

Sessions garanties disponibles

Formation PKI, mise en œuvre

Réf. SF33615

4 jours de formation pour implémenter une Infrastructure à clés publiques !

4 j Durée	3 200 € HT Inter / participant	8 200 € HT Intra (≤12 pers.)	4 Sessions à venir
--------------	-----------------------------------	---------------------------------	-----------------------

Objectifs pédagogiques

- ✓ Expliquer les principes de la cryptographie symétrique et asymétrique
- ✓ Concevoir une architecture d'infrastructure à clé publique (ICP)
- ✓ Mettre en œuvre des communications sécurisées
- ✓ Configurer et gérer l'émission, la validation et la révocation des certificats

Public visé & prérequis

Public visé Administrateurs systèmes et réseaux, Responsables de la sécurité des systèmes d'information (RSSI)

Prérequis De solides bases en administration de systèmes informatiques et de réseaux, des connaissances de base en sécurité informatique.

Programme détaillé

Principes de la cryptographie et des algorithmes cryptographiques

- Concepts de chiffrement, de déchiffrement et de hachage
- Cryptographie symétrique (AES)
- Cryptographie asymétrique (RSA, ECC)
- Algorithmes faibles (MD5, SHA-1)
- Vulnérabilités dans le monde réel
- Fonctions de hachage (vérification de l'intégrité, signatures numériques)
- Applications et limites des algorithmes cryptographiques (RSA, ECC, SHA-2)
- Évaluation des méthodes cryptographiques

Activités pratiques :

- Chiffrement et déchiffrement de données avec AES et RSA
- Calcul de hachages à l'aide de SHA-2
- Simulation de transferts de données sécurisés avec la cryptographie asymétrique.

Introduction à l'infrastructure à clé publique (PKI)

- Concepts fondamentaux de l'ICP
- Rôles et responsabilités des autorités de certification (AC)
- Modèles de confiance hiérarchiques des AC
- Vue d'ensemble de la norme X.509
- Extensions de la norme X.509v3
- Principes de validation de la chaîne de certificats
- Introduction aux autorités d'enregistrement (AE)
- Processus de l'ICP

Activités pratiques :

- Examen de la structure des certificats numériques
- Gérer les magasins de certificats
- Exporter/importer des certificats

- Analyser la chaîne de confiance des certificats existants

Conception d'une architecture PKI

- Architecture PKI hiérarchique
- AC racine et intermédiaires
- Politiques de certification (PC)
- Déclarations de pratiques de certification (CPS)
- Modèles de confiance : hiérarchique ou distribué
- Outils : Microsoft PKI, solutions d'AC à code source ouvert
- Gestion des hiérarchies d'AC

Activités pratiques :

- Déploiement de l'AC racine et des AC intermédiaires
- Configurer les CP et les CPS
- Délivrer des certificats d'utilisateur et de serveur pour différents cas d'utilisation

Mise en œuvre des processus de gestion des certificats

- Gestion du cycle de vie des certificats X.509
- Délivrance des certificats
- Processus de renouvellement
- Méthodes de validation (OCSP, CRLs)
- Techniques de révocation
- Gestion de l'expiration
- Enrôlement automatisé des certificats (Active Directory)
- Longueur des clés et normes de cryptage
- Stockage sécurisé des clés privées

Activités pratiques :

- Configuration de l'OCSP et des CRL
- Mise en place de flux de travail pour le renouvellement des certificats
- Dépannage des certificats révoqués ou expirés

Communications sécurisées et authentification forte à l'aide de certificats X.509

- Cryptage sécurisé du courrier électronique et signatures numériques (S/MIME)
- Authentification forte à deux facteurs
- Configuration de l'authentification unique (SSO)
- Gestion des certificats X.509

Activités pratiques :

- Configurer le courrier électronique sécurisé dans un environnement professionnel simulé
- Mise en place d'une authentification forte à l'aide de certificats X.509
- Tester des connexions sécurisées à l'aide d'un SSO basé sur une PKI

Planification et mise en œuvre d'un projet PKI

- Étapes clés du déploiement de l'ICP
- Sélection de la technologie
- Intégration à l'infrastructure informatique existante
- Considérations juridiques et de conformité
- Meilleures pratiques de l'industrie

Activités pratiques :

- Élaborer un plan de projet complet pour l'ICP
- Créer des listes de contrôle pour les tâches de déploiement
- Examiner et analyser des études de cas de projets PKI réussis

Prochaines sessions

DATE	LIEU	STATUT
23/11/2026	Paris	Sur confirmation
23/11/2026	à distance	Sur confirmation
07/12/2026	Lyon	Sur confirmation
07/12/2026	à distance	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Anis H. — Formateur Windows

Anis intervient sur des formations portant sur la sécurité défensive et l'architecture de sécurité (Blue Team). Les sujets abordés incluent notamment Windows. Son activité de formation remonte à 2014, soit...

Ils nous font confiance

Cette année notre filière Sécurité Défensive & Architecture (Blue Team) a accompagné plus de 25 entreprises dont :

ADVENTIEL ALTEN SA AMCS TECHNOLOGIES ARPEGE BIRDZ CA-GIP CHAPSVISION CHELA + CONSORT FRANCE ECONOCOM SERVICES & SOLUTION +15 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com