Intervalle Technologies
Smart Training & Business Solutions

FORMATION PKI

Public key infrastructure

INDEX

RÉSUMÉ EXÉCUTIF

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. Les PKI sont aujourd'hui au cœur de toutes les solutions de gestion d'identité, de contrôle d'accès et de sécurisation des communications.

Objectifs de la formation

La PKI (infrastructure à clé publique) est l'ensemble des composants physiques et logiciels qui permet de gérer le cycle de vie des certificats numériques électroniques.

Concevoir, déployer et gérer une infrastructure à clé publique (PKI) pour supporter les applications qui nécessitent la sécurité distribuée.

Vous allez apprendre à

Mettre en œuvre des solutions pour sécuriser les applications et les services PKI, tels que :

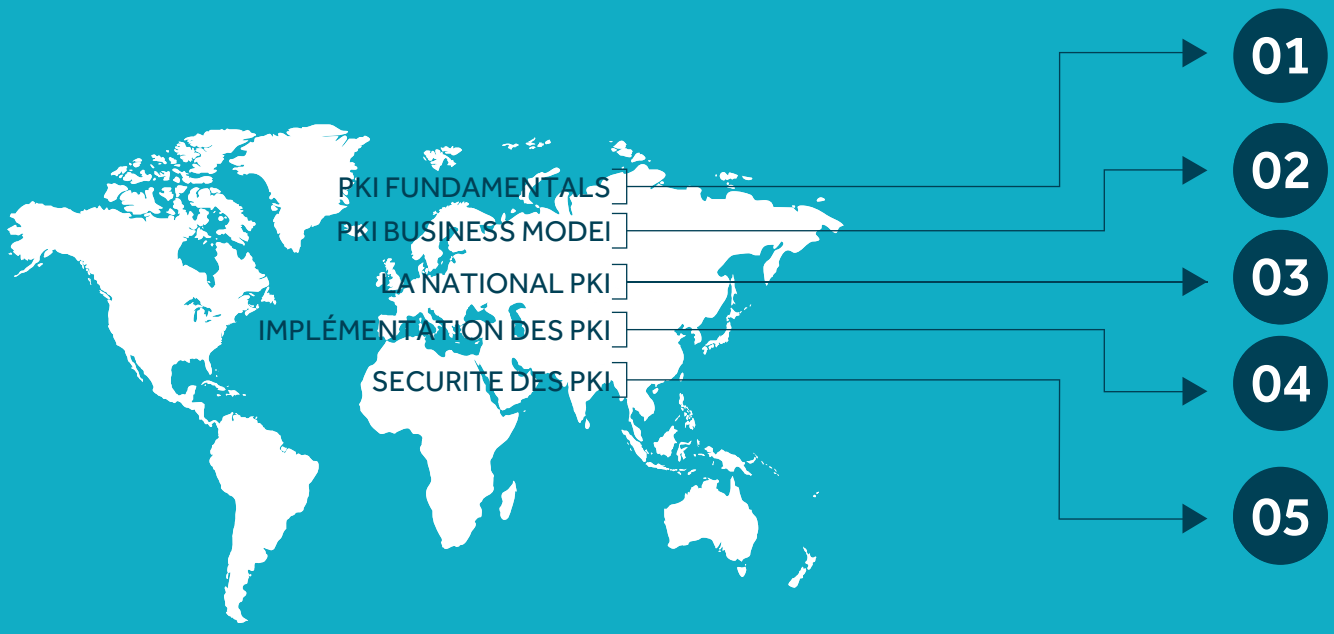
- Microsoft Internet Explorer
- Microsoft Exchange Server
- Microsoft Internet Information Server
- Microsoft Outlook
- Les services d'accès à distance

Public concerné

- Ingénieurs système
- Architectes
- Administrateurs systèmes et réseaux

Approche pédagogique

- Les formateurs certifiés sont expérimentés tant sur le plan pédagogique que technique.



PROGRAMME FORMATION PKI – SIGNATURE ELECTRONIQUE

Jour 1

PKI Fundamentals

Comprendre les concepts de base de la cryptographie, les certificats et les PKI. Utilisation et Application des PKI.

01 Concept de base de cryptographie

- Chiffrement Symétrique Vs Chiffrement Asymétrique
- Algorithme de chiffrement
- Notion de hachage
- Clé prive, Clé publique Gestion des Clé et Certificats
- Signature digitale et chiffrement
- Notion de certificat

02 Gestion des Certificats

- Notion de certificat
- Cycle de vie des certificats

03 Révocation des certificats

04 Public Key Infrastructure

- Définition d'une PKI
- Composition d'une PKI
- Architecture d'une solution PKI
- Autorité de certification Racine (Root CA) et subalterne (Sub CA)

Jour 2

PKI Business Model

Comprendre le rôle de la "Registration Authority" – "Certification Authority" – "Validation Authority"

01 Certificats et certification

02 Modèles de certificats

03 Quelques cas d'application des PKI

- Email sécurisé,
- Identity management,
- Control d'accès aux ressources
- secure code, FTP, SSL, securite des réseaux
- eCard, ePassport (eGovernement)

04 Exigences des PKI (PKI Requirements)

05 Model de confiance dans une PKI large

06 Le model business d'une PKI

- Certification Authority
- Registration Authority
- Verification Authority

07 Validation Authority (OCSP)

08 Entrepôts des certificats (base de donnes, Annuaires LDAP)

Jour 3

La National PKI

Déploiement et challenges de la nouvelle 'National PKI' Intégration de la national PK avec les PKI existantes comme celle du Ministère de l'intérieur

01 Etat Actuel des PKI en Algerie

02 Nécessite et challenge de la National PKI

03 Integration de la National PKI

04 Exigences de la National PKI (Strategic level, Business level, technical level)

05 Plan National de reprise après sinister (Disaster Planning and Recovery),

Jour 4

Implémentation des PKI

01 Politiques de certificats/certifications

- Politique de certification - Certification policy (CP)
- Enonce de pratique de certification – Certification Practice Statement (CPS) 2.

02 Choix d'un modèle (Hiérarchique ou distribuer)

03 Modes opérationnels d'une PKI

04 Gestion de capacité de la future PKI

- Identification des composants
- Combien de CA, RA,
- Dépôts des certificats (Base de données et annuaires)

05 Préparation de l'infrastructure matériel (serveurs, stations de travail)

06 Choix de la technologie.

07 Cérémonie des clés (Key Ceremony)

Jour 5

Securite des PKI

La protection des clés en utilisant les HSM devices, Recoverability et Redundancy, ainsi que d'autres contrôles Administratifs, techniques et physiques).

01 Les éléments de la sécurité des données (Confidentialité, Intégrité, disponibilité)

02 Valeur ajoute de la PKI sur la sécurité des onnées (non-répudiation)

03 Gestion des Risques d'une PKI

04 Les contrôles de sécurité d'une PKI (NIST, ISO, COBIT),

- Contrôles Administratives
- Contrôles Techniques
- Contrôles physiques (Sécurité physique d'une PKI

05 Sécurité de l'infrastructure qui support la PKI

06 Niveau de sécurité des personnes qui administrent la PKI (People Security Clearance)

07 Sauvegarde et recouvrement des clés (Software, hardware)

08 Sécurité des clés et l'utilisation des HSM (Hardware Security Module)

09 Security de la National PKI (People, Process, Technology)

PLANNING DE LA FORMATION

Module / Date	18/11/2018	19/11/2018	20/11/2018	21/11/2018	22/11/2018
PKI Fundamentals					
PKI Business Model					
La National PKI					
Implémentation des PKI					
Sécurité des PKI					

Intervalle Technologies
Smart Training & Business Solutions

CONTACTEZ NOUS

Mail: training@intervalle-technologies.com
Tél 1: 021 54 41 60
Tél 2: 021 44 87 82
Fax : 021 54 47 88