ACE MULTIPASS
Cybersécurité - Méthodes agiles

TRAINING DATASHEET

Training Provider

PKI Masterclass – Lessons Learned And Architecture Review

A 1-day course that goes beyond PKI theory, drawing on real-world implementation experience: key protection in constrained environments, OCSP/CRL trade-offs, managing thousands of certificates at scale and preventing expiry-related outages.

DURATION	PRICE	SCHEDULE
1 day	**€1,000**	**9:00 am - 5:00 pm** *(1.5-hour lunch break at midday)*

OVERVIEW

A public key infrastructure (PKI) is much more than installing a certification authority: it is a living system, critical to the whole organisation, that must last 15 to 20 years. This course draws on real-world implementation experience to go beyond theory and address the questions that only practice reveals: how to protect a private key on a constrained industrial device, how to choose between OCSP and CRL without creating a single point of failure, how to scale a PKI to thousands of certificates without suffering a service outage caused by a forgotten expiry.

The programme covers production PKI architectures (two-tier, three-tier, multi-root, cloud, air-gapped), HSM-based key protection, operational hygiene (rotation, revocation, time synchronisation), Certificate Lifecycle Management and its tooling, automated enrollment protocols (EST, SCEP, ACME), regulatory compliance (eIDAS, ISO 27001, NIST 800-53, ETSI, PCI-DSS) and resilience exercises in the event of a CA compromise. It also addresses the challenge of post-quantum migration, with the 2030 deadline set by NIST.

Note: for confidentiality reasons, this course is only available in-house.

LEARNING OBJECTIVES

By the end of the course, participants will be able to:

- assess the maturity of an existing PKI,
- choose an architecture suited to the organisational context,
- secure and evolve the management of critical keys,
- and structure the governance and compliance of an enterprise PKI.

TARGET AUDIENCE AND PREREQUISITES

Target audience: PKI administrators, security architects and IAM managers who already have the theoretical basics (cryptography, X.509 certificates, directory concepts).

PROGRAMME

Module 1 · The Threat Landscape and the Urgency of Migration (45 min)

- Recent threat trends (phishing-as-a-service, deepfakes, attacks targeting keys).
- The quantum threat to public-key cryptography and the NIST 2030 deadline.
- Why large-scale cryptographic migration has never been tested at this level.
- What this concretely means for an existing PKI.

Module 2 · PKI Architectures in Production: Beyond the Standard Model (1 h)

- The real roles of CAs (Root, Intermediate, Secondary, Issuing) and why the distinctions matter in practice.
- Two-tier vs three-tier architectures depending on context (standard enterprise vs finance/government).
- Multi-root PKI and cross-certification (Federal Bridge model) vs simply adding an external root CA to the trust store — the security implications of each choice.
- Cloud-managed PKI (Azure AD CS, AWS Private CA) and air-gapped PKI (defence, critical infrastructure): when each model is the right fit.

Module 3 · Private Key Protection and HSMs (1 h)

- Why file-based storage remains risky, even when encrypted, in constrained industrial/IoT environments.
- What an HSM really brings: internal key generation and cryptographic operations, tamper resistance, quorum-based access control (M-of-N), backup through secret sharing (Shamir).

Case study — Activating an HSM-protected Root CA with multi-officer approval.

Module 4 · Operational Hygiene for a Living PKI (1 h)

- Key rotation: NIST-recommended frequencies by CA level (root, subordinate, end entity).
- Automatic revocation at each renewal.
- OCSP vs CRL: the availability/security trade-off and the single-point-of-failure question.
- Reliable time synchronisation in isolated environments (GPS/NTP) — an often-overlooked prerequisite.
- Enrollment interfaces for users and devices: balancing automation and human intervention.

Module 5 · Certificate Lifecycle Management — Managing PKI at Scale (1 h 15 min)

- Why CLM becomes essential beyond a certain volume of certificates.
- Automated discovery (network scanning, agents, API integration with internal/external CAs) and centralised inventory.
- Compliance checks (detection of weak keys, self-signed certificates, excessive lifetimes).
- Automation and ITSM/SIEM integration.
- Expiry alerts and audit trail.
- Overview of market solutions (Venafi, Keyfactor, Entrust, Sectigo, DigiCert, CertSecure) — selection criteria, no one-size-fits-all recommendation.

Module 6 · Automated Enrollment Protocols (45 min)

- EST, SCEP and ACME compared: use cases, security level, current adoption.
- Why ACME now dominates public TLS and is gaining ground in the enterprise, while SCEP remains the standard for mobile/IoT (MDM).
- Active Directory auto-enrollment: strengths and limitations in a pure Microsoft environment.

Module 7 · PKI Compliance and Governance (1 h)

- Building a Certificate Policy and a Certification Practice Statement (CP/CPS).

- Overview of applicable frameworks: eIDAS, ISO 27001, NIST 800-53, ETSI EN 319 411, WebTrust, and sector-specific standards (PCI-DSS, GSMA SAS-SM for eSIM).
- Organising audits (compliance, security, operational) and the expected documentation (security strategy, risk map, RACI matrix).

Module 8 · Testing Your PKI Resilience (30 min)

- Business continuity and disaster recovery plans applied to a PKI: simulating a CA compromise.
- Three levels of testing — tabletop exercise, partial simulation, full-scale exercise — and what each one validates (RTO/RPO, procedures, crisis communication).

Case study — 12 real-world incidents that shaped PKI history.

Wrap-up · Summary and Discussion (30 min)

- Group review of the most common pitfalls encountered in real-world deployments.
- PKI maturity self-assessment grid (40% technical / 60% process, based on the ratio observed in the field).

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Each session can be adapted to the needs of people with disabilities. Participants concerned are invited to let us know before the start of the course so that we can examine possible arrangements together: room access conditions, adaptation of materials and teaching methods, or rescheduling of the session.

TEACHING AND TECHNICAL RESOURCES

Sessions are delivered using a variety of tools: audiovisual materials, documents handed out to trainees, practical exercises with their solutions for operational courses, and real-world case studies or lessons learned for more theoretical sessions.

At the end of each session, ACE-MULTIPASS gives trainees a satisfaction questionnaire, the results of which are then reviewed by the teaching team.

An attendance sheet is signed every half-day and handed in at the end of the course; a certificate of attendance is also issued to trainees who have attended the entire session.

TRAINER EXPERTISE

Our trainers are chosen for their expertise in the fields they teach. Each one is selected by our teaching team, which checks both their technical command of the subject and their ability to teach and lead a group. They generally have at least five to ten years of professional experience and hold or have held positions of responsibility in their sector.

ASSESSMENT METHODS

Throughout the course, the trainer measures trainees' progress through various exercises: multiple-choice questionnaires, role-plays or practical exercises.

A positioning test is also carried out before and after the course to measure the skills acquired by each participant.