

PKI - CHIFFREMENT, AUTHENTIFICATION FORTE, SIGNATURE ÉLECTRONIQUE

Durée	3 jours	Référence Formation	3-SR-PKI
--------------	----------------	----------------------------	-----------------

Objectifs

Comprendre et gérer un projet PKI dans les meilleures conditions. Comment Choisir une PKI, Déployer une autorité de certification, générer des certificats et à mettre en œuvre une messagerie sécurisée et une solution Single Sign-On (SSO)

Participants

Tout public

Pré-requis

Directeurs informatiques, responsables sécurité, chefs de projet, consultants techniques.
Bonnes connaissances en systèmes, réseaux et sécurité informatique

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.

Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.

En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.

Formateur expert dans son domaine d'intervention

Apports théoriques et exercices pratiques du formateur

Utilisation de cas concrets issus de l'expérience professionnelle des participants

Réflexion de groupe et travail d'échanges avec les participants

Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME

Introduction

- Les faiblesses des solutions traditionnelles
- Pourquoi la messagerie électronique n'est-elle pas sécurisée ?
- Peut-on faire confiance à une authentification basée sur un mot de passe ?
- Usurpation d'identité de l'expéditeur d'un message

Cryptographie

- Concepts et vocabulaire
- Algorithmes de chiffrement symétrique et asymétrique
- Fonctions de hachage : principe et utilité

- Les techniques d'échange de clés
- Installation et configuration d'un serveur SSH
- SSH et "man in the middle"
- SSH, l'usage du chiffrement asymétrique sans certificat

Certification numérique

- Présentation du standard X509 et X509v3
- Autorités de certifications
- La délégation de confiance
- Signature électronique et authentification
- Certificats personnels et clés privées
- Exportation et importation de certificats

L'architecture PKI

- Comment construire une politique de certification
- Autorité de certification. Publication des certificats
- Autorité d'enregistrement (RA)
- Modèles de confiance hiérarchique et distribuée
- Présentation du protocole LDAP v3
- Mise en œuvre d'une autorité de certification racine
- Génération de certificats utilisateurs et serveurs

Gestion des projets PKI : par quelles applications commencer ?

- Les différentes composantes d'un projet PKI
- Choix des technologies



CAP ÉLAN FORMATION

www.capelanformation.fr - Tél : 04.86.01.20.50

Mail : contact@capelanformation.fr

Organisme enregistré sous le N° 76 34 0908834

version 2025