Public Key Infrastructure (PKI) : niveau 1

Date et durée

Code formation : SEC16FR
Durée : 5 jours
Nombre d'heures : 35 heures

Description

La PKI (Public Key Infrastructure) ou Infrastructure à clé publique est un ensemble de composants permettant de gérer les identités, le contrôle d'accès et les échanges numériques. Utilisée par de nombreux dispositifs (identification biométrique, carte à puce, chiffrement, authentification réseau et Wifi) la PKI reste toutefois complexe à administrer et à déployer. La maîtrise de la PKI est donc fondamentale afin de garantir la sécurité de l'entreprise.

Objectifs

A l'issue de cette formation, le participant sera capable :

- de connaitre les grands concepts de la PKI
- d'identifier les composantes d'une PKI
- de comprendre de cycle de vie d'un certificat électronique et ses utilisations
- d'implémenter une PKI d'entreprise

Cette formation lui permet de s'initier aux concepts des services de confiance notamment la signature électronique

Pré-requis

Pour suivre ce cours il faut avoir des connaissances générales sur la sécurité de l'information.
Il est également préférable d'avoir une sensibilisation aux notions de base de la cryptographie.

Public

Cette formation s'adresse aux managers, administrateurs systèmes, administrateurs sécurité et tout professionnel désireux d'avoir une idée sur la PKI

Cette formation s'adresse aux profils suivants

Administrateur système
Ingénieur système

Programme

La confiance numérique face aux risques de sécurité

- Objectifs de la sécurité
- Principaux risques IT

- Rôle de la cryptographie

Notions de base de la cryptographie

- Hachage de données
- Chiffrement symétrique
- Chiffrement asymétrique
- Génération de nombres aléatoires
- Longueur de clé

Composantes d’une PKI

- Autorité de certification
- Autorité d’enregistrement
- Le certificat électronique
- Liste de révocation de certificats et OCSP

Gestion du cycle de vie d’un Certificat électronique
Standards relatifs à la PKI

- RSA et PKCS
- Les RFCs de l’IETF
- Les Standards ITU
- Les Normes et standards européens ETSI
- Les publications de NIST aux Etats Unis

Modèles de confiance
Solutions techniques

- OpenSSL
- Microsoft CA
- EJBCA

Aspect légal et procédural

- Services de confiance
- Signature électronique
- Politiques et procédures
- Règlement EIDAS de l’Union Européenne

Protection des secrets

- Hardware Security Module
- Token cryptographique et carte à puce

Utilisations pratiques de la PKI

- Authentification forte
- Protection des e-mails
- S/MIME
- VPN
- PKI et Cloud Computing
- PKI mobile

Introduction à la signature électronique

- Formats de signature
- Applications de signature

Time Stamping

Travaux pratiques

- Gestion du cycle de vie d’un certificat avec OpenSSL
- Construire une PKI avec Microsoft CA
- Installation et mise en œuvre d’EJBCA