Keyfactor Signum

DATASHEET

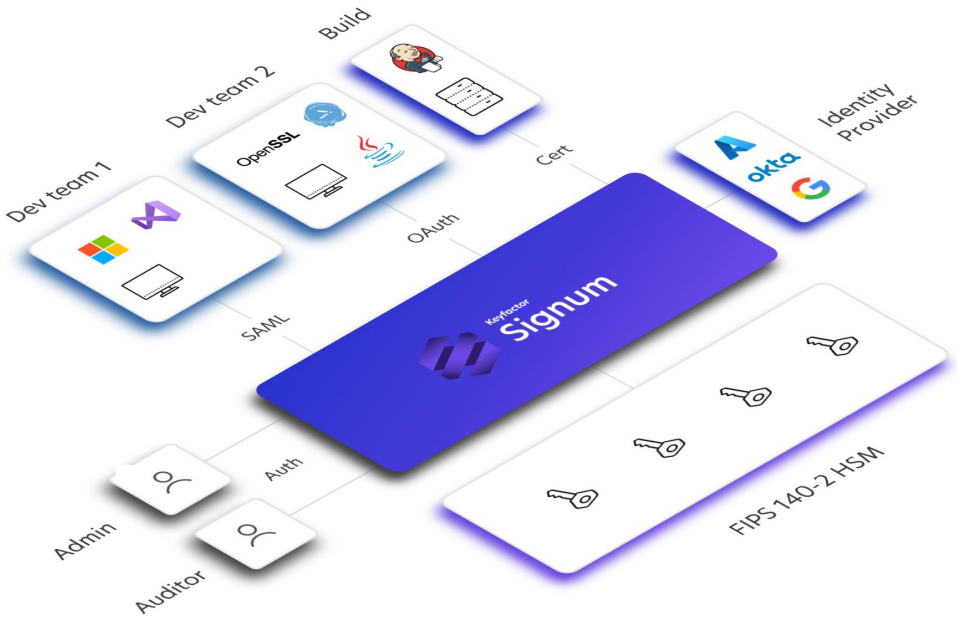
Secure digital signing, without the hassle.

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

Whether you build software applications, deploy scripts and containers, or deliver over-the-air (OTA) updates to connected IoT devices, code signing is a critical step to prevent malware spread and protect your business against malicious actors in the software supply chain.

However, insecure signing tools and processes leave many organizations vulnerable to attack. All too often, shortcuts result in private keys being stored on workstations, readme files, and build servers where they are susceptible to theft or misuse. Security teams struggle to manage signing keys, where they are stored, and who has access to them.

Keyfactor Signum helps security teams safeguard code signing processes with centralized key storage and policy enforcement from a single console, combined with lightweight agents to plugin to platform-native signing tools used in your development or IT environment. By integrating with existing tools, the platform makes it easy for IT teams and developers to sign code without friction, while the security team maintains control over key protection, access, and usage.



Use Cases:

- Protect IT infrastructure by signing and verifying scripts, macros, and internal applications
- Sign published software to protect your brand and your end-users
- Automate signing for artifacts, binaries, and builds in CI/CD environments
- Establish trusted and signed base images for containers and virtual machines (VMs)
- Enable secure over-the-air firmware updates for connected devices

Key Benefits:

- Protect sensitive code signing private keys against theft or misuse
- Maintain complete visibility of code signing activities across your environment
- Enforce signing policies to ensure only authorized users and machines can sign code
- Integrate easily with platform-native signing tools and build processes
- Prevent code tampering and unauthorized access to your signing infrastructure

Prevent unauthorized access, theft, and misuse

IT and application teams need quick, easy access to code signing keys to sign code, software, containers, and the like. However, disparate tools and remote development teams make it difficult for security teams to make keys accessible for developers, without exposing them to unauthorized access.

Keyfactor Signum ensures that sensitive code signing keys are generated and stored in a hardware security module (HSM), while making them accessible only to authorized users and machines for signing based on pre-configured policies.

Centralize visibility and policy management

With Keyfactor Signum, security teams have full control over user access and management, key and certificate access and usage policies, and certificate generation and storage from a centralized console. It also provides security teams with a detailed event log of all signing activities.

IT admins and developers can sign efficiently, while project owners can define who can access certificates, at what time and place, and which signing tools can be used. Policies can be assigned to specific certificates, users, and teams, ensuring proper usage and consistent compliance across the board.

Make signing effortless for your teams

Keyfactor Signum plugs directly into the code signing tools used in most development environments, making it easy to drop into build processes without requiring scripts or changes. Signing operations occur locally on the developer's workstation (interactive) or on a build server (automated), eliminating the need to transfer large executables over the network to a central signing service.

By delivering code signing as a service, the hassle of setting up infrastructure, managing disparate code signing keys, and handling continuous signing requests is eliminated. Security teams can work more efficiently and ensure that signing processes are compliant with best practices.

Key Features:

Key protection with HSM-backed code signing key generation and storage in a FIPS-certified HSM

Authentication via SAML, OAuth, or other methods ensures that users and machines are authenticated before signing or accessing the Signum platform

Granular policy controls allow security teams to define rules for certificate access and usage based on use cases and security requirements

PKCS11 & KSP interfaces integrate directly with signing tools such as SignTool, Jarsigner, Cosign, OpenSSL, and more to enable local signing

Event logs provide irrefutable records of code signing certificate access and usage for auditability

Centralized management for all code signing certificates, policies, approval workflows, reporting and auditing

SaaS platform makes deployment fast and simple, with a built in HSM and guaranteed SLAs for security and uptime

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.

For more information, visit www.keyfactor.com

Get Started

Ready to simplify and secure your code signing process?

Request a demo →