Verschlüsselung und Public Key Infrastructure PKI - Intensiv (VPKIK)

ID VPKIK **Prix** CHF 3 470,– (Hors Taxe) **Durée** 5 jours

A qui s'adresse cette formation

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

Pré-requis

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.

Objectifs

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
- Les trois types d'outils du marché : l'offre Microsoft Certificate Server, les offres commerciales IDNomic et l'offre Open Source (EJBCA).

Contenu

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

Implémentations techniques de la cryptographie

- Le certificat X509 : objectif, format, limitations et usages
- Implémentation cryptographique matérielles : HSM, Cartes accélératrices, Tokens et cartes à puce
- Implémentations 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

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

Verschlüsselung und Public Key Infrastructure PKI - Intensiv (VPKIK)

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)

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

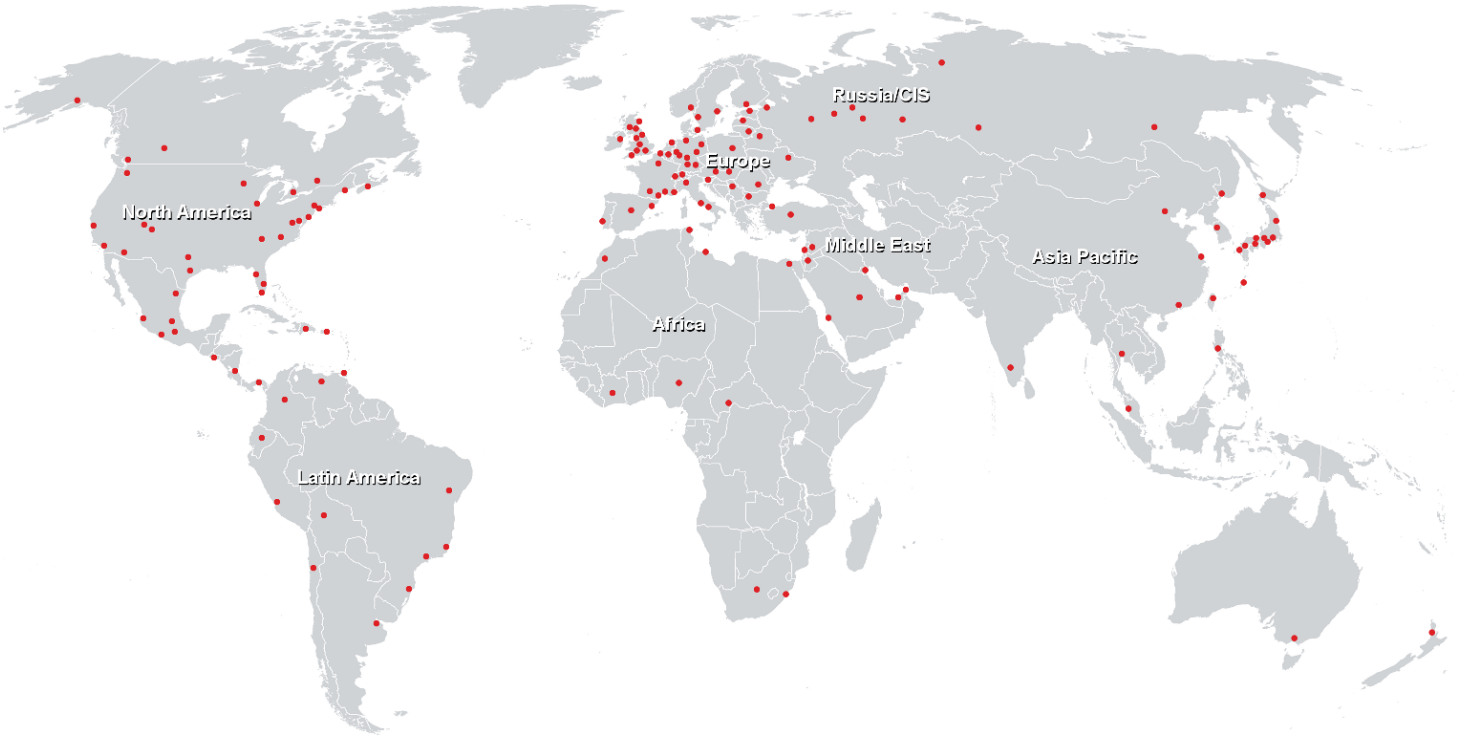
Aspects légaux et perspectives

Aspects juridiques

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

Verschlüsselung und Public Key Infrastructure PKI - Intensiv (VPKIK)

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch