Keyfactor SignServer

DATASHEET

Sign anything, securely. Code and document signing.

SignServer Enterprise is a powerful and versatile serverside signing engine that securely signs software, firmware, containers, documents, and more.

Organizations rely on digital signatures to ensure customers can trust the software they deliver, protect the integrity of sensitive documents, ensure reliability of IT operations, and enable secure firmware and over-the-air updates.

However, manual processes, disparate tools, and unprotected code signing credentials leave many companies exposed to key theft and software supply chain attacks, which undermine the trust we place in digital signatures.

SignServer Enterprise automates and secures the signing process, whatever the use case, ensuring that teams can sign code and documents quickly and easily, with full auditability and protection of signing keys, including support for quantum-resilient signing. By leveraging client-side hashing, organizations can maximize performance and control, supporting even the most complex and large-scale environments.

Protect sensitive signing keys

With SignServer, private signing keys never leave secure, encrypted storage, even during signing. Different project members or systems can authenticate and share the same protected signing key, while providing a record of who signed what. Meanwhile, signature keys are generated and used for signing within an HSM, and all audit logs are signed for complete traceability.

Enable fast and secure signing

One instance of SignServer can host multiple use cases, signers, organizations, and users. The platform covers all your signing use cases, including standard document signing, code signing in multiple formats, time-stamping service, eIDAS advanced signing and seal, and ICAO ePassport signing.

Instead of managing a myriad of signing tools, using a central signing solution simplifies administration, improves security, and lowers costs. The platform makes it possible for security teams to maintain security and control, while developers and automated processes can sign code fast and without complexity.

Signing Use Cases:

- Secure IT infrastructure by signing internal scripts, executables, and apps.
- Automate signing for containers, software images and code in CI/CD pipelines.
- Ensure product integrity by signing and verifying firmware and OTA updates.
- Digitally sign legal or financial invoices, contracts, and other sensitive documents.
- Enable digital signatures for government-issued eIDs and ePassports.

Key Benefits:

- Provide InfoSec teams with visibility and granular control over signing permissions and audit logs.
- Integrate fast and secure signing with existing DevOps workflows and tools.
- Reduce the risk of unauthorized signing, shared or misused keys, or key theft.
- Simplify and consolidate all code and document signing into one platform.
- Scale on-demand to support high transaction workloads as new use cases arise.

Integrate with your tools and workflows

Delivering security while supporting the speed and agility of the teams that rely on digital signatures is key. SignServer integrates well with your document workflow engines, CI/CD pipeline tools, identity and authorization platforms, or any other business applications via standard interfaces and plugins. It also offers built-in support for various HSMs to generate and protect signing keys.

Supported technologies

Code signing:

- MS Authenticode:
  - Windows executable files
  - Windows installer files (.MSI)
  - PowerShell scripts
- Java code signing:
  - JAR signing
  - Android signing
- Plain signing
- CMS signing and time-stamping
- OpenPGP signing with client-side hashing
- Debian package signing

Document signing:

- PDF document processing with support for:
  - Different certification levels
  - Requesting and embedding time-stamp responses
  - Requesting and embedding CRL
  - Requesting and embedding OCSP responses
- PDF Advanced Electronic Signatures (PAdES-B, -T, -LT, -LTA)

ePassport Document signing:

- Machine Readable Travel Documents (MRTD) for ePassports
  - Configurable time sources
  - Monitoring of time-source status
  - EN 319 422 eIDAS compliant time-stamps

TSA/Time-stamp signing:

- RFC 3161, RFC 5816 and MS Authenticode
  - Configurable time sources
  - Monitoring of time-source status
  - EN 319 422 eIDAS compliant time-stamps

SignClient and APIs:

- SignClient application:
  - Command line tool
  - Client-side hashing for MS Authenticode and JAR signing
  - Simple built-in failover/load balancing
- API for custom implementation:
  - Signers and crypto tokens
  - Authentication and authorization
  - Transaction logging
  - Archiving

Hardware security modules:

- Thales Luna
- Entrust/nCipher
- Fortanix DSM
- Utimaco
- Other PKCS#11 modules

Algorithms:

- RSA, DSA, ECDSA and EdDSA keys
- Dilithium and SPHINCS+ NIST PQC candidates signing algorithms

Key Features:

One signing platform, supporting a wide range of signing formats, code binaries, DevOps tools, and algorithms.

High performance using client-side hashing, so developers can sign code fast without needing to upload or transmit large files.

Deployment flexibility with SignServer as a software or hardware appliance, cloud instance, container, or SaaS.

Simple certificate renewal via peer connector with EJBCA® Enterprise.

Maximum protection for signing keys via integration with various cloud-based and on-prem HSMs, or a built-in HSM.

On-demand scalability with support for failover and load balancing.

Granular controls, including two-factor authentication and authorization and detailed transaction logs.

Time-stamping with a built in Time Stamp Authority (TSA) for RFC 3161 and MS Authenticode timestamps.

CycloneDX Software Bill of Materials (SBOM) available with the SignServer container.

About 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 information, visit www.keyfactor.com

Get Started

Ready to modernize your Signing?

To get started with SignServer, contact Keyfactor via email sales@keyfactor.com or phone + 216-785-2946.