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®

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)
- ePassports signer (MRTD)
- PDF signer
- Cryptographic Message Syntax signer (CMS, PKCS#7)
- MS Authenticode signer for executables, drivers, libraries and installers (MSI)
- Java and Android code signer
- PGP code signer
- Debian package signer
- DNSSEC 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 scalable, 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 based on CC EAL4+ certified CESeCore library

Use Cases

- Secure supply chain and device lifecycle management with code signing
- Flexible product licensing with signed license files
- eIDAS qualified Time Stamping Services
- Travel Documents/ePassports solutions
- PDF signing and integration with workflow engines

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 signing, including support for visible signatures
- Different certification levels
- Requesting and embedding time-stamp responses, CRLs and 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 / Machine Readable Travel Document (MRTD)
- LDS version 1.8 support
- Key usage counter (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 and Master Lists

Cryptographic Message Syntax signer support for
(CMS, PKCS#7)
- Encapsulated content or detached signatures
- Client-side hashing possible for detached signatures
- Requesting and embedding time-stamp responses

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

PGP Signer
- Generic clear-text and detached signatures
- Debian package signing

DNSSEC Signer
- Zone file signing

MS Authenticode signer
- Portable Executable files
- Windows installer files
- Universal Windows Platform apps (APPX)

JAR Signer
- Java code and Android apps

SignClient Application
- Command line tool
- Client-side hashing for Authenticode, JAR, PGP and Debian package 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
- ther 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 is one of the world's leading PKI solutions providers and has developed a number of innovative products, including EJBCA Enterprise, SignServer Enterprise, EJBCA Appliance, PrimeKey SEE, and Identity Authority Manager. As a pioneer in open-source security software, PrimeKey provides global businesses and organizations the ability to implement vital security solutions, such as e-ID, e-Passports, authentication, digital signatures, unified digital identities, and validation. PrimeKey products are Common Criteria and FIPS-certified, the company's internal processes are ISO 9001, 14001, and 27001 certified, and it has numerous Webtrust/ETSI and eIDAS-audited installations.

PrimeKey has offices in Stockholm, Sweden; Aachen, Germany; San Mateo, USA; and Melbourne, Australia. Together with a global network of technology and reselling partners, the company supports a customer roster that includes industry-leading companies and institutions across the IT, telecommunications, industry, finance and public sectors.

Contact
sales@primekey.com
www.primekey.com
Europe: +46 873 561 00
USA: +1 (855) 583-7971

PrimeKey Headquarters
Sundbybergsvägen 1
SE-171 73 Solna
Sweden

PrimeKey Labs
Krantzstr. 7
52070 Aachen
Germany

C2 – A PrimeKey company
951 Mariners Island Blvd
San Mateo, CA 94404
USA

Crypto Workshop – A PrimeKey company
520 Bourke Street, Level 2
Melbourne, VIC 3000
Australia

PrimeKey®