SARL ONEO
1025 rue Henri Becquerel
Parc Club du Millénaire, Bât. 27
34000 MONTPELLIER
N° organisme : 91 34 0570434

Nous contacter :
+33 (0)4 67 13 45 45
www.ait.fr
contact@ait.fr

Référence	**3-SR-PKI**
Durée	**3 jours (21 heures)**
Éligible CPF	**NON**
Mise à jour	**26/12/2022**

PKI - Chiffrement, authentification forte, signature électronique

Objectifs pédagogiques

- Comprendre et gérer un projet PKI dans les meilleures conditions. Comment Choisir une PKI,Déployer une autorité de certification, générer des certificats et à mettre en œuvre une messagerie sécurisée et une solution Single Sign-On (SSO)

Public concerné

- Directeurs informatiques, responsables sécurité, chefs de projet, consultants techniques.

Prérequis

- Bonnes connaissances en systèmes, réseaux et sécurité informatique

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques.
- Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
- Remise d'un support de cours.

Modalités d'évaluation

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Attestation de stage à chaque apprenant,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

Moyens techniques en présentiel

- Accueil des stagiaires dans une salle dédiée à la formation équipée à minima d'un vidéo projecteur et d'un tableau blanc et/ou paperboard.
- Pour les formations nécessitant un ordinateur, un PC est mis à disposition de chaque participant.

Moyens techniques en distanciel

- A l'aide d'un logiciel (Teams, Zoom…), d'un micro et éventuellement d'une caméra les apprenants interagissent et communiquent entre eux et avec le formateur.
- Sessions organisées en inter comme en intra entreprise.
- L'accès à l'environnement d'apprentissage ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Pour toute question avant et pendant le parcours, assistance technique à disposition au 04 67 13 45 45.

Organisation

- Délai d'accès : 5 jours ouvrés
(délai variable en fonction du financeur)
- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

Accessibilité

- Les personnes en situation d'handicap sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.
- Pour tout renseignement, notre référent handicap reste à votre disposition : mteyssedou@ait.fr

Profil formateur

- Nos formateur sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

Certification possible

- Aucune

PKI - Chiffrement, authentification forte, signature électronique

1. Introduction

- Les faiblesses des solutions traditionnelles
- Pourquoi la messagerie électronique n'est-elle pas sécurisée ?
- Peut-on faire confiance à une authentification basée sur un mot de passe ?
- Usurpation d'identité de l'expéditeur d'un message

2. Cryptographie

- Concepts et vocabulaire.
- Algorithmes de chiffrement symétrique et asymétrique
- Fonctions de hachage : principe et utilité
- Les techniques d'échange de clés
- Installation et configuration d'un serveur SSH
- SSH et "man in the middle"
- SSH, l'usage du chiffrement asymétrique sans certificat

3. Certification numérique

- Présentation du standard X509 et X509v3
- Autorités de certifications
- La délégation de confiance
- Signature électronique et authentification
- Certificats personnels et clés privées
- Exportation et importation de certificats

4. L'architecture PKI

- Comment construire une politique de certification
- Autorité de certification. Publication des certificats
- Autorité d'enregistrement (RA)
- Modèles de confiance hiérarchique et distribuée
- Présentation du protocole LDAP v3
- Mise en œuvre d'une autorité de certification racine
- Génération de certificats utilisateurs et serveurs

5. Gestion des projets PKI : par quelles applications commencer ?

- Les différentes composantes d'un projet PKI
- Choix des technologies

6. La législation