EBOOK

The Complete Guide:

When to use EJBCA Enterprise vs open-source CA software

A comparison between EJBCA Community and EJBCA Enterprise

Table of Contents

Cybersecurity is about community 3

EJBCA Community vs EJBCA Enterprise 4

When to choose EJBCA Enterprise 5

Technical specifications: EJBCA Community vs Enterprise 8

An easy path to enterprise PKI 9

What we'll cover in this eBook

EJBCA is a complete public key infrastructure (PKI) solution that helps teams to set up a flexible and scalable PKI architecture within minutes. Built as an open-source project, EJBCA is the most widely used and trusted certificate authority (CA) software in the market today.

In this eBook, you will learn how open source benefits all EJBCA users, what the differences are between EJBCA Community and Enterprise, when to choose EJBCA Enterprise, and how to upgrade from EJBCA Community to EJBCA Enterprise.

Cybersecurity is about community

Today we live in a world where everything is connected, and we have never had a more open, free, and innovative society. Now more than ever, our digital footprints are growing exponentially, and we need to take action to preserve our privacy and security. That responsibility rests on the collective IT and security community.

Cybersecurity is not a competition, it is a community-driven effort to defend against data breaches, hacks and identity theft. Keyfactor envisions an Internet that is safe for everyone – where every transaction between users, machines, devices, and applications is trusted and secure. Trust is built on openness and transparency, and at Keyfactor, we've built open-source solutions to establish digital trust everywhere.

EJBCA: A proven and flexible PKI solution

EJBCA is one of the longest running CA software projects, with more than 2,000+ downloads each month by developers, product teams, manufacturers, and the like. The solution is platform agnostic and multi-tenant, so it can easily scale to match the needs of your PKI environment, whether you're setting up a national electronic identity (eID), securing industrial IoT devices, or managing your own internal PKI.

EJBCA is available in a free open-source edition, known as EJBCA Community, as well as a Common Criteria-certified Enterprise edition that offers more flexible deployment, scalability, and extensibility required for modern large-scale PKI deployments.

> "PrimeKey [which is now part of Keyfactor] bases its enterprise offering on the open-source EJBCA platform. This very commonly used PKI provides deep integrations, and it meets many advanced PKI requirements. Access to the source code helps protect organizations from any potential abandonment of the software and facilitates the perpetuity of the CA."
>
> Gartner "Solution Comparison for PKI and Certificate Management Tools", 2021

EJBCA Community vs EJBCA Enterprise

Whether you're a community user or an enterprise customer, EJBCA offers a strong foundation for PKI in the enterprise. If you're looking to learn foundational PKI components without the need for certifications, service level agreements (SLAs), and enterprise-level functionality, then the free and open-source EJBCA Community might just be the perfect fit.

However, if you're looking for an enterprise-grade PKI, EJBCA Enterprise is the better choice, offering more advanced features and functionality, such as:

- **Secure segmentation of PKI components**, keeping CA, registration authority (RA), and validation authority (VA) on separate instances
- **Enterprise security features**, such as signed audit logs, tools to import and export configurations and OAuth authentication
- **Compliance with security regulations**, such as Common Criteria, eIDAS (electronic IDentification, Authentication and trust Services), or ICAO (International Civil Aviation Organization) 9303
- **A trusted security partner** with extensive experience and solid expertise in PKI and cryptography
- **Flexible deployment**, such as cloud solutions and on-premises software and hardware appliances
- **Use cases that require Enterprise PKI**, for example issuing certificates to ePassports, securing mobile networks, and enabling DevSecOps

At a glance: EJBCA Community vs EJBCA Enterprise

Features and services	EJBCA Community	EJBCA Enterprise
Core PKI Functionality	Yes	Yes
Advanced PKI Functionality – see Technical Specification below	No	Yes
Compliance to certifications and regulations	Not guaranteed	Yes
Community edition support (best effort)	Yes	No
Professional support with SLA	No	Yes
Access to Keyfactor's professional services	No	Yes
Basic online training and tutorials	Yes	Yes
Comprehensive product training; lectures and hands-on exercises	No	Yes
Scheduled releases	Yes	Yes
Maintenance and security releases	Not guaranteed	Yes
Advance notice and hotfixes	No	Yes

When to choose EJBCA Enterprise

In this section, we'll explore five reasons why teams and organizations choose EJBCA Enterprise vs open-source CA software, such as EJBCA Community.

High availability and secure segmentation

For a secure PKI deployment, issuing CAs should only run on a protected network behind a firewall, whereas the RA and VA must reside in lower security domains to be accessible to clients. This way, even if hackers would be able to take over the DMZ, they can't do much harm to the PKI, as the CA is in a protected environment.

With EJBCA Enterprise, customers can securely segment the PKI components, keeping the RA and VA on separate instances in the DMZ while communicating with the CA over mutually authenticated TLS. This secure segmentation is implemented with the help of the peer systems protocol in EJBCA Enterprise.

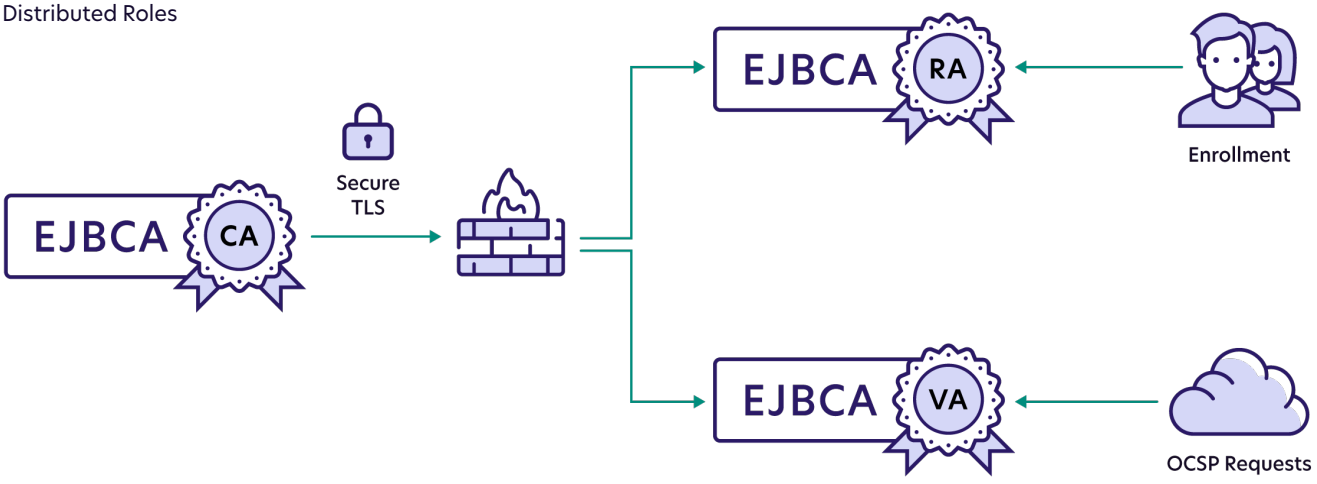
Component segmentation also enables secure hybrid deployments, for example with the RA and VA in the cloud and CA on-premises, as well as VA and RA redundancy for high availability settings.

Redundancy is needed for any PKI with high availability requirements over different geographical regions, or a sizeable scale of certificate and validation requests, to ensure that the failure of a single instance does not result in downtime. Redundancy for VAs and RAs is usually achieved using multiple standalone instances with the help of the peer systems protocol. For CAs, redundancy is mainly achieved using database clustering.

EJBCA Enterprise has for the past two decades been proven in large-scale production environments within IoT, enterprises, and government organizations.

EJBCA Architecture

Distributed Roles



Example EJBCA architecture with secure segmentation of CA, RA and VA over TLS

Security requirements

An open-source foundation ensures trust and transparency, but many enterprise organizations require advanced features to ensure their PKI is robust and secure. EJBCA Enterprise offers several security features to support these requirements.

Signed and integrity-protected audit logs that are available with EJBCA Enterprise ensure that log entries can't be edited or removed to hide signs of wrongdoing.

The EJBCA ConfigDump tool provided with EJBCA Enterprise allows you to export and import configurations, to facilitate mass deployments. The export is useful for auditing purposes and to compare configuration changes made in EJBCA. With the import functionality, you can easily import a complete configuration, to make sure that all your instances have the same settings, while minimizing the risk of human errors.

EJBCA Enterprise also comes with OAuth authentication, allowing for seamless integration into existing company identities and "one identity" policies. OAuth authentication can be used alongside or instead of client certificate authentication and provides a powerful tool for managing all users of a PKI from one single source.

Compliance with regulatory requirements

PKI deployments are increasingly under scrutiny by internal security teams and external auditors. As EJBCA Enterprise is Common Criteria-certified and offers additional security features like signed audit logs and role-based authorization, it provides an additional level of assurance and simplifies audits.

Keyfactor has numerous Webtrust/ETSI and eIDAS audited installations, and our internal processes are ISO 9001, 14001, and 27001 certified. Our PKI solutions help customers issue ePassports and eIDs in compliance with the ICAO 9303 and Extended Access Control (EAC) specifications, as well as stay compliant with standards and regulations such as NIS2, CSfC, FIPS, PSD2, CAB Forum, and GDPR.

Trusted expertise and partnership

PKI is critical security infrastructure to protect enterprise IT environments, connected IoT devices, smart manufacturing and industrial IoT, but getting it right can be complex. Finding and retaining the right expertise, adherence to industry standards, and the ongoing maintenance of CA and HSM infrastructure are all common challenges.

Enterprise customers benefit from a trusted security partner with a long history in PKI and cybersecurity. Our professional services team guides users through every step of the implementation process, from installation to configuration, testing and production deployment of your PKI system.

Product training is also provided throughout the project to ensure a smooth deployment and alignment with best practices. Our support and maintenance also includes continuous software updates and allows you to maintain a high level of security and agility throughout your PKI project.

With our expertise in PKI and cryptography, you can be sure that as technology advances, we help you stay up to date with the latest protocols and algorithms – and stay crypto-agile.

Flexible deployment

To account for the unique business challenges of your organization, including security, budget and the availability of internal resources, EJBCA Enterprise offers a combination of deployment options to suit your needs today and allow you to grow flexibly over time.


Software Appliance


Hardware Appliance


EJBCA Cloud


EJBCA Software as a Service


Hybrid

With EJBCA Enterprise, the PKI deployment can be adapted to your organization and use case instead of the other way around. An EJBCA PKI can be deployed as a turn-key software or hardware appliance, on AWS or Azure cloud, or as a SaaS-delivered PKI. And if you need a combination of on-premises and cloud, we can help you set up a hybrid solution.

Enterprise use cases

The use of PKI in certain industries and sectors requires a high level of security and very specific setups and installations. For example, if you need to produce and handle ePassports and eIDs, securely and in compliance with EAC, you'll need the ePassport solution that is provided with EJBCA Enterprise.

In enterprise IT environments, the Microsoft Intune and auto-enrollment support in EJBCA Enterprise allows you to overcome the limitations of the Active Directory Certificate Services (ADCS) PKI and still seamlessly integrate into your Microsoft infrastructure. A single instance of EJBCA can provide PKI services to all your Microsoft servers, workstations, and mobile devices, as well as non-Microsoft infrastructure and integration with DevOps toolchains.

With EJBCA Enterprise, mobile operators can securely manage their LTE/4G mobile networks using 3GPP-compliant PKI, using CMPv2 with multiple vendor CAs and vendor certificate authentication.

Technical specifications

Let's dive deeper into the functional differences between EJBCA Community and EJBCA Enterprise. Here you'll find key features that support flexibility, security, specific use cases, and integrations via APIs and protocols.

General features	Community	Enterprise
X.509 certificate issuance and management	Yes	Yes
Basic HSM support using Java PKCS#11	Yes	Yes
Advanced HSM support (e.g. EdDSA, AWS CloudHSM, AWS KMS)	No	Yes
Certificate transparency	No	Yes
PKI configuration import/export functions ConfigDump and StateDump	No	Yes
Cert Safe Publishing to HTTPS server	No	Yes
Security features		
Component separation with peer connectors, for example to have RA or VA on a separate instance	No	Yes
Database integrity protection – wards against database tampering via signing database tables by row	No	Yes
Pre-issuance key validation – allows the CA to refuse to sign known weak keys or detect policy violations before issuance	No	Yes
Audit logging to file or database	Yes	Yes
Integrity-protected audit log in database	No	Yes
OAuth authentication	No	Yes
Use cases		
ePassport (EAC) certificate issuance and management	No	Yes
Microsoft Auto-enrollment support for managing Microsoft servers and devices	No	Yes
LTE/4G mobile network security using CMP 3GPP	No	Yes
IoT device security using EST protocol	No	Yes
Enrollment protocols and APIs		
CMP	Yes	Yes
CMP 3GPP Vendor Mode	No	Yes
SCEP Client mode	Yes	Yes
SCEP RA Mode	No	Yes
EST	No	Yes
ACME	No	Yes
SOAP API	Yes	Yes
Enrollment REST API	Yes	Yes
Management REST API	No	Yes

For more details, see EJBCA Interoperability and Certifications in our online documentation.

An easy path to enterprise PKI

If you think EJBCA Enterprise is right for your team or organization, Keyfactor offers a simple path for you to try it out or go ahead and migrate from another CA.

Try EJBCA Cloud

Ready to put EJBCA Enterprise to the test? Getting started is simple with a 30-day free trial of EJBCA Cloud in the AWS or Azure marketplace. Our available how-to videos and self-service documentation make it easy to get up and running with a cloud PKI.

Try EJBCA Cloud on AWS | Try EJBCA Cloud on Azure

Explore deployment options

If you're ready to run with EJBCA Enterprise, Keyfactor offers multiple flexible deployment options to meet your specific use cases and architectural requirements. For example, you might need a hardware appliance for your manufacturing facility or security-critical use cases, a cloud PKI for your IoT or DevOps use cases, or a hybrid solution to cover all your PKI needs.

Deployment Options | Software | Hardware | Cloud | SaaS

Get started with EJBCA Enterprise

If you're already using EJBCA Community and you're considering an upgrade, the path to enterprise PKI is easier than you think. Our professional services team has worked with many customers to migrate from Community to Enterprise as they scale. If you're ready to get started with EJBCA Enterprise, contact our team today.

Contact Us

KEYFACTOR

Keyfactor is the machine and IoT identity platform for modern enterprises. The company helps security teams manage cryptography as critical infrastructure by simplifying PKI, automating certificate lifecycle management, and enabling crypto-agility at scale.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook.

Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

Contact Us

- www.keyfactor.com
- +1.216.785.2946