



EJBCA

PKI for enterprises

Open standards compliance, performance, scalability and robustness, are the hallmarks of PrimeKey's PKI implementation - EJBCA - the most widely used open-source enterprise PKI.

The best choice for enterprise PKI implementation

Large organizations regularly select the PrimeKey Solutions AB PKI, -- EJBCA -- to provide their enterprise, mission-critical PKI infrastructure. A reason for preferring PrimeKey's EJBCA is cost reduction. With the EJBCA Certificate Management System, organizations can manage several PKI hierarchies efficiently.

Open Standards, Open Source, Professional Support

Open standards in PrimeKey's EJBCA and open-source code work together with PrimeKey strategic services. Open standards and open source contribute maturity to PKI security while PrimeKey strategic services protect your brand throughout the lifetime of a mission-critical service.

To reduce downtime and maximize profitability, PrimeKey strategic services for enterprises combine big-picture asset protection and protection of your customers with world-class traditional support and assistance, starting with project planning and continuing throughout the life cycle of the envisioned capability.

Designed for Flexibility and Industrial Strength

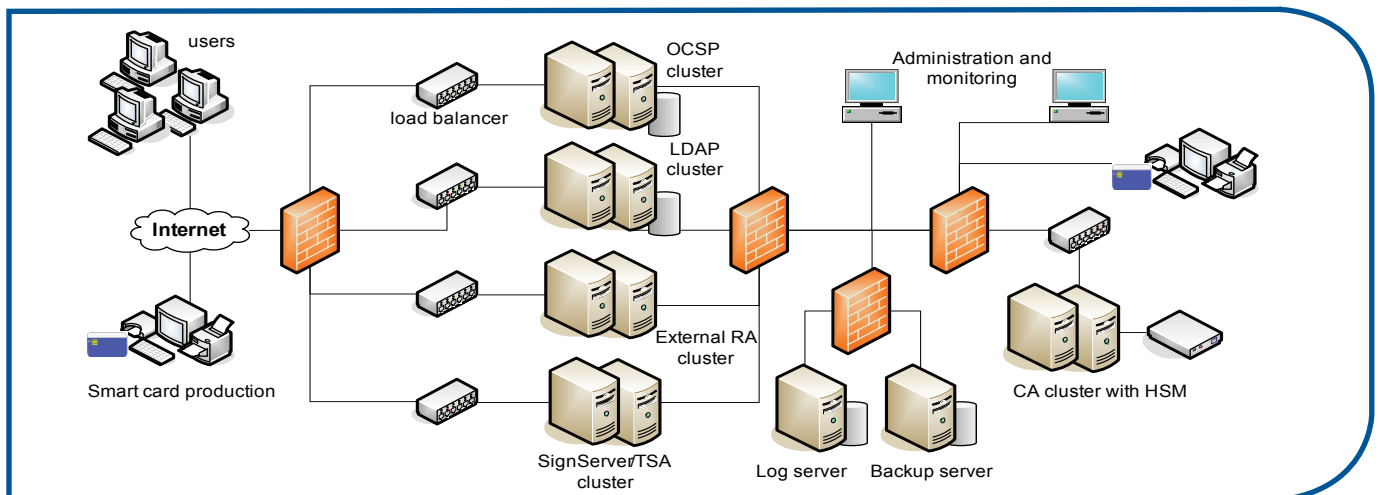
EJBCA is by design created to allow flexible integration possibilities, making possible almost transparent PKI implementations - whenever feasible, the complexities of cryptography are hidden for the end user. Another important aspect of the EJBCA design is its robustness - capability to serve millions of users, in high availability environments.

EJBCA in practice

There are many ways how a PKI can be implemented, depending on particular needs within an organization. The picture below gives an overview of an implementation with users on Internet accessing diverse services through a set of firewalls. For large-scale implementations, there are load balancers in front of clustered OSCP, LDAP, external RA or SignServer/TSA services. The log and backup servers keep track of activities. The CA cluster is normally equipped with a HSM for security reasons.

Highlights

- Full PKI standards compliance
- Supports all major PKI algorithms and protocols
- Manages millions of certificates under high transaction loads
- Supports leading hardware security modules (HSMs)
- Proven in practice for enterprise and national ID installations
- Prevents vendor lock-in
- Designed for Common Criteria certification



Key Features

Lowest Total Cost of Ownership (TCO)

- Zero software-license fee; Zero per-use fee; and Zero vendor lock-in
- Most-useful, most RESTful API, with WS
- Short project duration, with fast project deployment
- Simplest usage tracking
- Least volatility in operations, due to EJBCA's designs for Common Criteria EAL4+ certification
- Least likelihood of disruptive software defects, due to mature, widely proven source code
- Least likelihood of material incidents, with PrimeKey comprehensive strategic services menu
- Most personal, site-specific response mapping to each enterprise customer

High Security

- Detailed audit and transaction logs
- Role-based authorization
- Hardware security modules
- Designed for Common Criteria EAL4+ certification
- Scalability and Reliability
- Service availability across maintenance windows
- Scalability and availability using clusters

Flexibility

- Configurable profiles
- Integration interfaces
- Standard SQL database

Audit Compliance

- ETSI/CWA-compliant and WebTrust-compliant references

Technical specifications

Supported Standards

- X.509 and RFC5280 Certificates and CRLs
- ICAO 9303 and EAC 1.11 ePassport certificates
- PKCS#10, CRMF and SPKAC certificate requests
- PKCS#12, JKS, PEM and PKCS#11 keystores

Protocols

- LDAP application protocol
- CMP and OCSP Internet protocols
- SCEP Internet Draft
- HTTP transport protocol
- Web-service protocols: <List of pky supported>

Hardware security modules

- SafeNet
- nCipher
- Utimaco
- AEP
- other PKCS#11-compliant modules.

Cryptography support

- RSA, DSA and ECDSA keys
- SHA-1 and SHA-2 hash algorithms.

Enabling Software Stack

- 32- or 64-bit Linux operating system recommended
- Oracle's JDK 7 or OpenJDK 6
- JBoss application server
- MySQL, PostgreSQL, Oracle, DB2, Ingres.

About PrimeKey

World leading open source PKI (Public Key Infrastructure) company, founder and commercial force behind EJBCA and SignServer - the most downloaded open source PKI project.

PrimeKey's enterprise class integration, dedication to open standards, training and support services, help customers achieve their organizational goals.