PKI - Conception et Architecture

4 jour(s), soit 28 heures

Programme de formation

Public visé
Ingénieurs, administrateurs systèmes et réseaux

Pré-requis
Bonnes connaissances en systèmes, réseaux et sécurité informatique

Objectifs pédagogiques
Appréhender les différents algorithmes de chiffrement symétrique et asymétrique
Mettre en œuvre une hiérarchie d'autorités de certification
Mettre en place une messagerie sécurisée
Mettre en œuvre une authentification forte par certificat X509

Description / Contenu
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 NUMERIQUE
Présentation du standard X509 et X509v3
Autorités de certification
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 oeuvre d'une autorité de certification racine

JCD and CO – 193 RUE DU GENERAL METMAN, 57070 METZ France – 03 87 37 97 70 – formation@jcd-groupe.fr – SIRET : 80187958600031
Déclaration d'activité enregistrée sous le numéro 41570348657 auprès du préfet de région Lorraine

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

PANORAMA DES OFFRES DU MARCHE
L'approche Microsoft
Les offres commerciales dédiées : Betrusted (ex-Baltimore) et Entrust
OpenPKI : la communauté Open Source
IdealX, entre solution commerciale et open source
Les offres externalisées Certplus, Versign...

Modalités pédagogiques
Pédagogie active, avec alternance de phases théoriques et d'exercices pratiques. Ces derniers permettent une utilisation immédiate et quotidienne des outils proposés.

Moyens et supports pédagogiques
Fourniture de documents et supports de cours qui restent la propriété des stagiaires
Salles équipées : vidéoprojecteur, paperboard, ordinateur individuel, support de cours papier ou électronique, outils de prise de notes

Modalités d'évaluation et de suivi
Compte rendu de fin de formation et analyse interne
Questionnaire « évaluation de la formation » rempli par le stagiaire

Validation de stage
Attestation de stage

Profil du formateur
Professionnel et expert en informatique

Lieu
JCD and CO - 193 RUE DU GENERAL METMAN, 57070 METZ France

Informations sur l'accessibilité
La formation est accessible aux personnes à mobilité réduite et toute demande d'adaptation peut être étudiée en amont de la formation en fonction du besoin des personnes. Nous contacter pour plus d'informations.