Keyfactor

Put a Stop to Certificate Outages

Gain visibility and control of every certificate in your environment

In today's digital landscape, certificates are crucial in securing communication channels and ensuring data privacy. But here's the problem: as organizations issue more and more certificates, it becomes difficult to manage them. Teams can't keep track of how many certificates they have or get an idea of the certificates they can't see. To make matters worse, different teams within the same company handle certificates in their own way.

To stay ahead of outages caused by expired or misconfigured certificates, PKI teams need visibility of all certificates, centralized management, and automation to avoid manual, error-prone processes. Visibility enables IT teams to monitor certificates in real-time and identify potential issues before they result in outages. Effective certificate management ensures that certificates are valid and up to date, reducing the risk of unexpected expirations. Certificate automation streamlines the renewal and deployment process, eliminating the need for manual intervention and reducing the risk of human error.

Keyfactor provides a foundation of visibility across public and private Certificate Authorities (CAs), network devices, and cloud infrastructure. By bringing your certificates into a single inventory, you can effectively monitor and automate their lifecycle to prevent outages — even on a massive scale.

Keyfactor solutions:

Certificate Lifecycle Management

You can't manage what you can't measure. Discover, manage, and automate every certificate

74% of organizations say they are deploying more keys and certificates

2023 State of Machine Identity Management Report

Challenges

Properly managing cryptographic assets is increasingly important to keep critical applications and websites secure and reliable. One of the biggest challenges businesses encounter is keeping track of all their certificates and keys. As they scale and use new technologies, the volume of issued certificates increases. If they lose track of these certificates, they can expire, leading to downtime, lost revenue, and a bad rep.

To protect these certificates and keys, businesses need to use modern management and automation capabilities. However, these measures can be tough to stand up, especially if businesses don't have the right tools or expertise.

3 common challenges of certificate outages:

01 Lack of visibility

Many enterprises are unaware of the true extent of their cryptographic assets, including keys and certificates, and are often unable to track when they expire. The limited visibility offered by spreadsheets and tools provided by Certificate Authorities leaves these organizations vulnerable to human error and increases the risk of security breaches.

02 Process inefficiencies

For security teams, speed is crucial. Unfortunately, manual certificate management processes can't keep up with the rapid pace and high volume at which teams work and new use cases arise. This creates significant challenges for organizations, making it tough to maintain efficiency and meet business demands.

03 Organizational risks

Legacy internal PKI systems and Certificate Authorities (CAs), like Microsoft CA, can present significant management and maintenance challenges for organizations. These systems become even more complicated by the current shortage of cybersecurity professionals, making it challenging to secure digital certificates and ensure that PKI remains up to date. Organizations need to simplify and consolidate their PKI to meet the emerging use cases while reducing the overall complexity of their IT infrastructure.

End-to-end visibility, management, and automation

With PKI and certificates, you must crawl before you walk and walk before you run. Discover, manage, and automate. With Keyfactor Command PKI teams reduce the potential for errors, ensuring that certificates are issued, renewed, and revoked correctly. The platform provides one-click approval workflows, fully automated certificate renewal, and provisioning to end devices without admin intervention.

Discovery (Crawl)

Uncover hidden certificates and potential risks effortlessly with thorough discovery. Gain 100 percent visibility via real-time CA synchronization, network SSL/TLS scanning, and key and certificate store discovery — ensuring comprehensive monitoring and proactive risk mitigation.

Management (Walk)

Effortlessly organize and maintain your certificate inventory while enabling alerts to notify users about expiring or non-compliant certificates. The simple, powerful UI with an interactive dashboard, certificate search engine, and drill-down capabilities enable users to find and easily remediate issues in seconds.

Automation (Run)

Work smarter, not harder, with real automation. Leverage the power of Keyfactor Orchestrators and their pre-built plugins to automate critical tasks like certificate renewal, provisioning, and installation. Provide your users convenient access to certificates through a self-service portal, REST API, and seamless integrations with server, cloud, and DevOps infrastructure for swift and efficient operations.

The Solution:

Machine Identity Management

Keyfactor

Command

Learn more ↗

Keyfactor Command enables you to orchestrate and automate your digital certificates from one platform allowing you to discover, manage, and automate the lifecycle of every machine identity. The platform offers customizable dashboards, detailed reporting, and automation capabilities, simplifying and streamlining certificate management, ensuring that your organization maintains compliance and establishes digital trust.

> "Certificates would expire, but we wouldn't know until systems went down. Since deploying Keyfactor, we've eliminated these incidents entirely."

David Yu
VP Security Architecture,
EQ Bank

Leverage Keyfactor Command in a deployment model that best fits your needs:

On-premises

Self-hosted

Deploy certificate lifecycle automation software in your data center or cloud

Cloud

Available in Azure

Deploy Keyfactor Command directly from the Azure Marketplace

CLAaaS

Hosted by Keyfactor

Consume certificate lifecycle automation as a service hosted by Keyfactor

PKIaaS

Hosted by Keyfactor

Combine Keyfactor Command with a fully hosted, 24/7 managed private PKI

Key benefits of outage prevention with Keyfactor

- ✓ Discover unknown certificates in your CAs, network, and CA stores
- ✓ Tag certificates with custom metadata to better organize your inventory
- ✓ Easily find and remediate risks like self-signed certificates with an interactive dashboard and certificate search engine
- ✓ Define user-based access controls and policies for more secure and simple management
- ✓ Automate certificate renewal and provisioning to end devices
- ✓ See all your certificates in a single, easy-to-use dashboard

Want more information about preventing disruptive certificate outages?

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946
  (North America)
- +46 8 735 61 01
  (Europe)