SignServer
PKI by PrimeKey

A versatile server-side application for **creating digital signatures**

Server side digital signatures give maximum control and security, allowing your staff and applications to conveniently sign code and documents. SignServer comes as our turn-key Appliance or as flexible software.

PrimeKey® by KEYFACTOR®

SignServer
PKI for Enterprises

SignServer Enterprise is a versatile server-side application for creating digital signatures and capable of performing complex cryptographic operations, even at very high loads. SignServer Enterprise is suitable for Trust Center environments.

Large Scale, Cryptographic Processing
SignServer Enterprise provides built-in modules for fully controlled, cryptographic processing, utilized for signing documents and code. Signing can be done large-scale, guaranteeing both availability and speed. One or several Hardware Security Modules (HSMs) can be integrated to secure signature keys.

Centralized and Auditable Digital Signatures
In large organizations, the digital signature keys for documents and code are commonly spread out in several places, using different security policies. However, from an audit and maintainability point of view, it is often convenient to centralize cryptographic operations. Using SignServer, all signature operations are brought into a single, auditable server, making security, control and audit a breeze.

Many Standards, One Solution
SignServer supports many standards for server-side document processing. After using SignServer in one area, it is fairly easy to add new modes of operations, thus avoiding costs of both additional hardware purchases, and training your personnel with new products.

SignServer can be deployed as:

- Time Stamp Authority (TSA), RFC#3161 and MS Authenticode
- Machine Readable Travel Documents (MRTD) signer, for ePassports
- PDF signer, including support for visible signatures, embedded CRLs and OCSPs Cryptographic Message Syntax signer (CMS, PKCS#7)
- MS Authenticode signer for executables, drivers, libraries and installers (MSI)
- Java code signer
- Android code signer

Designed for Flexibility and Integration
SignServer allows flexible integration possibilities, hiding the complexities of cryptography whenever possible. SignServer can be managed from a command line, a graphical user interface, or be integrated directly from your own application using Web Services. Several development APIs are ready to enable custom implementations.

Highlights

- Highly scaleable, providing for high transaction loads
- Transaction logging and archiving capabilities
- Supports leading hardware security modules (HSMs)
- Proven in practice for enterprise and national eID and ePassport installations
- Secure log & audit by using CC EAL4+ certified CESeCore library

New in SignServer

- Brand new web administration interface
- Support for:
  - Large files
  - Authenticode MSI signing
  - RFC 5816 time-stamps
  - ICAO deviation lists
- Client-side hashing with SignClient
- Certificate renewals from EJBCA Enterprise using peer connector
- Failover/loadbalancing in SignClient

Key Features

Lowest Total Cost of Ownership (TCO)
- Short project duration, with fast project deployment
- Least likelihood of disruptive software defects, due to mature, widely proven, open source code
- Least likelihood of material incidents, with PrimeKey's comprehensive services menu

High Security
- Two factor client authentication and authorization
- Detailed transaction logs
- Hardware security modules
- Service availability across maintenance windows

Flexibility
- Almost linear scalability and availability
- Configurable settings
- Integration interfaces, HTTP, WS, CLI
- Ability to customize or add new types of document processing

Technical specifications

PDF document processing, including support for visible signatures
- different certification levels
- requesting and embedding times-tamp responses
- requesting and embedding CRLs
- requesting and embedding OCSP responses
- PDF permissions
- Server-side archiving of signed documents to disk

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

ePassport Document Signer (MRTD)
- LDS version 1.8 support
- Support for limiting the number of signings (i.e. ICAO limits up to 100,000 signatures)
- Support for key usage period
- Multiple active logical signers with fail-over when the sign limit is exceeded
- Deviation lists
- Master lists

Cryptographic Message Syntax signer
(CMS, PKCS#7)
- Support for encapsulated content or detached signatures
- Support for client-side hashing possible for detached signatures

XML signing and validation
- XAdES-BES and XAdES-T

MS Authenticode signer
- Portable Executable files
- Windows installer files

JAR Signer
- Java code and Android apps

SignClient Application
- Command line tool
- Client-side hashing for Authenticode and JAR signing
- Simple built-in failover/load balancing support

API for custom implementations of:
- Signers and Crypto tokens
- Authentication/authorization
- Transaction logging
- Archiving

Hardware security modules
- SafeNet, Thales, Utimaco, AEP
- other PKCS#11-compliant modules

Cryptography support
- RSA, DSA and ECDSA keys

Enabling Software Stack
- 64-bit Linux operating system recommended
- JBoss EAP/WildFly application server
- MySQL/MariaDB, PostgreSQL, Oracle database

Integration with EJBCA Enterprise
- Automatic certificate renewal service using EJBCA Enterprise Web Services
- One click certificate renewal from within EJBCA Enterprise using peer connector

About PrimeKey

PrimeKey Solutions AB is one of the world's leading companies for PKI solutions. PrimeKey has developed successful solutions, such as EJBCA Enterprise, SignServer Enterprise and PrimeKey PKI Appliance. PrimeKey is a pioneer in open source security software that provides businesses and organisations around the world with the ability to implement security solutions such as e-ID, e-Passports, authentication, digital signatures, unified digital identities and validation. PrimeKey has its head office in Stockholm, Sweden. As of June 2021, PrimeKey is a part of Keyfactor.

sales@primekey.com
+46 873 561 01

www.primekey.com

PrimeKey® by KEYFACTOR®