PKI : Mise en place de Services de certificats PKI avec Windows Server 2012 R2

Formation Informatique / Réseaux et Sécurité / Réseaux

Qu'est ce que les PKI ? Les PKI (Public Key Infrastructure) du système d'exploitation Windows Serveur 2012 r2 sont le fondement indispensables de la sécurité sous Windows 2012 r2.
Quels sont les PLUS de cette formations ? Cette formation présente aussi les notions essentielles de la cryptographie, bases de la PKI. La session est fortement orientée pratique et illustrée de tous les cas les plus fréquents d'utilisation en entreprise.

OBJECTIFS

- Connaitre les **notions essentielles** de la **cryptographie**.
- Acquérir la **maitrise des PKI** (Public Key Infrastructure).
- Implémenter **quotidiennement** les PKI avec **Windows Server 2012 r2**

PUBLIC

Informaticiens, administrateurs systèmes et réseaux, spécialistes des architectures Microsoft, Ingénieurs systèmes souhaitant implémenter, gérer et dépanner une PKI Serveur 2012 r2.

PRE-REQUIS

- Expérience de base de la gestion de l'Active Directory et des réseaux et systèmes d'exploitation Microsoft Windows serveur 2012 r2.

PROGRAMME

Cryptographie - Notions essentielles

- Les composantes d'une PKI d'entreprise Cryptage Symétrique
- Cryptage Asymétrique
- Structure des certificats
- Combinaison des deux méthodes de cryptage
- Application : Cryptage de fichiers (Efs)

Autorité de certification

- Type d'autorité de certification
- Implémentation d'une autorité de certification d'entreprise
- Paramétrage d'une autorité de certification
- Sauvegarde et restauration

Demande manuelle de certificat

- Inscription de certificats par mmc
- Inscription de certificats par le navigateur Internet
- Personnalisation de modèles de certificats

Déploiement automatique de certificats

- Configuration des stratégies de groupe pour le déploiement automatique certificats
- Mise à jour des modèles de certificats
- Stockage des certificats dans l'Active Directory

Gestion de la révocation des certificats

- Processus de révocation d'un certificat
- Publication de la liste de révocation pour un accès externe

Serveur OCSP (Online Certificate Status Protocol)

- Implémentation d'un serveur OCSP
- Validation du répondeur en ligne OSCP

Archivage des certificats

- Concept d'archivage et de récupération des certificats
- Création des agents de récupération
- Activation de l'archivage des certificats
- Récupération de certificats archivés

Implémenter une architecture sécurisée (CA Racine hors ligne)

A retenir

Durée : **5 jours** soit 35h.
Réf. **PKIMS**

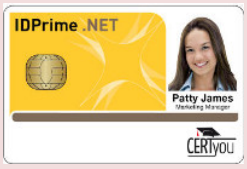
01 42 93 52 72

Dates des sessions

Paris
04/11/2024
09/12/2024
06/01/2025
17/02/2025
31/03/2025
12/05/2025
23/06/2025
04/08/2025
15/09/2025
27/10/2025
08/12/2025

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation



Une carte à Puce vous est offerte

Cette carte à puce vous offrira de nouvelles possibilités de développement et d'utilisation. Elle est idéale pour une utilisation au sein d'une infrastructure Microsoft (du développement à l'utilisation) car elle est gérée nativement par le Microsoft Base Smard Card CSP qui est désormais pré-installé sur Les clients Microsoft (Vista, 7, 8, 8.1, ...). Les anciens systèmes d'exploitation de

- Installer la CA Racine Hors ligne
- Installer la CA émettrice secondaire en ligne
- Implémentation d'une autorité de certification secondaire
- Valider le bon fonctionnement de l'architecture de PKI deux tiers

Microsoft Certificate Enrollment Protocol (Mscep)

- Scénarios d'utilisation
- Les services de rôle Cep\Ces
- Mode « renouvellement seul »
- Implémentation et configuration

Services d'inscription de périphériques réseau (Ndes)

- Processus d'inscription
- Installation et configuration du rôle
- Gestion du « mot de passe chalenge »
- Bonnes pratiques et sécurité

Application PKI - EFS (Encryptions File System)

- Cryptage de fichiers
- Ajout d'un menu contextuel pour le chiffrement
- Tester l'accès aux fichiers cryptés
- Partage De Fichiers Cryptés

Application PKI - Agent de récupération Efs

- Génération des certificats d'agent de récupération
- Modification de la stratégie
- Récupération de fichiers cryptes
- Exportation de certificat

Application PKI - Sécurisation de sites Web (Ssl)

- Fonctionnement de Ssl
- Inscription d'un certificat Ssl
- Liaison Ssl
- Test d'accès en Ssl
- Révocation de certificat Ssl

Application PKI - Signature de code PowerShell

- Certificat pour l'authentification et l'intégrité
- Signature de code PowerShell
- Révocation de certificat de signature de code

Application PKI – Vpn (Sstp)

- Implémenter un serveur Vpn\Sstp
- Valider a connexion au serveur
- Révocation de certificat Sstp

Application PKI – Carte à puce\Jeton Usb

- Présentation du matériel
- Stratégies de la double authentification
- Déploiement rapide avec un « agent d'inscription »
- Gestion des cartes à puces et jetons Usb

Horaires, Planning et Déroulement de cette formation

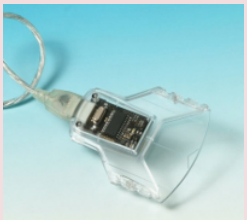
Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

Microsoft peuvent être mis à jour avec le MS Base Smart Card CSP à travers les mises jour en ligne. Cette carte est préchargée avec, outre l'assembly pour le Mini driver, l'assembly Protiva (OATH OTP) permettant à la carte de générer des mots de passe dynamiques (One time Passwords). Elle est aussi supportée par Microsoft ILM (Identiy Lifecycle Manager/Certificate Lifecycle Manager) et peut être gérée par ce système gestion de cartes pour l'entreprise. Algorithmes cryptographiques : RSA 2048, 3DES, AES.



un lecteur de carte à puce est COMPRIS

Ce lecteur de cartes à puce est transparent pour mettre en valeur le design de vos cartes à puces. Interfaces / Connexions : USB. Normes/Certifications : PC/SC, ISO/IEC 7816-1, 2, 3, 4: IC Carte avec contact. Cartes lues : ISO 7816 1, 2, 3, 4. OS compatibles : Clients Windows, Servers Windows, Linux Redhat WS3.0, WS4.0, Suse Professionnal 9.2, DEBIAN "Sarge".

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

PKI : Mise en place de Services de certificats PKI avec Windows Server 2012 R2

Formation Informatique / Réseaux et Sécurité / Réseaux

PROCHAINES FORMATIONS

ITIL Foundation
PRINCE2 Foundation
PRINCE2 Foundation et PRINCE2 Practitioner

CERTyou est certifié Qualiopi

CERTyou a été reconnu par le BUREAU VERITAS pour la qualité de ces procédures et lui a décerné la certification Qualiopi Formation Professionnelle. La certification de services Qualiopi Formation Professionnelle répond aux exigences qualité décrites dans l'article 1 du décret n°2015-790 du 30 juin 2015.

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'actions suivantes : **ACTIONS DE FORMATION**

Retrouvez cette formation sur notre site :
PKI : Mise en place de Services de certificats PKI avec Windows Server 2012 R2