+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 08/19/2026

Sign Up

PKI Training

2 days (14 hours)

Overview

PKI, or Public Key Infrastructure, secures digital identities, communications, and services using X.509 certificates, asymmetric cryptography, and controlled key management.

Our PKI training will provide you with a practical understanding of the trust mechanisms essential for securing IT environments. You will learn to distinguish between the roles of a certificate authority, a registration authority, and the various components involved in the certificate lifecycle.

You will study the structure of X.509 certificates, the uses of key pairs, certificate chains, extensions, certificate policies, and the validation mechanisms used by applications and infrastructures.

The training will guide you in designing a PKI architecture tailored to your organization’s needs, with a particular focus on the certificate hierarchy, private key protection, certificate issuance, and renewal.

Upon completion of the training, you will be able to manage the certificate lifecycle, configure issuance templates, handle revocation via CRLs and OCSP, and apply security best practices to ensure the reliability of a PKI in a professional environment.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the principles of asymmetric cryptography and digital trust.

- Identify the components, roles, and architectures of a PKI.
- Analyze the structure and uses of X.509 certificates.
- Configure the issuance and deployment of certificates using AD CS.
- Manage certificate renewal, revocation, and validation.
- Apply best practices for securing keys and certification services.

Target Audience

- System Administrator
- Security administrator
- Infrastructure engineer
- Cybersecurity engineer
- Security architect

Prerequisites

- Knowledge of TCP/IP networks and DNS protocols.
- Experience administering Windows Server systems.
- Basic understanding of Active Directory administration and account management.
- Basic knowledge of encryption, authentication, and access control concepts.

Technical Prerequisites

- A computer running Windows 10 or Windows 11, with installation privileges if the exercises are completed locally.
- A stable Wi-Fi or Ethernet connection to access training resources.
- A modern web browser, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.
- Access to a lab environment including Windows Server 2022, Active Directory, and AD CS, provided or set up according to the training terms.

Our PKI Training Curriculum

[Day 1 - Morning]

Fundamentals of PKI and Digital Trust

- Principles of symmetric and asymmetric cryptography.
- Hash functions, digital signatures, encryption, and authentication.
- Definition of a PKI and overview of its security objectives.
- Roles of the certificate authority, registration authority, and end entities.
- Use cases for certificates in TLS, VPNs, email, Wi-Fi, and authentication.
- Hands-on workshop: Analyzing a key pair and identifying the security information in a certificate.

[Day 1 - Afternoon]

X.509 Certificates and Certification Architecture

- Structure of an X.509 certificate, subject, issuer, serial number, and validity period.
- Critical extensions, key uses, EKU, subject alternative names, and certificate policies.
- Certificate chains, trust stores, and certificate path validation.
- Designing a hierarchy with an offline root authority and subordinate certificate authorities.
- Selection of algorithms, key sizes, validity periods, and private key protection.
- Hands-on workshop: Designing a two-tier PKI architecture for a business scenario.

[Day 2 - Morning]

Certificate Issuance and Deployment

- Overview of Active Directory Certificate Services and its components.
- Installing and configuring an enterprise certificate authority.
- The role of certificate templates in issuance, usage, and permissions.
- Certificate requests, manual enrollment, auto-enrollment, and integration with Active Directory.
- Deploying certificates for servers, users, and workstations.
- Hands-on workshop: Create a server certificate template, publish it, and issue a test certificate.

[Day 2 - Afternoon]

Lifecycle, revocation, and operational security

- Certificate lifecycle management, renewal, replacement, and archiving.
- Causes and processes for certificate revocation.
- How CRLs, distribution points, and the OCSP protocol work.
- Access control, logging, backup, and restoration of certification services.
- Best practices for monitoring, auditing, and protecting the certification authority’s keys.
- Hands-on workshop: revoking a certificate, publishing a CRL, and verifying its validation status.

Relevant companies

This training program is designed for both individuals and businesses—large and small—that wish to train their teams in new, advanced IT technologies or to acquire specific industry knowledge or modern methods.

Placement Assessment at the Start of Training

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also enables us to anticipate certain connection issues or

internal security issues within the company (in-house or virtual classroom) that could hinder the monitoring and smooth running of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.