Empire Training

Plan de Formation

PKI

Description de la formation

Les PKI – Public Key Infrastructure, ou Infrastructure à clé publique sont une solution de sécurité pour gérer les identités, le contrôle d'accès et les échanges numériques. Face à la multiplicité des outils et des usages, elles doivent être compatibles avec tous les supports et les langages – type de terminal, de réseau, de technologies de menace, et intégrer ses propres évolutions technologiques et réglementaires.

Cette formation PKI vous propose une découverte opérationnelle des PKI, à la fois panorama des solutions disponibles sur le marché, apprentissage des fondamentaux théoriques et mise en pratique sur la solution du marché la plus universelle.

PKI

Objectifs

Opérationnel

Savoir maîtriser les principes et mise en œuvre PKI.

Pédagogiques

À l'issue de cette formation PKI vous aurez acquis les connaissances et compétences nécessaires pour :

- Les technologies et normes (cryptographie gros grains)
- Les implémentations : architectures, problématiques d'intégration (organisation d'une PKI, format de certificats, points d'achoppement)
- Les aspects organisationnels et certifications
- Les impératifs de droit : signature électronique, clés de recouvrement, utilisation, export / usage international

A qui s'adresse cette formation ?

Public

Cette formation s'adresse aux Architectes, Chefs de projets, Responsables sécurité/RSSI ayant une orientation technique, Développeurs senior, Administrateurs système et réseau sénior.

Prérequis

Pour suivre ce cours de façon optimale, vous devez posséder une formation initiale ou une expérience avérée en informatique, telle que savoir lancer une ligne de commande, avoir des notions d'API et connaître le fonctionnement des réseaux IP.

PKI

Contenu du cours

Technique & cryptographie

- Primitives cryptographiques la synthèse
- Cadre général : Historique, Définitions
- Mécanismes : Chiffrement, condensat, MAC, Modes
- Assemblages courants : signature, combinaison symétrique & asymétrique, clé de session, IV
- Attaques cryptographiques : de la force brute à la cryptanalyse quantique
- Attaques système: "side channel", « man in the middle », attaques sur la gestion des clés
- Gestion des secrets : Gestion des clés HSM, containeurs logiciels
- Recommandations ANSSI/NIST/ECRYPT
- Le besoin de PKI

PKI

Contenu du cours

Implémentations techniques de la cryptographie

- Le certificat X509 : objectif, format, limitations et usages
- Implémentation cryptographique matérielles : HSM, Cartes accélératrices, Tokens et cartes à puce
- mplémentations logicielles communes : Microsoft CryptoApi, Openssl
- Intégration de tokens et cartes à puce : PKCS #11, Java JCE, Ms CryptoAPI
- Usages de la cryptographie : Authentification système et réseau, intégration dans les domaines Windows, intégration sous UNIX, NAC (i802x) VPN
- SSL/TLS: principes et attaques
- Signature électronique : principes, usages et normes (PKCS#7/CMS Standards ETSI: PAdEs/XAdes/CAdEs)
- Horodatage
- Chiffrement de messagerie avec S/MIME
- Chiffrement de disques : Bitlocker, EFS, FileVault, LUKS, Ecryptfs

PKI

Contenu du cours

Mise en œuvre des PKI

- Architecture et intégration
- Architecture PKI-X: CA/Sub-CA/RA
- Architectures communes: déclinaisons concrètes des rôles
- Définition d'une politique de certification et d'une politique de sécurité
- Détails de mise en œuvre: Génération de clé et émission des certificats, révocation, diffusion des clés
- Typologie de PKI: Interne à usage dédié Interne transversale Externe dédiée (PKI As A Service) Externe partagée (Certificate As A Service), PKI embarquées
- Aspects Organisationnels: Processus clés, contrôle.
- Certification : Exigences ETSI: 102042, 101456, 102023 Exigences RGS, PSC

PKI

Contenu du cours

Conduite d'un projet PKI

Pré études :

- Synthèse du besoin
- Définition de l'infrastructure technique
- Définition du volet organisationnel

Atelier de cadrage

- Conduite d'un atelier de cadrage
- Support de cadrage

Cahier des charges fonctionnels

- Expressions des besoins
- Cahier des charges fonctionnel

Etudes des solutions et comparaisons

- Microsoft (ADCS)
- Open (EJBCA)
- Commerciale (IDNomic)

PKI

Contenu du cours

Mise en œuvre d'une PKI

Présentation d’une solution Open Source, EJBCA
Présentation d’une solution commerciale, IDNomic
Présentation de Microsoft Certificat Services
Présentation de l’architecture des produits
Démonstration d'usage courant :
- Mise en place et configuration de la CA Racine
- Mise en place et configuration de la RA
- Mise en place du modèle de confiance- Génération de clés
- Certificat, Options de certificats
- Révocation, publication
Génération de token

Contenu du cours

Aspects légaux et perspectives

-Aspects juridiques

- Signature électronique : valeur juridique, cadre…
- Réglementations d'usage : limitations, escrow (tiers de confiance), export
- Usage international

Empire
Training

Knowledge forges Empires

Nos Contacts


empire-training.tn


+216 55 826 628
+216 74 201 616


16 Rue D'Athènes, Sfax


Contact@empire-training.tn