Date de publication : 05/08/2025

Formation : Infrastructure à clé publique (PKI) et services de certificats Windows

Formation pratique - 4j - 28h00 - Réf. PKG
Prix : 2260 € H.T.

NEW

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Maitriser les notions essentielles du chiffrement
- Installer et configurer une autorité de certification Windows
- Gérer le déploiement, le renouvellement et la restauration des certificats
- Utiliser le Trusted Platform Module (TPM) et les cartes à puce pour le stockage des certificats
- Implémenter le chiffrement, la signature et l'authenticité des données à l'aide de certificats
- Gérer la révocation des certificats

Public concerné

Ingénieurs, administrateurs systèmes et réseaux.

Prérequis

Bonnes connaissances du système d'exploitation Windows Server, des réseaux et de la sécurité informatique.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

PARTICIPANTS

Ingénieurs, administrateurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances du système d'exploitation Windows Server, des réseaux et de la sécurité informatique.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

1 Chiffrement, les notions essentielles

- Pourquoi une PKI ?
- Rôles et infrastructures.
- Les composantes d'une PKI d'entreprise.
- Chiffrements symétrique et asymétrique.
- Combinaison des deux méthodes de chiffrement.

Travaux pratiques

Comprendre les protocoles de chiffrement symétrique et leurs utilisations combinées avec le chiffrement asymétrique.

2 Autorité de certification

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

Travaux pratiques

Déploiement manuel et automatisé d'une autorité de certification racine d'entreprise. Gestion des modèles de certificats.

3 Gestion des certificats

- Composantes d'un certificat.
- Inscription de certificats.
- Modèles de certificats.
- Déploiement automatique de certificats.
- Configuration des stratégies de groupe pour le déploiement automatique de certificats.
- Mise à jour des modèles de certificats.
- Emplacements de stockage des certificats.
- Certificats machine et TPM.
- Cartes à puce et agents d'inscription de certificats.

Travaux pratiques

Déployer manuellement et automatiquement différents certificats Windows. Protéger les certificats ordinateurs à l'aide du TPM. Gestion des cartes à puce.

4 Chiffrement de données

- Présentation du concept et des avantages du chiffrement de données.
- Implémenter et dépanner le chiffrement EFS (Encrypting Flie System).
- Partage de fichiers chiffrés.
- Implémentation d'agent de récupération.
- Chiffrement et authentification forte.

Travaux pratiques

Implémenter le chiffrement de fichiers et récupérer des fichiers chiffrés à l'aide d'agent de récupération.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

5 Signature de données

- Authentification et intégrité des données.
- Concept et techniques de signature avec certificats.
- Validation de l'intégrité des données.

Travaux pratiques
Configurer la signature de code PowerShell. Déployer automatiquement les "éditeurs authentifiés".

6 Sécurisation de sites web

- Inscription d'un certificat pour serveur web.
- Implémenter un serveur web sécurisé.
- Gestion des erreurs de connexion.
- Révocation de certificat serveur web.

Travaux pratiques
Configurer l'authentification et le chiffrement sur un serveur web sécurisé.

7 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.

Travaux pratiques
Importer et exporter des certificats. Archiver des certificats et récupérer des certificats archivés.

8 Gestion de la révocation des certificats

- Processus de révocation des certificats.
- Modification des listes CDP et AIA des certificats.
- Publication des listes de révocation.
- Publication de la révocation en HTTP.

Travaux pratiques
Modification des emplacements CDP (plateforme de données clients) et AIA et tests de l'accès aux listes de révocation.

9 Serveur OCSP (Online Certificate Status Protocol)

- Concept et implémentation d'un serveur OCSP.
- Personnalisation du certificat OCSP.
- Installer le serveur OCSP.
- Modifier les "extensions" de l'autorité de certification.
- Configuration de révocation.
- Résolution DNS Interne\Internet du serveur OCSP.
- Révocation OCSP pour un serveur VPN SSTP.
- Validation du répondeur en ligne OSCP.

Travaux pratiques
Implémentation, configuration et validation d'un serveur OCSP Windows.

Dates et lieux

CLASSE À DISTANCE
2026 : 16 juin, 8 sep., 8 déc.

PARIS LA DÉFENSE
2026 : 9 juin, 1 sep., 1 déc.