ACE MULTIPASS
Cybersécurité - Méthodes agiles

FICHE DE FORMATION

Organisme de formation

PKI Masterclass – Retour D'expérience Et Revue D'architecture

Formation d'1 jour qui va au-delà de la théorie PKI, en s'appuyant sur des retours d'implémentation réelle : protection des clés en environnement contraint, arbitrage OCSP/CRL, gestion à l'échelle de milliers de certificats et prévention des interruptions liées aux expirations.

DURÉE	PRIX	HORAIRES
1 jour	**1 000 €**	**9h00 - 17h00** *(pause déjeuner de 1h30 à midi)*

PRÉSENTATION

Une infrastructure à clés publiques (PKI) ne se résume pas à installer une autorité de certification : c'est un système vivant, critique pour toute l'entreprise, qui doit tenir 15 à 20 ans. Cette formation s'appuie sur des retours d'implémentation réelle pour aller au-delà de la théorie et aborder les questions que seule la pratique révèle : comment protéger une clé privée sur un device industriel contraint, comment choisir entre OCSP et CRL sans créer un point de défaillance unique, comment faire tenir une PKI à l'échelle de milliers de certificats sans subir d'interruption de service liée à une expiration oubliée.

Le programme couvre les architectures PKI en production (deux-tiers, trois-tiers, multi-root, cloud, air-gapped), la protection des clés par HSM, l'hygiène opérationnelle (rotation, révocation, synchronisation temporelle), le Certificate Lifecycle Management et son outillage, les protocoles d'enrôlement automatisés (EST, SCEP, ACME), la conformité réglementaire (eIDAS, ISO 27001, NIST 800-53, ETSI, PCI-DSS) et les exercices de résilience face à une compromission de CA. Il intègre également l'enjeu de la migration post-quantique, avec l'échéance 2030 fixée par le NIST.

Note : pour des raisons de confidentialité, cette formation n'est disponible qu'en intra-entreprise.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation, les participants seront capables :

- d'évaluer la maturité d'une PKI existante,
- de choisir une architecture adaptée au contexte organisationnel,
- de sécuriser et faire évoluer la gestion des clés critiques,
- et de structurer la gouvernance et la conformité d'une PKI d'entreprise.

PUBLIC CIBLE ET PRÉREQUIS

Public visé : administrateurs PKI, architectes sécurité, responsables IAM disposant déjà des bases théoriques (cryptographie, certificats X.509, notions d'annuaires).

PROGRAMME

Module 1 · Paysage des menaces et urgence de la migration (45 min)

- Évolution des menaces récentes (phishing as a service, deep fakes, attaques ciblant les clés).
- La menace quantique sur le chiffrement à clé publique et l'échéance NIST 2030.
- Pourquoi la migration cryptographique à grande échelle n'a jamais été testée à ce niveau.
- Ce que ça implique concrètement pour une PKI existante.

Module 2 · Architectures PKI en production : au-delà du modèle standard (1h)

- Rôles réels des CA (Root, Intermediate, Secondary, Issuing) et pourquoi les distinctions comptent en pratique.
- Comparatif deux-tiers vs trois-tiers selon le contexte (entreprise standard vs finance/gouvernement).
- PKI multi-root et cross-certification (modèle Federal Bridge) vs simple ajout d'une root CA externe au magasin de confiance — les implications de sécurité de chaque choix.
- PKI cloud-managée (Azure AD CS, AWS Private CA) et PKI air-gapped (défense, infrastructures critiques) : quand chaque modèle s'impose.

Module 3 · Protection des clés privées et HSM (1h)

- Pourquoi le stockage fichier reste risqué, même chiffré, en environnement industriel/IoT contraint.
- Ce qu'apporte réellement un HSM : génération et opérations cryptographiques internes, tamper-resistance, contrôle d'accès par quorum (M-of-N), sauvegarde par partage de secret (Shamir).

Étude de cas — Activation d'une Root CA protégée par HSM avec approbation multi-officiers.

Module 4 · Hygiène opérationnelle d'une PKI vivante (1h)

- Rotation des clés : fréquences recommandées par le NIST selon le niveau de CA (root, subordonnée, entité finale).
- Révocation automatique à chaque renouvellement.
- OCSP vs CRL : le compromis disponibilité/sécurité et la question du point de défaillance unique.
- Synchronisation temporelle fiable en environnement isolé (GPS/NTP) — un prérequis souvent négligé.
- Interfaces d'enrôlement pour utilisateurs et devices : équilibrer automatisation et intervention humaine.

Module 5 · Certificate Lifecycle Management — gérer une PKI à l'échelle (1h15)

- Pourquoi le CLM devient indispensable passé un certain volume de certificats.
- Découverte automatique (scan réseau, agents, intégration API avec les CA internes/externes) et inventaire centralisé.
- Contrôle de conformité (détection de clés faibles, certificats auto-signés, durées de vie excessives).
- Automatisation et intégration ITSM/SIEM.
- Alerte d'expiration et audit trail.
- Tour d'horizon des solutions du marché (Venafi, Keyfactor, Entrust, Sectigo, DigiCert, CertSecure) — critères de choix, pas de recommandation figée.

Module 6 · Protocoles d'enrôlement automatisés (45 min)

- Comparatif EST, SCEP et ACME : cas d'usage, niveau de sécurité, adoption actuelle.
- Pourquoi ACME domine désormais le TLS public et gagne du terrain en entreprise, alors que SCEP reste la norme sur le mobile/IoT (MDM).
- Auto-enrollment Active Directory : forces et limites en environnement Microsoft pur.

Module 7 · Conformité et gouvernance PKI (1h)

- Construire une Certificate Policy et une Certification Practice Statement (CP/CPS).

- Panorama des référentiels applicables : eIDAS, ISO 27001, NIST 800-53, ETSI EN 319 411, WebTrust, et normes sectorielles (PCI-DSS, GSMA SAS-SM pour l'eSIM).
- Organisation des audits (conformité, sécurité, opérationnel) et documentation attendue (stratégie sécurité, cartographie des risques, matrice RACI).

Module 8 · Tester sa résilience PKI (30 min)

- Plans de continuité et de reprise appliqués à une PKI : simulation de compromission d'une CA.
- Trois niveaux de test — exercice sur table, simulation partielle, exercice grandeur nature — et ce que chacun permet de valider (RTO/RPO, procédures, communication de crise).

Étude de cas — 12 incidents réels qui ont marqué l'histoire des PKI.

Clôture · Synthèse et échanges (30 min)

- Retour collectif sur les pièges les plus fréquents rencontrés en déploiement réel.
- Grille d'auto-évaluation de maturité PKI (technique 40 % / processus 60 %, selon le ratio observé sur le terrain).

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Chaque session peut être adaptée aux besoins des personnes en situation de handicap. Nous invitons les participants concernés à nous en informer avant le début de la formation, afin d'examiner ensemble les aménagements possibles : conditions d'accès aux salles, adaptation des supports et des méthodes pédagogiques, ou réorganisation du planning de la session.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

L'animation des sessions s'appuie sur des outils variés : supports audiovisuels, documents remis aux stagiaires, mises en application pratiques accompagnées de leurs corrigés pour les formations à vocation opérationnelle, et études de cas concrets ou retours d'expérience pour les sessions à caractère plus théorique.

À la fin de chaque session, ACE-MULTIPASS remet aux stagiaires un questionnaire de satisfaction, dont les résultats sont ensuite examinés par l'équipe pédagogique.

Une feuille de présence est signée à chaque demi-journée et remise en fin de parcours ; une attestation de suivi de formation est également délivrée aux stagiaires ayant participé à l'intégralité de la session.

COMPÉTENCES DU FORMATEUR

Nos intervenants sont choisis pour leur expertise dans les domaines qu'ils enseignent. Chacun est sélectionné par notre équipe pédagogique, qui vérifie à la fois sa maîtrise technique du sujet et ses aptitudes à transmettre et animer un groupe. Ils justifient généralement de cinq à dix ans d'expérience professionnelle au minimum, et occupent ou ont occupé des fonctions à responsabilité dans leur secteur d'activité.

MODALITÉS D'ÉVALUATION

Tout au long du parcours, le formateur mesure la progression des stagiaires à travers différents exercices : questionnaires à choix multiples, mises en situation ou exercices pratiques.

Un test de positionnement est par ailleurs réalisé avant et après la formation, afin de mesurer les compétences acquises par chaque participant.