Keyfactor for U.S. Federal Government

Establishing digital trust and protecting critical infrastructure for government agencies with secure PKI, certificate management, and signing solutions.

Keyfactor's PKI and digital trust solutions enable 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. and across the globe, Keyfactor delivers post-quantum ready solutions with enhanced visibility, governance, and operational efficiency through automation.

With new government mandates and agency standards around post-quantum cryptography (PQC), zero trust architecture, and software supply chains, having a trusted partner for PKI and digital trust is essential to maintain compliance and ensure security.

PKI is Critical Infrastructure

Post-Quantum Cryptography (PQC) Preparedness

In 2022 HR 7535, the Quantum Computing Cybersecurity Preparedness Act, was signed into law, requiring all federal agencies to assess cryptographic assets and develop a PQC transition timeline. In 2024 NIST announced its first set of standards for PQC algorithms and subsequently deadlines related to the PQC transition, officially deprecating RSA, ECDSA, EdDSA, DH, and ECDH by 2030 and disallowing them after 2035.

Why Choose Keyfactor?

One solution stack

Natively integrated PKI, digital signing, certificate discovery, and lifecycle automation give you the power to meet any use case that comes your way.

Flexible deployment

Choose from a software appliance, hardware appliance, containers, SaaS-delivered, or a fully managed, single-tenant solution. Whether it's on-premises, in the cloud, or in a hybrid model, we can meet your unique needs.

Automation that Works

Automated PKI configuration, deployment, and certificate management to boost productivity and reduce manual processes. Or let us handle it for you with SaaS and managed options.

Trust and Compliance

Keyfactor actively maintains certifications with industry standards and regulations including Common Criteria/NIAP, ISO 27001, FedRAMP, SOC 2 Type II for hosted customers, and more.

Identity as the Foundation for Zero Trust Architecture

Between the Presidential Executive Order on Cybersecurity 14028, OMB M-22-09 and emerging standards by NIST, CISA, NSA, DoD, and others, zero trust is now a national security priority. 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 to provide identity to all NPE devices, workloads and things.

Increasing Security and Supply Chain Risks

As attackers deliver devastating supply chain attacks, agencies need to protect sensitive keys, enforce policy and governance, and sign sensitive documents and code to ensure the integrity and authenticity of their systems.

A secure centralized server-side certificate backed signing of code and software provides authenticity and integrity assurances to clients that the software has not been modified or tampered with throughout the supply chain.

Adopted by a Global Community

Keyfactor's solutions are widely adopted by a global community of thousands of developers and PKI practitioners, including 15+ U.S. Federal and international agencies.

Interoperability

Keyfactor's solutions are integrated with all major certificate authorities (CAs), HSMs, and cloud platforms. Popular protocols like ACME, EST, CMP, CMPv2, and many more are supported.

Quantum-Readiness

At Keyfactor we're at the cutting-edge of quantum readiness. Our customers are already one step ahead, with tools to discover and inventory assets, test NIST-selected PQC algorithms, and build a path towards migration.

6 Key Areas Keyfactor Partners with Government Agencies

Challenge	How Keyfactor Partners with Agencies
Preparing for Post-Quantum Cryptography (PQC)	Keyfactor is a technology partner and collaborator in the NIST Consortium for Quantum-readiness and is actively involved in the PQC transition with the National Cybersecurity Center of Excellence (NCCoE). Keyfactor has already implemented PQC support based on NIST standards across its solutions in its PKI, certificate lifecycle management (CLM), and signing solutions and will continue to deliver support as standards change. Keyfactor Command CLM offers extensive discovery capabilities for an accurate cryptographic inventory, a key first step and requirement of HR 7535 in the PQC transition.

Challenge	How Keyfactor Partners with Agencies
Modernizing Infrastructure with a Zero-Trust Architecture	Managing machine identities is critical to a zero trust architecture, a key requirement of Executive Order (EO) OMB Memo-22-09. 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 digital trust solutions offer full lifecycle control of identity to maintain control.
Ensuring Software Supply Chain Security	Keyfactor code signing solutions offer seamless CI/CD pipeline integration for easy deployment to complex environments. HSM-backed key protection with scalable key management provides centralized visibility and protection against key theft or abuse. Administrators can set up role-based access control, enforce policy guard-rails, and audit signing activities to ensure a comprehensive and secure software supply chain.
Meeting Government Standards and Security Certifications	• Keyfactor Command's Certificate Lifecycle Automation as a Service (CLAaaS) offering is FedRAMP "In-Process", demonstrating our commitment to federal agencies, and ensuring they can seamlessly discover, inventory, and automate certificate lifecycles • Keyfactor's EJBCA PKI Platform is Common Criteria certified in compliance with the National Information Assurance Partnership (NIAP) approved Protection Profile for Certification Authorities Version 2.1 and is listed on the Commercial Solutions for Classified (CSfC) Components List as able to operate a CA in classified environments • Keyfactor's PKI as a Service offering, which combines Keyfactor-managed PKI and CLAaaS, is SOC 2 Type II and ISO 26001 certified
Increased Workloads as Certificate Lifespans Shorten	With the shift to shortened public certificate TLS lifecycles of 45-90 days recommended by Google and Apple in the CA/Browser Forum, organizations need to prepare for increased workloads and move away from slow, error-prone processes. Keyfactor's certificate lifecycle automation capabilities include integrations with 100+ partners and can be deployed at scale in complex hybrid environments to reduce the likelihood of expensive and disruptive outages.
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. Many legacy CAs do not efficiently scale, lack key use cases, and have an unclear PQC roadmap. Agencies need to simplify and consolidate their PKI to meet emerging use cases while reducing the overall complexity of their IT infrastructure. Keyfactor's EJBCA PKI Platform is PQC-ready, meets any PKI use case, and offers flexibility of deployment from on-premises, to hybrid, to fully-managed PKIaaS.

Quantum-ready PKI

Ensuring the security of keys throughout their lifecycle starts with a trusted certificate authority (CA) and PKI platform. EJBCA is fast to deploy, offers flexible deployment options, scales on-demand, and supports any use case. EJBCA Enterprise offers high levels of security with Common Criteria certification through NIAP and is listed on the CSfC as able to operate a CA in classified environments.

Keyfactor EJBCA

Learn more ↗

End-to-end visibility and automation

Getting an accurate register starts with visibility. Establish an enterprise-wide inventory of all certificate authorities (CAs) and machine identities with Keyfactor Command. Easily take back control of your certificates and keys with automated workflows to reduce the likelihood of outages, misconfigurations, or expirations. Keyfactor CLAaaS is FedRAMP “In Process”, ensuring high security with the convenience of a managed cloud deployment.

Keyfactor Command

Learn more ↗

One-Stop PKI Solution

Keyfactor PKI as a Service combines a fully-managed PKI service and certificate lifecycle automation into a single, cloud-delivered platform. It’s your PKI, built and operated by experts, to reduce your operational burden, improve efficiency, and provide unmatched security and compliance. Keyfactor’s PKI as a Service offering is SOC 2 Type II and ISO 27001 certified.

Learn more ↗

Secure Signing

Protect the integrity of documents, code, containers, and software with secure signing as a service. Keyfactor Signum protects sensitive keys & documents, automates policy, and integrates with your native tools and build pipeline.

Keyfactor Signum

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 us on Linkedin.

Contact us

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