

Mis à jour le 19/08/2026

S'inscrire

Formation PKI

2 jours (14 heures)

Présentation

La PKI, ou Public key infrastructure, permet de sécuriser les identités, les échanges et les services numériques grâce aux certificats X.509, à la cryptographie asymétrique et à une gestion maîtrisée des clés.

Notre formation PKI vous permettra d'acquérir une compréhension opérationnelle des mécanismes de confiance indispensables à la sécurisation des environnements informatiques. Vous apprendrez à distinguer les rôles d'une autorité de certification, d'une autorité d'enregistrement et des différents composants participant au cycle de vie des certificats.

Vous étudierez la structure des certificats X.509, les usages des paires de clés, les chaînes de certification, les extensions, les politiques de certificats et les mécanismes de validation utilisés par les applications et les infrastructures.

La formation vous guidera dans la conception d'une architecture PKI adaptée aux besoins de l'organisation, avec une attention particulière portée à la hiérarchie de certification, à la protection des clés privées, à l'émission des certificats et à leur renouvellement.

À l'issue de la formation, vous serez en mesure d'administrer le cycle de vie des certificats, de configurer des modèles d'émission, de gérer la révocation via les CRL et OCSP, et d'appliquer les bonnes pratiques de sécurité pour fiabiliser une PKI en environnement professionnel.

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

Objectifs

- Comprendre les principes de la cryptographie asymétrique et de la confiance numérique.

- Identifier les composants, les rôles et les architectures d'une PKI.
- Analyser la structure et les usages des certificats X.509.
- Configurer l'émission et le déploiement de certificats avec AD CS.
- Gérer le renouvellement, la révocation et la validation des certificats.
- Appliquer les bonnes pratiques de sécurisation des clés et des services de certification.

Public visé

- Administrateur système
- Administrateur sécurité
- Ingénieur infrastructure
- Ingénieur cybersécurité
- Architecte sécurité

Pré-requis

- Connaissances des réseaux TCP/IP et des protocoles DNS.
- Expérience de l'administration de systèmes Windows Server.
- Notions d'administration Active Directory et de gestion des comptes.
- Connaissances de base des notions de chiffrement, d'authentification et de contrôle d'accès.

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou Windows 11, avec droits d'installation si les exercices sont réalisés en local.
- Connexion Wi-Fi ou Ethernet stable pour accéder aux ressources de formation.
- Navigateur récent, tel que Microsoft Edge, Google Chrome ou Mozilla Firefox.
- Accès à un environnement de laboratoire comprenant Windows Server 2022, Active Directory et AD CS, fourni ou préparé selon les modalités de formation.

Programme de notre formation PKI

[Jour 1 - Matin]

Fondamentaux de la PKI et de la confiance numérique

- Principes de la cryptographie symétrique et de la cryptographie asymétrique.
- Fonctions de hachage, signatures numériques, chiffrement et authentification.
- Définition d'une PKI et présentation de ses objectifs de sécurité.
- Rôles de l'autorité de certification, de l'autorité d'enregistrement et des entités finales.
- Cas d'usage des certificats pour TLS, VPN, messagerie, Wi-Fi et authentification.
- Atelier pratique : analyser une paire de clés et identifier les informations de sécurité d'un certificat.

[Jour 1 - Après-midi]

Certificats X.509 et architecture de certification

- Structure d'un certificat X.509, sujet, émetteur, numéro de série et période de validité.
- Extensions critiques, usages de clé, EKU, noms alternatifs de sujet et politiques de certificats.
- Chaînes de certification, magasins de confiance et validation du chemin de certification.
- Conception d'une hiérarchie avec autorité racine hors ligne et autorités de certification subordonnées.
- Choix des algorithmes, tailles de clés, durées de validité et protection des clés privées.
- Atelier pratique : concevoir une architecture PKI à deux niveaux pour un scénario d'entreprise.

[Jour 2 - Matin]

Émission et déploiement des certificats

- Présentation des services Active Directory Certificate Services et de leurs composants.
- Installation et paramétrage d'une autorité de certification d'entreprise.
- Rôle des modèles de certificats dans l'émission, les usages et les permissions.
- Demandes de certificats, enrôlement manuel, auto-enrôlement et intégration avec Active Directory.
- Déploiement de certificats pour serveurs, utilisateurs et postes de travail.
- Atelier pratique : créer un modèle de certificat serveur, le publier et émettre un certificat de test.

[Jour 2 - Après-midi]

Cycle de vie, révocation et sécurisation opérationnelle

- Gestion du cycle de vie, renouvellement, remplacement et archivage des certificats.
- Causes et processus de révocation des certificats.
- Fonctionnement des CRL, des points de distribution et du protocole OCSP.
- Contrôle des droits, journalisation, sauvegarde et restauration des services de certification.
- Bonnes pratiques de supervision, d'audit et de protection des clés de l'autorité de certification.
- Atelier pratique : révoquer un certificat, publier une CRL et vérifier son statut de validation.

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.