KEYFACTOR

Keyfactor for

# Federal Government

Establishing digital trust and protecting critical infrastructure for government agencies with PKI and machine identity management

## Keyfactor Solutions for Government:

### EJBCA ENTERPRISE

A flexible and trusted PKI solution based on open standards designed to issue identities at scale in government IT for all PKI use cases. EJBCA is compliant with industry standards like Common Criteria, NIAP, and CSfC.

### KEYFACTOR COMMAND

End-to-end machine identity management for continuous visibility, policy enforcement, and automation of keys and digital certificates across hybrid and multi-cloud environments.

### KEYFACTOR SIGNSERVER

Highly secure and seamless code and document signing to ensure the integrity of sensitive documents and code running on critical systems.

Agencies are now embracing a zero-trust approach to secure data and systems. In this perimeterless reality, public key infrastructure (PKI) and machine identities, such as SSL/TLS and code signing certificates, are foundational technologies to enable zero trust and enhance security in the software supply chain.

To support zero trust architecture (ZTA), agencies must be able to manage machine identities in the same way they must protect employee and contractor PIV-201 identities. All machine certificates need to be accounted for and properly assigned to the correct system owner(s) to ensure compliance, system security, and availability.

Keyfactor's PKI and machine identity management platform enables government agencies and departments to issue, monitor, and automate the lifecycle of keys and digital certificates across complex, hybrid IT environments. Trusted by federal, state, and local governments in the U.S. across the globe, Keyfactor delivers visibility, governance, and operational efficiency.

## PKI and Machine Identities are Critical Infrastructure

### New Government Mandates and Agency Standards

Between the Presidential Executive Order on Cybersecurity 14082, OMB-22-9 and emerging standards by NIST, CISA, NSA, DoD, and others, zero trust is now a national security priority.

### Identity as the Foundation for Zero Trust Architecture

To meet zero trust requirements and ensure that every connection is authenticated and encrypted with trusted digital identities, PKI sits at the foundation for modern security.

### Increasing Security and Supply Chain Risks

Cyber criminals, nation-state hackers, and even malicious insiders know that most agencies lack proper visibility and control over their PKI and machine identities, making them high-value and vulnerable targets.

# Challenges

### MODERNIZING INFRASTRUCTURE WITH ZERO TRUST

Government IT leaders are faced with the enormous challenge of modernizing decades-old legacy systems and accelerating the move to digital government, while maintaining tight controls around security. One of the primary drivers to ensure that cyber-security keeps pace with modernization is Executive Order (EO) OMB Memo-22-09, which outlines key requirements for government agencies to establish a zero-trust architecture (ZTA).

Enabling zero trust in a quickly expanding digital footprint brings with it the need to authenticate and authorize connections between thousands of devices, applications, workloads, and users – whether workforce, contractors, or even citizens. As a result, the rapid growth of machine identities has outpaced manual and homegrown management tools used by many federal agencies, leading to:

## Security and availability risks

Application and operations teams often request waivers or leave unmanaged keys unprotected on workstations and servers, making them easy targets for misuse or theft by attackers.

Without proper visibility, security teams struggle to maintain a complete and accurate inventory of their cryptographic assets. In addition to security risks, unknown or expired certificates often lead to disruptive, unplanned outages that bring down systems and applications.

## Slow, error-prone processes

Manual and error-prone certificate management processes are unable to keep pace with the volume or speed of certificate issuance as agencies start to adopt dynamic IT infrastructure such as cloud workloads, containers, and microservices.

## Outdated PKI systems

Legacy internal PKI systems and certificate authorities (CAs), such as Microsoft CA, are often difficult to manage and maintain, further complicated by the security skills shortage. Agencies need to simplify and consolidate their PKI to meet emerging use cases while reducing the overall complexity of their IT infrastructure.

# The Solution

### PKI AND MACHINE IDENTITY AUTOMATION

Together, Keyfactor Command and EJBCA Enterprise provide agencies with highly scalable certificate issuance, automation, and lifecycle management across their network and hybrid cloud infrastructure.

With EJBCA, the most widely adopted certificate authority (CA) software, security teams can set up a complete PKI platform to meet any certificate use case. Combined with Keyfactor Command, agencies have complete visibility of all keys and certificates, regardless of where they live, or which certificate authority (CA) they were issued from.

Security teams can proactively identify risks before they lead to outages or security incidents and enforce policies to ensure that every certificate is issued from a trusted and compliant CA. Meanwhile, application and operations teams can automate certificate provisioning and renewal processes to reduce risk and move faster.

# Benefits

- Simplify and consolidate PKI infrastructure across legacy and modern IT
- Eliminate certificate-related outages with automation
- Improve visibility and governance of cryptographic assets
- Remediate risks in the event of security vulnerabilities or CA compromise
- Accelerate cybersecurity modernization and zero-trust architecture (ZTA)

### ABOUT KEYFACTOR

Keyfactor is the machine and IoT identity platform for modern enterprises. The company helps security teams manage cryptography as critical infrastructure by simplifying PKI, automating certificate lifecycle management, and enabling crypto-agility at scale.

### CONTACT US


- www.keyfactor.com
- +1.216.785.2990