crypto-agility—the ability to thwart current threats while preparing for the post-quantum cryptography attacks of the future. These certificates follow a newly-proposed standard that can serve as a transition from today's algorithms to the post-quantum future on the horizon.

Sun Tzu wrote in *Art of War* that *"To … not prepare is the greatest of crimes; to be prepared beforehand for any contingency is the greatest of virtues."* In our quickly changing computing environment, the risk of not being ready for this post-quantum era is potentially calamitous.

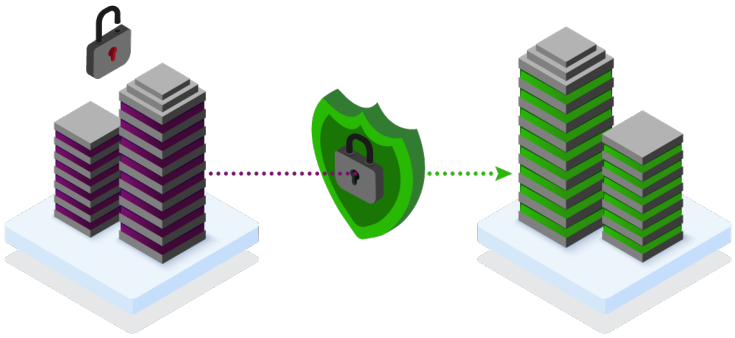
Next Steps

Sudden and unpredictable disruptions in the cryptographic landscape can leave your organization exposed to serious risk and disruption to productivity.

Keyfactor is the industry leader in crypto-agility solutions. We provide teams with the tools they need to deploy, manage, and automate keys and digital certificates across their business.

Ready to enable crypto-agility in your enterprise? See our products in action now.

See a Demo ▶



KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the impact that breaches, outages and failed audits from mismanaged digital certificates and keys have on brand loyalty and the bottom line. Powered by an award-winning PKI as-a-service platform for certificate lifecycle automation and IoT device security, IT and InfoSec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale. Exceptional products and a white-glove customer experience for its 500+ global customers have earned Keyfactor a 98.5% retention rate and a 99% support satisfaction rate.

Learn more at **keyfactor.com**

CONTACT US

- www.keyfactor.com
- +1.216.785.2990