



FORMATION APPROFONDISSEMENT CRYPTOLOGIE, ÉTAT DE L'ART

OBJECTIFS

Ce stage permet aux participants d'acquérir les bases technologiques de la gestion des identités et de la cryptologie, afin de déployer des solutions dans les systèmes d'information.

À l'issue de la formation, les stagiaires seront capables de :

- définir la terminologie
- décrire les concepts de base de la cryptologie et de la gestion des identités : concepts de clé publique, clé privée et certificat
- définir les avantages et limites de chaque technologie de cryptographie
- différencier les principaux éléments de l'offre du marché, les enjeux et limites des infrastructures de gestion de clés
- décrire les enjeux du déploiement, tant techniques qu'organisationnels

MÉTHODE

Les exposés théoriques sont illustrés d'exemples concrets, des représentations schématiques, des démonstrations et travaux pratiques.

Le formateur restera disponible aux questions de la salle, et y répondra immédiatement dans la mesure du possible.

Tout au long de la formation, du temps sera consacré à des jeux de questions réponses, permettant d'intégrer les notions de base et de les manipuler en groupe.

PERSONNES CONCERNÉES, PRÉREQUIS

DSI, DRH, toute personne nouvellement en charge de la sécurité des SI, chargés du déploiement de solutions de gestion des identités et de cryptage. De bonnes connaissances dans la sécurité des SI sont nécessaires pour suivre cette formation d'approfondissement.

DURÉE

Une journée de formation en intra-entreprise pour 3 à 10 participants.

Identité et authentification

- communication et identité
- qu'est-ce qu'une identité ?
- distinction entre identité « naturelle », identité numérique et biométrie
- qu'est-ce qu'une authentification ?
- identifier et authentifier
- les technologies de l'identification et de l'authentification : cryptographie et biométrie

Bases de la cryptographie

- problématique de l'échange des documents numériques
- vocabulaire et notions de base
- chiffrement symétrique : DES
- chiffrement asymétrique : RSA, Diffie-Hellman
- les fonctions de hachage : MD5
- la signature numérique

Les protocoles d'authentification à clés privées

- le crypto-système de Needham-Schoeder
- KERBEROS et SSO

Les protocoles à clé publique

- les crypto-systèmes asymétriques de Needham-Schoeder
- PKI ou ICP (infrastructure à clés publiques)
- les cas de SSL, VPN et IPSec

ICP : la gestion des clés et la certification

- introduction
- autorité d'enregistrement et autorité de certification
- exemples de solutions: SSH et PGP
- problématique de la certification : les certificats et standard X.509
- champs standards et extensions X.509 v3
- panorama des certificats inclus dans Windows 2000
- sécurisation des échanges avec SSL/TLS,

Le marché de la gestion des identités (Open Source & commerciales)

- offres (PKIX, Microsoft, Baltimore, Entrust, etc.), critères de sélection, descriptions et choix techniques