

Facts that every IT-security professional needs to know about



WHAT

What is EJBCA?

EJBCA is a J2EE-based implementation of an X509 Certificate Authority. It is full featured, it has proven industrial strength, it is used world-wide and it is open source.

What does the name EJBCA stands for?

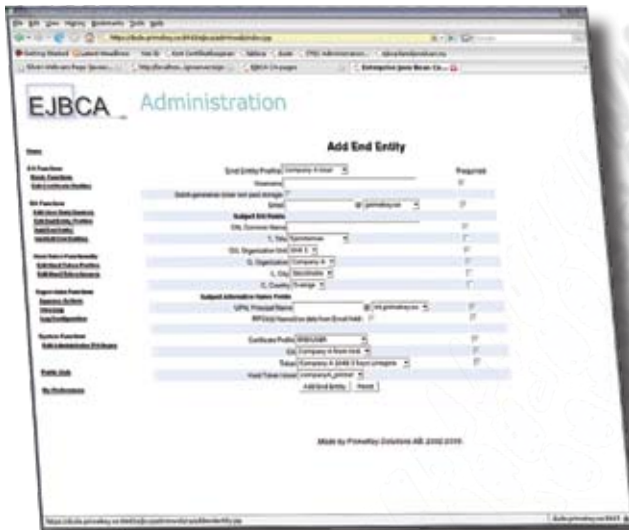
EJBCA stands for Enterprise Java Beans Certificate Authority.

What are the license costs?

Nothing. There are no license costs with EJBCA.

What Is the primary purpose of EJBCA?

EJBCA is an enterprise class PKI, meaning that you can use EJBCA to build and manage a complete PKI infrastructure for your organization. If you only want to issue a few single certificates for testing, there are probably options that will get you started quicker, but if you want a serious PKI we recommend EJBCA.



WHO

Who is behind EJBCA?

PrimeKey Solutions AB, a Swedish IT-security company with niched competence in information and system security and product development within Public Key Infrastructure (PKI) and smart card appliances. PrimeKey Solutions AB is the originator, main contributor and administrator of EJBCA at SourceForge.net.

Who provides support, training and professional services?

You may choose to do the complete planning, installation and maintenance done internally by your organization or you may choose to get support, training and other professional services, "EJBCA Subscription", from PrimeKey Solutions AB or some of the "EJBCA Certified Partners".

WHY

Why should you use EJBCA?

There are several reasons. Chances are that you want flexible yet robust PKI, you want it to be able to follow the workflow of your organization, and you want it to keep up with technical advances and industry standards. You may want your PKI to have support for leading hardware security modules as well as smart cards; you want it to run on your platform of choice. In addition to human users, you may want to issue digital certificates to applications or hardware devices. You want to have clear understanding when and how you get the return of your investments in the certificate infrastructure. Also, you may wish to be able to inspect the source code.

WHERE

Where can I find more information about EJBCA?

We recommend you to visit the *official* EJBCA web page at www.ejbca.org. There you can take a look at some of the references, access technical documentation and other resources.

Where can I download EJBCA?

You can download EJBCA either by following links from the official site, or go directly to <http://sourceforge.net/projects/ejbca/>

Where is the feature list?

The complete and the most current feature list is always available at the official site.

- EJBCA runs standalone or integrated in a J2EE application, operating one or several complete infrastructures, with diverse available topologies (all-in-one, clustered), with external RA and/or external OCSP, etc.
- Follows X509 and PKIX (RFC3280) standards where applicable; CRL and CRLDistribution Points according to RFC3280. Support for SCEP, EU/ETSI qualified certificates (RFC3739), OCSP (RFC2560); CMP (RFC4210 and RFC4211), synchronous XKMS version 2 requests.
- Certificate signing with either RSA (keys up to 4096 bits) or ECDSA with named curves or implicitlyCA.
- Modular API for HSMs with built in support for nCipher HSMs, Eracom, SafeNet Luna, Utimaco CryptoServer, PrimeCardHSM.
- Individual enrollment trough browsers or batch production of certificates. Enrollment generating complete OpenVPN installers for VPN users, or for other applications through open API.
- Certificate export as PKCS12, JKS or PEM.
- Certificates and CRLs are stored in a SQL database, LDAP/ActiveDirectory and/or other custom data source.
- Web based administration GUI with strong authentication, available in several languages. Command line administration for scripts etc.
- Multiple kinds of administrators with specified privileges and user groups.
- Configurable certificate profiles for different types and contents of certificates.
- Configurable entity profiles for different types of users.

WHEN

When did the EJBCA project start at SourceForge and when was the latest release?

EJBCA started in december 2001. The current version is 3.4, released in January 2007.

When will you implement feature X?

If the feature is not supported yet, please check the development roadmap for EJBCA - chances are that the desired feature is in the roadmap. If your organization is willing to sponsor development of some particular feature, then we can diverge from the roadmap and put it on fast track.

HOW

How does EJBCA work in practice?

There are many ways how 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 trough a set of firewalls. For large-scale implementations, there are load balancers in front of clustered OCSP, 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. Please visit us at www.primekey.se for more information.

