EBOOK

A Framework for Enterprise Cryptography Management

TAG CYBER

KEYFACTOR

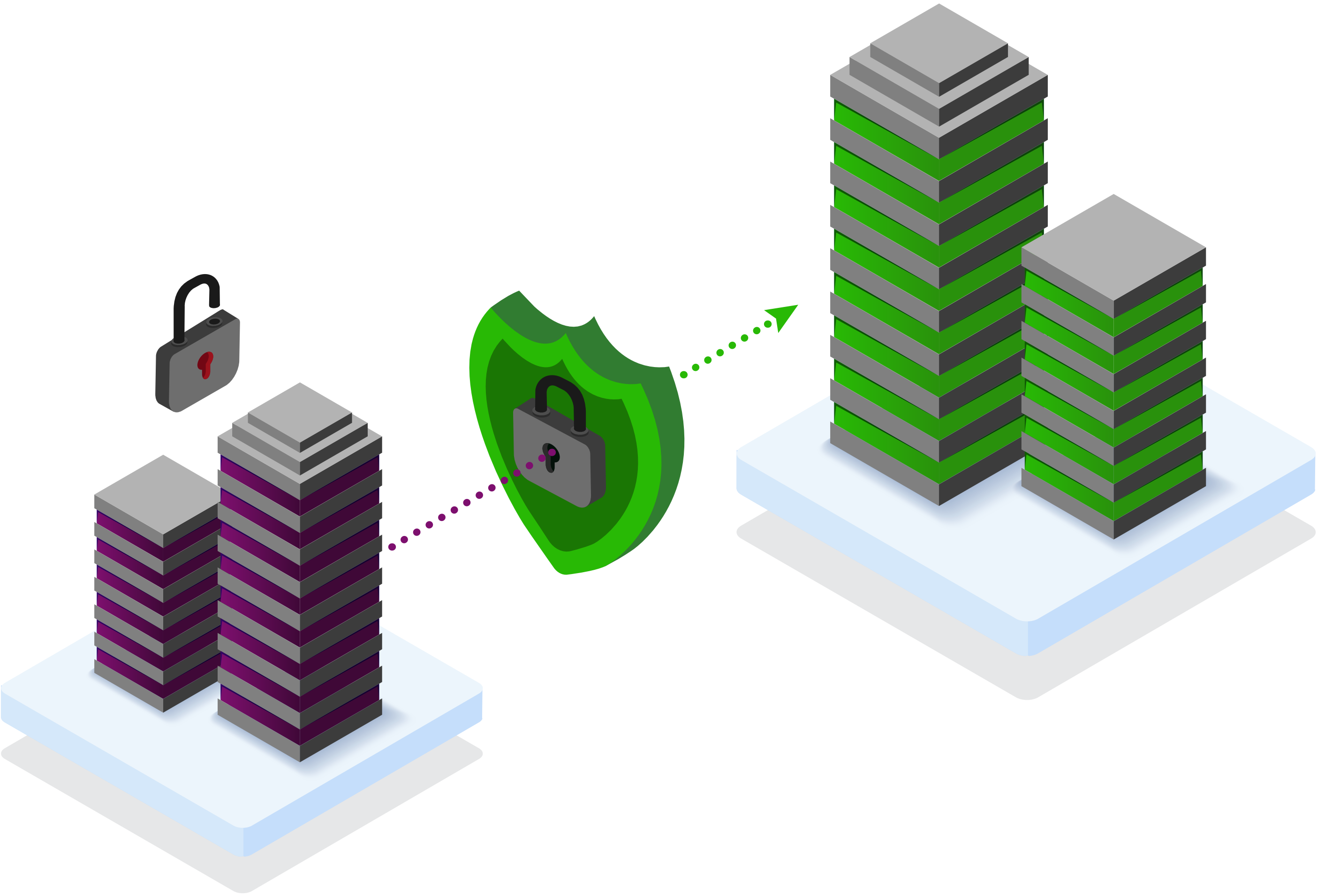


Table of Contents

HOW CRYPTOGRAPHY IS USED IN THE ENTERPRISE 4

PROPOSED FRAMEWORK IMPLEMENTATION 7

STEP 1: DEFINE POLICIES AND RESPONSIBILITIES 7

STEP 2: DEVELOP A CRYPTOGRAPHIC INVENTORY 8

STEP 3: IDENTIFY AND REMEDIATE VULNERABILITIES 9

STEP 4: CONTINUOUSLY MONITOR AND AUDIT 10

STEP 5: AUTOMATE THE LIFECYCLE IN AN AGILE MANNER 11

NEXT STEPS 12

Introduction

By far, cryptography is the most familiar method ever used to protect sensitive data for personal, business, government, and infrastructure applications. Available today in many different types, and across a range of different strengths, cryptography has always served as the primary means for securing data—long pre-dating even the use of computers and networks to process, store, and exchange information.

Because of this maturity, cryptography is generally accepted by most technology and business leaders as an important security control. Most understand that conventional symmetric algorithms are well-suited to protect their stored data, and that public key infrastructure (PKI)-based asymmetric methods are good at protecting communications and secrets exchanged between devices, workloads, and applications.

More recently, enterprise teams have recognized the need to understand their existing and planned cryptographic deployment in more detail. With a clear shift toward increased dependence on software-defined systems, virtualized infrastructure, and more intelligent control of operations, cryptographic controls have taken on a more prominent role in enterprise protection.

With the acceleration of enterprise infrastructure toward software-defined systems, the ubiquity of DevOps with its rapid CI/CD pipeline, instantaneous deployment of cloud-based services and IoT devices, enterprises end up with tens of thousands to millions of keys and certificates—and are typically unaware of the total number of these entities.

Thus, a mature understanding of the support requirements for end-to-end cryptography across the broad enterprise lifecycle is imperative for management teams. As the adage goes, you cannot protect what you cannot see—so when unmanaged keys and certificates are in use throughout the enterprise, unnecessary business-critical risk is introduced. This can only be addressed through careful attention across the end-to-end lifecycle.

IT and security leaders are now learning, often through difficult experience, that business-critical systems and data can be compromised due to sloppy key and certificate management, and that security and compliance requirements are often missed due to insufficient attention to end-to-end cryptography management. Managers now recognize that while cryptography addresses data security, it also introduces the obligation for good cryptographic key management. Cryptography has moved from a technical to a business issue.

This report introduces a framework for managing the lifecycle of cryptographic identities in the enterprise. The focus is to help bridge the gap between the traditional technical orientation of decisions made regarding cryptography in the enterprise—often by disparate groups located across the organization—and the more strategic management decision making required to minimize unnecessary costs, mitigate risks, and reduce or eliminate threats.

How Cryptography is Used in the Enterprise

To understand our proposed framework for end-to-end management of the cryptographic lifecycle for the enterprise, it is important first to take inventory of some of the more prominent aspects of enterprise cryptography management (ECM) in use today. Understanding how and where cryptography is used in the organization provides a baseline for implementing the practices and process described in this framework.

PKI-BASED OPERATIONS

Any discussion of cryptographic management must start with the day-to-day operational functions performed in support of all PKI-based systems. Such work includes selection and coordination of optimal PKI and certification authority (CA) vendors, as well as developing the preferred security policies, administrative procedures, and handling methods to be used for all PKI-based infrastructure.

USAGE

Considerations during PKI operations, often performed in conjunction with the identity and access management (IAM) team, include business and technical issues related to managing cost (with budget reductions common for PKI), reducing complexity (often for infrastructure that relies on PKI), and addressing scalability (which generally lines up with the size and scope of the organization).

CHALLENGES

PKI-based operations have traditionally been bogged down by high levels of complexity, especially for functions such as user registration, maintenance, and support. PKI solutions must therefore include simplified processes for these day-to-day support capabilities. Managers must also take the time to test and review the effectiveness of their PKI operations, including for special cases, exceptional conditions, and extreme situations.

SSL/TLS CERTIFICATES

A major component that must be identified during an inventory of enterprise key management functions is the use of SSL/TLS certificates used for server authentication, authentication to services and applications, and client authentication. Attention should be placed on which encryption algorithms are being used (e.g., Elliptic curve, RSA, DSA), as well as the applications that rely on these certificates (e.g., eCommerce, email).

USAGE

Other considerations for SSL/TLS certificate management, often performed by teams supporting network security, include issues related to the visibility of the certificates (i.e., certificate locations, validity and owners), agility of the certificates (which is complicated by different teams using multiple CA vendors), and identification of manual methods for certificate provisioning and renewal that would be improved through self-service workflows and automation.

CHALLENGES

The vast number of use-cases for SSL/TLS certificates —particularly in microservices and cloud environments —creates an inventory challenge for security teams. Nevertheless, identifying all cases of SSL/TLS usage is required to maintain full certificate lifecycle management and prevent outages.

CODE SIGNING

Another critical component in cryptographic management is the use of code signing certificates. This function involves providing proof by the software creator that the software is valid using a trusted signature. Generally, a standard cryptographic hash function algorithm is used as the basis of the code signing process.

USAGE

Primary considerations for code signing by development teams include how code signing keys are stored, accessed, and protected. Since code signing is an embedded component of the software lifecycle, with implications on audit and control, it is not always easy to identify its use via the standard inventory process. Code signing is also part of the supply chain process for enterprise teams. With increasing risk from third-party and open-source code, the need arises for secure distribution and updates to avoid forgery and tampering. Code signing helps prove the authenticity and integrity of software being used.

CHALLENGES

Enterprise teams have come to understand that their code signing processes can only establish sufficient trust and authenticity when the private keys used to sign code are kept under tight control. At the same time, software developers require fast access to sign code without leaving their native toolset or workflow.

SSH KEYS

Secure Shell (SSH) keys are widely used by network and infrastructure teams to secure and automate access to remote systems and applications. However, poor management of the widely used protocol creates significant exposure, including issues related to SSH key sprawl, access control, and key rotation. Considerations for SSH keys, often performed by network operations and administration teams supporting the enterprise, include issues related to the key sprawl, access controls, and key rotation.

USAGE

Best-practice guides for SSH key management are generally available to practitioners, and they tend to reinforce good cyber administration. This includes being particularly attentive to privileged sessions, getting an accurate inventory of SSH keys, focusing on rotating keys, bringing all SSH keys under active management, and avoiding the shared use of keys between multiple individuals. These are mostly common-sense measures to reduce the risk of orphaned or mishandled keys.

CHALLENGES

The fact that SSH key administration is controlled by network and infrastructure teams creates a challenge for security teams. They will have to coordinate proper security attention to ensure that automation is introduced in a suitable manner that will prevent any new threats from emerging into SSH use-cases.

SYMMETRIC KEYS

An additional element in the inventory process for ECM involves the more mature and familiar management of symmetric keys. While this was often implemented in a business using centralized key distribution center (KDC), along with a standard algorithm and protocol, it has since evolved into a distributed activity which can touch all aspects of an organization, and which can involve a myriad of different algorithms, protocols, and keys.

USAGE

Today, just about every aspect of the computing and networking infrastructure in a company includes the use of symmetric keys, ranging from the databases used to store sensitive information, to endpoint devices and virtual machines. The management of these keys can require action by the enterprise team (as with databases), or it can be hidden and performed by the operator (as with cloud services).

CHALLENGES

This can create challenges for organizations being asked to take full inventory of the key use considered in scope for tasks such as regulatory response or security audit. Making matters more difficult, the management and ownership of symmetric keys must also address issues related to multi-cloud use and virtualized infrastructure—neither of which lend comfortably to the inventory process.

EKM FUNCTION	TYPICAL RESPONSIBLE TEAM	COMMON CHALLENGES
PKI-Based Operations	Security/IAM Team	Cost, Complexity, Scalability
SSL/TLS Certificates	Network Security Team	Visibility, Agility Automation
Code Signing	Development Team	Software Process, Audit, Control
SSH Keys	Network Operations Team	Key Sprawl, Access Control, Key Rotation
Symmetric Keys	Multiple Teams (Including BUs)	Multi-Cloud, Virtual, BU Coordination

FIGURE 1. ECM FUNCTIONS, TEAMS, AND CHALLENGES

The implication here is that identifying the ECM processes in an enterprise is a more difficult task than one might expect, given the various different use cases, toolsets, and groups involved. The good news is that commercial tools and platforms do exist that can offer assistance to the security and other teams performing this function. Enterprise managers are advised to seek assistance from such vendors in the context of a lifecycle management process.

Proposed Framework Implementation

Below is a practical, end-to-end lifecycle framework for ECM that is intended primarily for business managers, and also technology practitioners who might be making important decisions about cryptographic solutions. The goal is to introduce a consistent framework to balance the cost, risk, threat, and practical usage goals that influence management and use of cryptography in the enterprise at scale.

The framework should be used in a stepwise manner, but practitioners will recognize that each of the steps might be interwoven, and that nothing demands that the process proceed in a monolithic direction.

STEP 1: Define Policies and Responsibilities

OBJECTIVES

- **Goals:** ECM goals should be defined and documented
- **Roles:** ECM-related roles and responsibilities should be determined
- **Design:** Initial architecture decisions related to encryption should be made

DESCRIPTION

Like any other IT or cybersecurity policy, defining policies and responsibilities for ECM must streamline the component tasks so that security objectives are met and business goals are respected. A thorough policy should start with high-level strategy and proceed to more tactical details, including generation, distribution, accounting, storage, use, and destruction of keys, as well as authorization guidelines and security controls for keys. Important steps in the creation of an organizational ECM lifecycle process include the following tasks:

- **Define ECM Goals and Strategy:** Develop and document the organization's key and certificate management goals and strategy, including whether the program will be centralized or de-centralized, who will be responsible, where policies will be stored, and how they will be maintained.
- **Document Existing ECM Architecture:** Develop and document the organization's current key and certificate management architecture. This requires early attention to inventory for the relevant ECM tasks that are ongoing.
- **Identify Relevant Encryption Requirements:** Validate present and future encryption requirements, including any audit or regulatory mandates from external bodies.

One challenge in writing an ECM policy is that cryptographic operations are typically not part of a centrally managed program. Instead, different departments and individuals will be responsible for various aspects of key management, which could lead to varying policy documents. To complicate matters further, managing and tracking keys at scale, across hybrid environments grows proportionally with an organization's attack surface. As hosts proliferate, so does the complexity of key management, and this has implications on policy.

Some enterprises might reasonably decide to maintain disparate policy documents for their ECM. This is particularly true for organizations that might include security and control requirements that vary depending on the application or data type in question. An ECM policy must also be written to accommodate the needs of different business units while simplifying processes. For example, with an enterprise, certain business units might be working on particularly sensitive data, which could result in special policy considerations.

At a high level, any ECM policy should describe the standards and organizational goals that the overall ECM program supports. It should take into account industry best practices and any legal or regulatory requirements, such as compliance with regulatory standards like FIPS 140-2 for Cryptographic Modules, and industry-specific mandates such as HIPAA and PCI DSS. ECM policies must also address key ownership, including who is responsible for what within business units regarding the management of keys and certificates.

ECM policies should start by considering all relevant controls, processes, and operations that support the organization's overall risk management strategy. This implies that ECM must be addressed in the context of an existing enterprise security architecture, infrastructure, and set of procedures. Cryptography should not be defined as an overlay to enterprise security, but should be created as an integrated component of the organizational defense.

At a foundational level, every ECM policy document should include the following important elements:

- **Classification:** This includes the type of keys (e.g., public, private, symmetric, asymmetric) based on the data, application, or process it's securing.
- **Authorization:** This specifies who and what has authorized access to keys; this also includes key storage and retention policies.
- **Identity:** This dictates how identity will be validated, how users/processes will be authenticated, and how least privilege will be enforced.
- **Lifecycle:** This covers how keys will be generated, distributed, deployed, provisioned, and governed; the crypto-period of individual keys; how administrators will handle end-of-life and/or restoration of keys.
- **Audit:** This is important for audit and control related tasks and includes requirements for logging.
- **Recovery:** This covers the backup, continuity, and disaster recovery testing of keys.

As with any security policy, organizations must perform a periodic review of their ECM policy and procedures document to ensure that it is up to date and relevant to both internal needs and external requirements, such as new compliance mandates, cryptographic standards, and business deployment needs.

STEP 2:

Develop a Cryptographic Inventory

OBJECTIVES

- **Goals:** Inventory processes must identify all aspects and usage of ECM
- **Automation:** ECM-related inventory processes can only scale using tools
- **Visibility:** Inventory enables insight and understanding of key and certificate usage

DESCRIPTION

As explained in the earlier sections, it is imperative to have full visibility into how and where cryptography is being used in the enterprise, including where keys and certificates are located and how they are being maintained across application, computing, service, and network environments. This is accomplished by a cryptographic inventory, and it is likely that the process will be ongoing since encryption usage will continually change.

Except for the most isolated and small-scale applications, manual inventory with spreadsheets is too time-consuming, error-prone, and inaccurate. In contrast, modern enterprise teams understand the need to deploy automated technology that can discover their cryptography, including key and certificate usage. If done properly, inventory processes can also help to identify anomalies such as rogue keys.

Automated cryptographic inventory tools are designed specifically to locate, identify, and report configured keys and certificates. These tools help administrators track cryptographic usage, as well as to help limit key sprawl, validate access controls, and ensure the timely rotation of SSH keys. Some common methods of discovery that are critical to gaining complete visibility using tool support include the following:

- **CA Integration for SSL/TLS:** Direct integration with certificate authorities helps to identify every certificate issued.
- **Network-based Discovery for SSL/TLS:** Tools can scan IP ranges, subnets, and ports to find SSL certificates.
- **On-Device Discovery of SSH and SSL/TLS Keys:** This includes agent-based or agentless discovery of key stores and file systems.
- **IaaS for Cloud-Issued Certifications:** New protocols such as the Key Management Interoperability Protocol (KMIP) from OASIS help different cloud providers discover certificates and provide bring-your-own-key (BYOK) capabilities.

With the implementation and use of the aforementioned automated methods of cryptographic discovery across the enterprise, management and operations teams will be able to answer the following questions:

- **Usage:** How many different CAs are being used throughout the organization, including internal, embedded, and external?
- **Location:** Where are the SSL/TLS certificates, code-signing certificates, and SSH keys being used?
- **Expiration:** Which keys and certificates are currently in active use versus expired or orphaned?
- **Strength:** What cryptographic algorithms and key lengths are being used for issuing CAs, keys, and certificates?
- **Lifecycle:** Who is responsible for the use and lifecycle handling of each key and certificate?
- **Rotation:** When will certificates or keys expire? What is the process for rotation or re-issuance?

Accurate inventory will also support overall governance of the cryptographic lifecycle to develop a big-picture view of ECM. This can resolve conflicts between teams, predict changes in the type of controls required to keep the organization secure, and achieve crypto-agility.

STEP 3:

Identify and Remediate Vulnerabilities

OBJECTIVES

- **Goals:** ECM vulnerabilities should be identified and remediated
- **Automation:** ECM vulnerability removal is best done using automated tools
- **Principles:** Security principles such as least privilege guide ECM risk reduction

DESCRIPTION

The use of cryptography, as with any cybersecurity management systems or protocols, can include its own vulnerabilities that might threaten the confidentiality, integrity, or availability of the data or systems which it is meant to protect. Some of the more common vulnerabilities enterprise teams might identify in their deployed cryptographic algorithms, protocols, tools, and systems include the following:

- **Algorithms:** Weak algorithms that may be vulnerable to present and future attacks
- **Storage:** Improper key storage and management which can lead to lost data
- **Configuration:** Poor configuration management which complicates administration
- **Rules:** Lax rules for key generation, authorization, and authentication
- **Visibility:** Lack of visibility into digital signing and other cryptographic tasks

An end-to-end cryptographic strategy supported by technology that addresses the full lifecycle can identify these weaknesses and pass remediation recommendations and/or tickets to supporting management tools (e.g. ITSM, SIEM, etc.). For this step, it is recommended to incorporate ECM into the organization's overall digital risk management framework, perhaps benchmarking against industry standards such as NIST Cybersecurity Framework (CSF), ISACA Control Objectives for Information Technologies (COBIT), or Capability Maturity Model Certification (CMMC).

At a more tactical level, in addition to obvious measures such as replacing bad or weak cryptography (often out-of-date), security teams also should plan to improve their cryptographic usage by the following activities:

- **Automation:** Teams can reduce risk by automating processes such as configuration management, and this is best accomplished at set-up time.
- **Auditability:** Teams should develop and maintain an immutable audit log of all key and certificate-related activities.
- **Least Privilege:** Teams should limit the use of, and access to, any cryptographic secrets—even for administrators.
- **Strengthening:** Teams should take the time to replace weaker encryption with stronger algorithms, and this extends to third-party and open-source systems.
- **Self-service:** Teams should be empowered to easily obtain security approved certificates.

STEP 4:

Continuously Monitor and Audit

OBJECTIVES

- **Goals:** ECM processes should include monitoring and auditing
- **Automation:** Continuous ECM monitoring can only be achieved by automated processes
- **Checklist:** A checklist provides guidance on the best elements for ECM monitoring

DESCRIPTION

As the digital ecosystem of modern enterprise continues to grow, especially for cloud services and containerized applications, key and certificate sprawl becomes inevitable. Similarly, new technologies such as Internet of Things (IoT)-based applications will tend to rely on the use of certificates for authentication and other cooperative protocols. As a result, cryptography will proportionately expand across the enterprise, thus increasing the challenges of ECM.

Management practice in any organizational use of cryptography should thus involve technology and processes for continuous monitoring and regular auditing. Continuous coverage implies having an accurate and ongoing understanding that approximates real-time visibility to the greatest degree possible. To do this, an organization must have defined plans for all aspects of ECM review, data collection, monitoring, and assessment. A sample checklist may include:

- **Audit:** ECM teams should regularly audit access and use of code-signing certificates, with attention to signers, approvers, and signing times.
- **Monitor:** Monitoring certificate authority-related activity will help ensure that certificate issuance remains within defined thresholds.
- **Time Stamps:** ECM teams should be continuously reviewing time-stamped code for issues or anomalies.
- **Expiration:** Teams should identify and remediate expired or out-of-policy certificates as policies evolve (e.g., self-signed, unauthorized, or weak).
- **Authorization:** It is important to audit processes for authorization and verification of trustworthiness of trust anchors.
- **Signing:** Review of the code signing submission and approval process can prevent signing of unapproved or malicious code.
- **Revocation:** The monitoring process should include repeat audit of certificate revocation processes.
- **Logs:** The overall ECM monitoring process should include regular review of all applicable audit logs.

STEP 5:

Automate the Lifecycle in an Agile Manner

OBJECTIVES

- **Goals:** The full ECM lifecycle should be automated to the highest degree possible
- **Roles:** Automation of ECM should involve all participants in the lifecycle
- **Design:** The goal should be agile, continuous management of cryptography

DESCRIPTION

Each of the four steps described above include references to the use of automated processes. This is driven by the desire to scale the ECM process, and to provide for continuous visibility into inventory, usage, and vulnerabilities. The goal of this fifth step—which can be performed in parallel with the other steps of the process—is to unify the automation into a common architecture to streamline usage and minimize both risk and costs.

The challenge in this automation design and development task is to select a suitable end-to-end platform that works seamlessly across all aspects of the environment and that integrates with development and deployment lifecycles. Enterprise security teams are thus advised to do their homework to select the best commercial ECM partner that can help automate the process in an effective manner.

Such automation should also be implemented in the context of the goals of modern agility. That is, just as DevOps has revolutionized how software is developed, maintained, and used, agile processes for ECM should have similar impacts to traditional key management processes. The goal is speed with accuracy, and this can only be achieved through automated platforms from capable commercial provider partners.

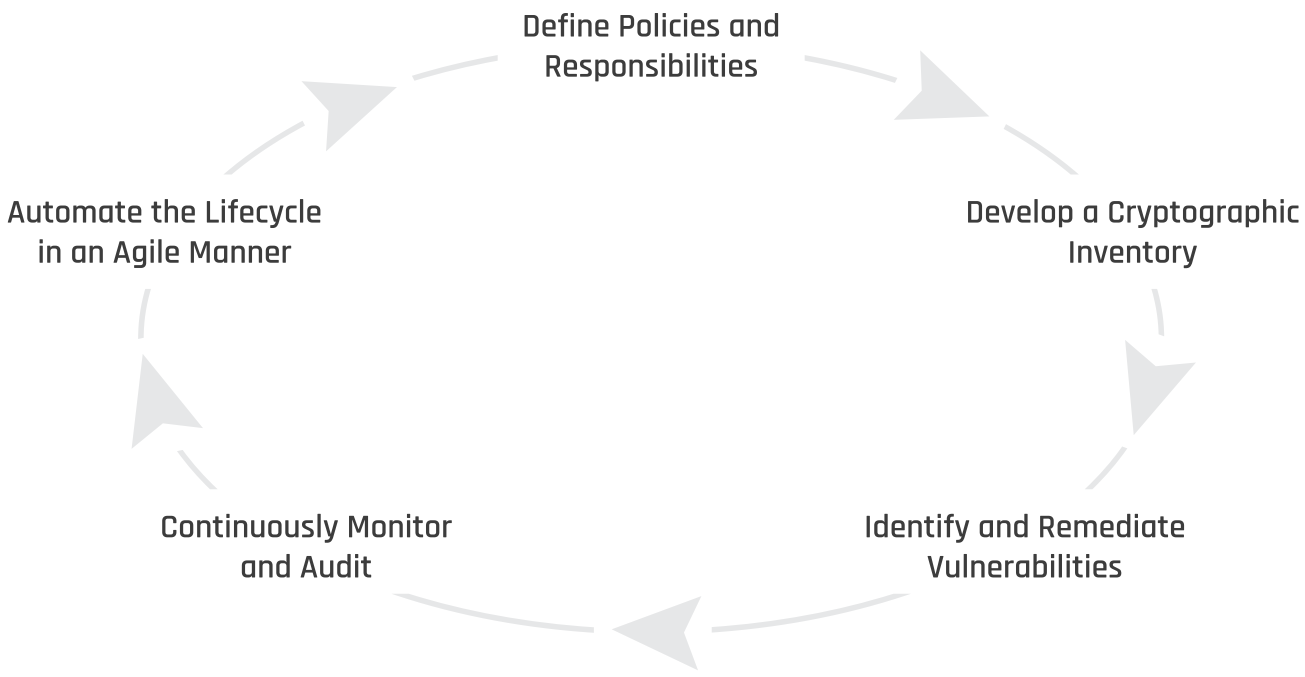

Define Policies and Responsibilities
Develop a Cryptographic Inventory
Identify and Remediate Vulnerabilities
Continuously Monitor and Audit
Automate the Lifecycle in an Agile Manner

FIGURE 2. END-TO-END METHODOLOGY FOR MANAGING THE CRYPTOGRAPHIC LIFECYCLE

Next Steps

The typical enterprise will benefit by first self assessing the degree to which the listed ECM functions, responsible groups, and typical challenges shown in Figure 1 match up with their current situation. This provides a suitable basis on which to implement the recommended end-to-end lifecycle methodology—which is also likely to be tailored to the local environment. Regardless of the path forward, enterprise teams are strongly encouraged to partner with a world-class commercial vendor with experience in practical ECM.

In summary, there are several reasons why an enterprise-wide strategy for end-to-end management of cryptography is so important, especially now. These include:

QUANTUM THREATS:

While this has not been emphasized in this report, the looming threat of quantum computing does introduce the need for inventory of existing ECM.

REGULATION AND AUDIT:

Enterprise teams in larger, more consequential environments, understand the increasing intensity of regulatory and audit requirements for ECM.

CRYPTOGRAPHIC STANDARDS:

With stricter industry standards, such as one-year SSL/TLS certificate lifespans, the need for a well-defined ECM strategy is imperative.

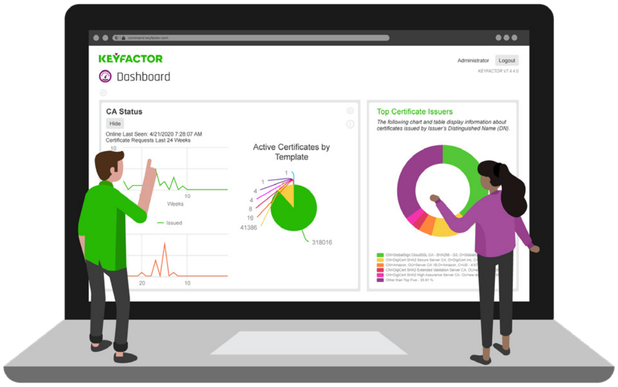
GROWTH:

The rapid growth of cryptographic identities for machines, cloud workloads, IoT systems, and mobile devices increases the need for certificates to replace passwords.

Conclusion

To see how Keyfactor can help manage all your cryptography through a single pane of glass, request a demo with us today.

Request a Demo ▶



The following chart and table display information about certificates issued by Issuer's Distinguished Name (DN).

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, InfoSec, and DevOps 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.

TAG CYBER

Founded in 2016 by Dr. Edward Amoroso, TAG Cyber bridges the gap between enterprise security practitioners and commercial cyber vendors. The company democratizes research and advisory content and services, and provides a range of consultative solutions for businesses and government. TAG Cyber's security portal is used by organizations of all sizes to obtain timely, personalized security information.