

Mis à jour le 26/05/2026

S'inscrire

Formation Enterprise JavaBeans Certificate Authority

2 jours (14 heures)

Présentation

La formation Enterprise JavaBeans Certificate Authority vous apprend à mettre en place une autorité de certification basée sur EJB pour gérer des identités, certificats et clés dans un SI. Vous sécurisez l'émission, le renouvellement et la révocation de certificats pour des usages TLS, authentification applicative et signature.

Lors de cette formation, vous construisez une CA opérationnelle, de l'architecture aux flux PKI, en intégrant les contraintes d'exploitation : politiques de certificats, profils, gestion des rôles et audit. L'approche met l'accent sur la configuration, la sécurité des secrets et la traçabilité des opérations.

La pédagogie est pratique : ateliers guidés, démos d'émission et de révocation, diagnostic d'erreurs courantes (chaînes, CRL/OCSP, keystores). Vous repartez avec des scripts de déploiement, des modèles de profils, et une checklist d'exploitation pour industrialiser en environnement de test puis de production.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Installer et configurer une CA EJB et ses composants.
- Définir des politiques et profils de certificats adaptés aux usages.
- Émettre, renouveler et révoquer des certificats avec traçabilité.
- Mettre en place CRL et OCSP et valider les chaînes.
- Sécuriser les clés (keystores/HSM), rôles et accès d'administration.

Public visé

- Développeurs Java / Jakarta EE
- Ingénieurs sécurité / PKI
- Administrateurs systèmes et middleware
- DevOps en charge de la gestion des certificats

Pré-requis

- Bonnes bases en Java et notions Jakarta EE
- Compréhension de TLS, certificats X.509 et chaînes de confiance
- Pratique de la ligne de commande et des keystores (JKS/PKCS12)
- Notions réseau : DNS, ports, proxy

Pré-requis techniques

- Machine 64 bits avec 8 Go RAM minimum (16 Go recommandé)
- Linux, macOS ou Windows avec WSL2
- JDK LTS, serveur d'applications compatible Jakarta EE
- Outils : OpenSSL, client HTTP, éditeur de code, Git

Programme de notre formation Enterprise JavaBeans Certificate Authority

[Jour 1 - Matin]

Fondamentaux EJB et architecture d'une PKI

- Rappels Jakarta EE : conteneur, injection, transactions et sécurité
- EJB : Stateless/Stateful/Singleton, timers et bonnes pratiques de conception
- PKI : rôles Root CA, Intermediate CA, RA, cycle de vie des certificats
- Flux CA : CSR, émission, renouvellement, révocation, publication
- Atelier pratique : Mettre en place un projet Jakarta EE et modéliser le flux d'émission d'un certificat.

[Jour 1 - Après-midi]

Implémenter un service d'autorité de certification avec EJB

- Concevoir les services EJB : API d'émission, validation des demandes et règles métier
- Persistance : entités Certificate, Request, Revocation et mapping JPA
- Transactions : atomicité émission + enregistrement + audit, gestion des erreurs
- Sécurisation : rôles applicatifs, contrôle d'accès et séparation des responsabilités
- Atelier pratique : Développer un EJB d'émission de certificats et persister l'état (émis/refusé).

[Jour 2 - Matin]

Cryptographie, gestion des clés et intégration HSM/keystore

- Java Security : KeyStore, TrustStore, providers et formats (JKS, PKCS12)
- Chaînes de certification : construction, validation et contraintes (KeyUsage, BasicConstraints)
- Signature : algorithmes, tailles de clés, paramètres et compatibilité clients
- Bonnes pratiques CA : rotation, protection des clés privées, séparation Root/Intermediate
- Atelier pratique : Générer une CA intermédiaire, signer un certificat et vérifier la chaîne côté application.

[Jour 2 - Après-midi]

Révocation, publication et exploitation (CRL/OCSP, audit, supervision)

- Révocation : motifs, gestion des statuts et propagation
- Publication CRL : génération planifiée (EJB Timer), stockage et distribution
- OCSP : principes, endpoints, réponses signées et cache
- Exploitation : journalisation, traçabilité, alerting et indicateurs (taux d'échec, latence)
- Atelier pratique : Implémenter un service de révocation avec génération CRL planifiée et endpoint de vérification.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des

séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.