ACE MULTIPASS
Cybersécurité - Méthodes agiles

TRAINING DATASHEET

Training Provider

PKI Introduction, Implementation And Administration

A 4-day course to design, deploy, configure and operate an enterprise public key infrastructure (PKI) based on Microsoft Active Directory Certificate Services (AD CS), combining a solid theoretical grounding with in-depth hands-on labs.

DURATION	PRICE	SCHEDULE
4 days	**€2,800**	**9:00 am - 5:00 pm** *(1.5-hour lunch break at midday)*

OVERVIEW

Note: the course can be adapted to use EJBCA instead of Microsoft AD CS.

Public key infrastructure (PKI) is a cornerstone of modern IT security, enabling authentication, encryption, digital signatures and secure communications. This course covers PKI concepts, from the fundamentals to advanced enterprise use cases, with a focus on real-world deployment and administration.

Through guided hands-on labs, participants:

- install and configure a multi-tier PKI
- manage certificate templates
- automate enrollment
- implement key archival and recovery
- secure data with EFS
- sign PowerShell scripts
- deploy smart card authentication
- use certificates to secure services such as VPN

The course emphasises operational security, best practices and troubleshooting.

LEARNING OBJECTIVES

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

- Understand PKI concepts, standards and trust models.
- Design and deploy an enterprise PKI architecture.
- Install and configure root and subordinate certification authorities.
- Manage certificate templates and enrollment policies.
- Set up auto-enrollment via GPO.

- Manage the certificate lifecycle (renewal, revocation, CRL).
- Enable key archival and recover certificates.
- Configure EFS and data recovery agents (DRA).
- Sign and verify PowerShell scripts.
- Deploy smart card authentication.
- Secure services (VPN…) with certificates.
- Apply PKI best practices.

TARGET AUDIENCE AND PREREQUISITES

As this is a technical course, participants should have a good knowledge of IT security, Windows Server (Active Directory, Windows Server…), system administration and Internet protocols. The target audience is:

- Systems and infrastructure administrators
- Security engineers and architects
- IAM specialists
- IT professionals responsible for certificate-based security
- Engineers working with Windows Server / Active Directory

PROGRAMME

Module 1 · Cryptography & PKI Fundamentals (3.5 h)

- Security objectives: confidentiality, integrity, authentication, non-repudiation.
- Symmetric vs asymmetric cryptography.
- Hash functions and digital signatures.
- PKI: objectives and use cases.
- Certificates and chains of trust.
- Standards: X.509, PKCS, TLS.

Hands-on lab — Protocol analysis (FTP vs HTTP), network capture, Diffie-Hellman simulation.

Module 2 · Secure Communications & OpenSSL (3.5 h)

- Key pairs.
- CSR (Certificate Signing Request).
- Certificate validation.
- Limitations of asymmetric encryption.
- Hybrid models.

Hands-on lab — SSH installation, key-based authentication, OpenSSL: key generation, certificates, signatures, secure file exchange.

Module 3 · PKI Architecture (3 h)

- PKI types: internal, public, restricted.
- Hierarchical architectures.
- CA / RA roles.
- Certificate Policy (CP) and Certification Practice Statement (CPS).
- Security: offline Root CA, HSM…

Hands-on lab — Designing a PKI architecture, lab preparation.

Module 4 · Deploying an Offline Root CA (4 h)

- Securing the Root CA.
- Certificate validity periods.

- Certificate Revocation Lists (CRL).
- Audit.

Hands-on lab — Root CA installation, configuring CDP / AIA extensions.

Module 5 · Subordinate CA (2.5 h)

- Chain of trust.
- Integration with IIS.

Hands-on lab — Sub CA installation, certificate publication.

Module 6 · OCSP (2.5 h)

- Deployment strategies.
- OCSP vs CRL.

Hands-on lab — OCSP service installation, testing.

Module 7 · Certificate Stores (2 h)

- Windows certificate stores.
- Certificate formats: PFX, CER.

Hands-on lab — Certificate import/export, SSL/TLS authentication.

Module 8 · Key Archival & EFS (2 h)

- Key archival.
- KRA / DRA (key recovery agents).
- File encryption with EFS.

Hands-on lab — Certificate recovery, file encryption.

Module 9 · Automation (1.5 h)

- Certificate templates.
- Auto-enrollment.

Hands-on lab — GPO configuration, testing.

Module 10 · Code Signing (1.5 h)

- Code signing principles.
- Signing PowerShell scripts.

Hands-on lab — Script signing.

Module 11 · Smart Cards (2 h)

- Multi-factor authentication (MFA).
- Enrollment agents.

Hands-on lab — Smart card and YubiKey token authentication.

Module 12 · Use Cases & Conclusion (4 h)

- Certificate-based VPN.
- PKI best practices.
- PKI audit.

Hands-on lab — SSTP VPN, end-to-end validation.

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.