



PKI - Chiffrement, authentification forte, signature électronique

Mise à jour : Fév. 2024

Durée : 3 jours - 21 heures

OBJECTIFS PÉDAGOGIQUES

- 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)

PRÉREQUIS

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

PARTICIPANTS

- Tout public

MOYENS PÉDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Remise d'un support de cours

MODALITÉS D'ÉVALUATION

- Feuille de présence signée en demi-journée
- Evaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Evaluation formative tout au long de la formation
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

MOYENS TECHNIQUES EN PRÉSENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

MOYENS TECHNIQUES DES CLASSES À DISTANCE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants reçoivent une invitation avec un lien de connexion
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

ACCESSIBILITÉ

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation. Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages

Programme de formation

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

La législation