

Updated on 05/26/2026

Sign up

Enterprise JavaBeans Certificate Authority Training

2 days (14 hours)

Overview

The Enterprise JavaBeans Certificate Authority training teaches you how to set up an EJB-based certificate authority to manage identities, certificates, and keys in an IT system. You will secure the issuance, renewal, and revocation of certificates for TLS, application authentication, and digital signing.

During this course, you will build a fully operational CA, from architecture to PKI workflows, while incorporating operational constraints: certificate policies, profiles, role management, and auditing. The approach emphasizes configuration, secret security, and operational traceability.

The training is hands-on: guided workshops, issuance and revocation demos, and troubleshooting common errors (chains, CRL/OCSP, keystores). You'll leave with deployment scripts, profile templates, and an operational checklist to scale up in a test environment and then in production.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Install and configure an EJB CA and its components.
- Define certificate policies and profiles tailored to specific use cases.
- Issue, renew, and revoke certificates with traceability.
- Set up CRL and OCSP and validate certificate chains.
- Secure keys (keystores/HSM), roles, and administrative access.

Target Audience

- Java / Jakarta EE developers
- Security / PKI engineers
- System and middleware administrators
- DevOps responsible for certificate management

Prerequisites

- Solid foundation in Java and basic knowledge of Jakarta EE
- Understanding of TLS, X.509 certificates, and trust chains
- Experience with the command line and keystores (JKS/PKCS12)
- Basic network knowledge: DNS, ports, proxy

Technical prerequisites

- 64-bit machine with at least 8 GB of RAM (16 GB recommended)
- Linux, macOS, or Windows with WSL2
- JDK LTS, Jakarta EE-compatible application server
- Tools: OpenSSL, HTTP client, code editor, Git

Curriculum for our Enterprise JavaBeans Certificate Authority training

[Day 1 - Morning]

EJB Fundamentals and PKI Architecture

- Jakarta EE review: container, injection, transactions, and security
- EJB: Stateless/Stateful/Singleton, timers, and design best practices
- PKI: Root CA, Intermediate CA, and RA roles; certificate lifecycle
- CA Workflow: CSR, Issuance, Renewal, Revocation, Publication
- Hands-on workshop: Setting up a Jakarta EE project and modeling the certificate issuance workflow.

[Day 1 - Afternoon]

Implementing a Certificate Authority service with EJB

- Designing EJB services: Issuance API, request validation, and business rules
- Persistence: Certificate, Request, and Revocation entities and JPA mapping
- Transactions: atomicity of issuance + registration + audit, error handling
- Security: application roles, access control, and separation of concerns
- Hands-on workshop: Developing an EJB for issuing certificates and persisting status (issued/rejected).

[Day 2 - Morning]

Cryptography, key management, and HSM/keystore integration

- Java Security: KeyStore, TrustStore, providers, and formats (JKS, PKCS12)
- Certificate chains: construction, validation, and constraints (KeyUsage, BasicConstraints)
- Signature: algorithms, key sizes, parameters, and client compatibility
- CA best practices: rotation, private key protection, Root/Intermediate separation
- Hands-on workshop: Generate an intermediate CA, sign a certificate, and verify the chain on the application side.

[Day 2 - Afternoon]

Revocation, publication, and operation (CRL/OCSP, audit, monitoring)

- Revocation: reasons, status management, and propagation
- CRL publication: scheduled generation (EJB Timer), storage, and distribution
- OCSP: principles, endpoints, signed responses, and cache
- Operation: logging, traceability, alerting, and metrics (failure rate, latency)
- Hands-on workshop: Implementing a revocation service with scheduled CRL generation and a verification endpoint.

Target Audience

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals regarding the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and

reflection sessions and group work.

Certification

At the end of the session, a multiple-choice quiz is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.