EJBCA Enterprise
PKI by PrimeKey

A powerful and flexible way to **issue, manage and maintain digital certificates**

EJBCA is arguably the most used Certificate Issuance and Management System in the world. With proven industrial strength and scalability in enterprises and governments alike, EJBCA is a de-facto choice for serious PKI.

PrimeKey

SECURE METRIC *TECHNOLOGY*

EJBCA
PKI for Enterprises

A powerful and flexible Certificate Authority (CA) and Public Key Infrastructure (PKI) Management system to issue, manage and maintain digital certificates; enabling secure and encrypted communication whatever the use case.

The best choice for enterprise PKI implementation
Built on open standards and an open source platform, EJBCA Enterprise brings the maturity and transparency required for any security focused PKI solution. It's designed for robustness and security, and follows best practice Common Criteria EAL4+ security evaluation standards. EJBCA Enterprise has been proven time and again both in high security governmental applications as well as in various applications and industries in the private sector.

Designed for flexibility and industrial strength
The inherent design of EJBCA opens up for a multipurpose PKI solution which is highly scalable, and enables management of several parallel PKI hierarchies within the same deployment. EJBCA relies on widely used standard protocols enabling support for many different platforms, environments, and use cases. Supporting issuance of both machine-, device-, and personal certificates, EJBCA can be used for securing anything from digital and physical resource access to ensuring privacy and encryption in all kinds of communications.

Simplicity is the key
All security environments have different demands, different requirements for structure, and will need to adhere to different sets of organizational policies. For this reason, EJBCA enables flexible integration with most 3rd party and PKI dependent systems, and will fit in to any PKI environment, regardless of the level of customization. EJBCA offers full blown support for high level and complex cryptographic operations, without requiring the administrators to be cryptology experts. Managed through a web-based graphical user interface EJBCA's easy operation will simplify all aspects of PKI management.

EJBCA in practice
EJBCA will provide the backbone of all your digital security needs while saving your time, minimizing your costs and reducing your downtime. As it secures your mission-critical services, EJBCA will help to protect your brand, assets, and reputation. The robustness of EJBCA provides the capability of serving both smallscale but also larger implementations with millions of users in high availability environments without compromising on security.

Highlights

- Supports all major PKI algorithms and protocols
- Manages billions of certificates under high transaction loads
- Proven in practice for enterprise and national e-ID installations
- Supports WebTrust, ETSI/eIDAS and PIV Certificates

Recent Tech Updates

- CA/B-Forum and Chrome Requirements, incl. CAA and Certificate Transparency
- EJBCA RA, a secure proxy for the CA
- CWA/ETSI compliant
- Support for ACME, EST, CMP and SCEP
- RESTful and SOAP APIs
- A dynamic and powerful approvals system
- Increased support to simplify audit

Tomas Gustavsson is the CTO of PrimeKey and the founder of EJBCA, the most used PKI in the world.

Key Features

Technical specifications

Lowest Total Cost of Ownership (TCO)
- Short project duration, with fast project deployment
- Least volatility in operations, thanks to EJBCA's design for Common Criteria EAL4+ certification
- Least likelihood of disruptive software defects, due to mature, widelyproven source code
- Least likelihood of material incidents, with PrimeKey comprehensive strategic engineering services

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

Flexibility
- Configurable profiles
- Integration interfaces
- Supports most major databases

Audit Compliance
- ETSI/eIDAS- and WebTrust compliant references

Supported Standards
- RFC5280 compliant X.509 certificates and CRLs
- ICAO 9303, EAC 1.11 and EAC 2.10 ePassport and eID certificates
- PKCS#10, CRMF and SPKAC certificate requests
- PKCS#12, JKS, PEM and PKCS #11keystores
- EN 319 412 eIDAS compliant certificates
- Payment Service Directive 2 (PSD2) ETSI TS 119495 Section 4

Protocols
- LDAP application protocol
- Full OCSP support
- ACME, CMP, EST and SCEP enrollment/management protocols
- HTTP transport protocol
- 3GPP, i.e. LTE/4G compatible

Hardware Security Modules supported
- SafeNet
- nCipher
- Utimaco
- AEP
- other PKCS#11-compliant modules

Cryptography support
- RSA, DSA and ECDSA keys
- NSA SUITE B compliant