



18-HOUR INTENSIVE HANDS-ON WORKSHOP

ENTERPRISE PKI & MICROSOFT AD CS

Architecture, Deployment, Enrollment,
Operations and Security

A structured learning programme covering enterprise certificate services from cryptographic foundations and CA hierarchy design through enrollment, revocation, NDES, recovery, hardening and diagnostics.

18 Hours

DURATION

6 Modules

CURRICULUM

Hands-On

DELIVERY

PUBLIC KEY INFRASTRUCTURE

Microsoft Active Directory Certificate Services | Student Course Guide

Be Wise. Be Secure.

PROGRAMME OVERVIEW

Build enterprise PKI capability

A focused path from first principles to operational confidence.

Public Key Infrastructure underpins trusted identities, encrypted communications and certificate-based access across modern enterprises. This workshop develops the knowledge required to understand, deploy and operate Microsoft Active Directory Certificate Services in a controlled enterprise environment.

Learning outcomes

- Explain symmetric and asymmetric cryptography, hashing and key-pair operations.
- Read X.509 certificate fields and interpret KU, EKU and trust chains.
- Design and deploy a secure offline Root CA with an online Issuing CA.
- Create templates and configure manual and automatic certificate enrollment.
- Publish and validate CRLs, AIA paths and OCSP responses.
- Plan backup, migration, NDES integration, auditing and role separation.
- Use certutil and certreq to diagnose certificate and enrollment failures.

Course at a glance

Duration
18 instructional hours

Format
6 sessions x 3 hours

Approach
Concepts, demonstration and guided practice

Who should attend

- Windows and Active Directory administrators
- IAM, PAM and security engineers
- Infrastructure and network professionals
- SOC and blue-team analysts
- Cybersecurity learners moving into enterprise PKI

Recommended preparation

Participants should be familiar with basic Windows Server administration, Active Directory concepts, DNS and IP networking. Prior PKI experience is not required. Comfort with administrative consoles and PowerShell is helpful.

LEARNING LEVEL Foundation to operational intermediate

CURRICULUM

Foundations and CA architecture

Understand the trust model before deploying certificate services.

01

PKI Fundamentals & Cryptography

CRYPTOGRAPHIC FOUNDATIONS AND CERTIFICATE TRUST

- Symmetric and asymmetric encryption: where each model is used and how hybrid encryption works.
- Hashing algorithms, integrity, digital signatures and public/private key pairs.
- X.509 certificate structure: Subject, Issuer, serial number, validity, SAN and signature fields.
- Key Usage (KU) and Extended/Enhanced Key Usage (EKU) for application-specific certificate use.
- CA trust chains, trust anchors and certificate hierarchy baselines.

PRACTICAL FOCUS

Inspect certificate properties and trace a certificate chain using Windows certificate tools.

02

Architecture & CA Deployment

TWO-TIER AND THREE-TIER HIERARCHY DESIGN

- Two-tier and three-tier PKI models, separation of duties and hierarchy decisions.
- Secure standalone Offline Root CA separated from the active Online Issuing CA.
- CAPolicy.inf installation settings, certificate validity and policy configuration.
- Path-length constraints and controls that restrict subordinate CA creation.
- Hierarchy validation and baseline configuration for secure certificate issuance.

PRACTICAL FOCUS

Configure CAPolicy.inf and follow the deployment sequence for an Offline Root CA and Online Issuing CA.

CURRICULUM

Enrollment and certificate validation

Move from controlled issuance to reliable lifecycle validation.

03

Certificate Templates & Enrollment

POLICY-DRIVEN CERTIFICATE DELIVERY

- Create, duplicate and manage version 2, version 3 and version 4 certificate templates.
- Configure compatibility, cryptography, subject naming, KU/EKU and enrollment permissions.
- Use Active Directory Auto-Enrollment for background user and computer certificate delivery.
- Perform manual enrollment through Certificate Management Console (MMC).
- Understand Certificate Web Enrollment capabilities and limitations.

PRACTICAL FOCUS

Create purpose-specific templates and test both interactive and automatic enrollment workflows.

04

Revocation & Validation Mechanisms

CRL, AIA AND OCSP SERVICE DESIGN

- Construct CRL Distribution Point (CDP) locations and publish Certificate Revocation Lists.
- Design highly available HTTP publication paths for relying-party access.
- Configure Authority Information Access (AIA) for issuing-CA certificate discovery.
- Deploy an Online Responder and configure OCSP for near real-time, low-bandwidth validation.
- Validate certificate chains, publication paths and revocation status.

PRACTICAL FOCUS

Publish CRL and AIA objects, configure OCSP and confirm that client validation paths are healthy.

CURRICULUM

Operations, integration and security

Protect the CA throughout recovery, change and incident response.

05

Advanced Operations, Maintenance & Hybrid Integration

RECOVERY, MIGRATION AND NDES

- Develop backup strategies for the CA database, registry configuration and private keys.
- Plan disaster recovery, restoration evidence and recovery testing.
- Migrate legacy Cryptographic Service Providers (CSPs) to modern Key Storage Providers (KSPs).
- Understand CA operating-system upgrade and migration considerations.
- Configure Network Device Enrollment Service (NDES) for SCEP-capable network appliances.

PRACTICAL FOCUS

Create a CA backup plan, review migration controls and map the NDES service and enrollment flow.

06

Security Hardening & Troubleshooting

GOVERNANCE, AUDIT AND DIAGNOSTICS

- Separate CA Administrator and Certificate Officer responsibilities.
- Configure auditing and identify security-critical certificate-service events.
- Review permissions, administrative boundaries and operational accountability.
- Use certutil to inspect CA configuration, certificates, CRLs and trust-chain failures.
- Use certreq to diagnose template matching, request submission, enrollment and expiration problems.

PRACTICAL FOCUS

Enable audit controls and investigate controlled certificate and enrollment failures with certutil and certreq.

18-HOUR LEARNING JOURNEY

Six focused learning sessions

6 sessions x 3 hours | 18 instructional hours in total

SESSION 1 | 3 HOURS | MODULE 1**PKI fundamentals & cryptography**

- Encryption, hashing, signatures and key pairs
- X.509 fields, KU/EKU and trust chains

PRACTICAL FOCUS

Inspect certificates and trace a trust chain.

SESSION 2 | 3 HOURS | MODULE 2**Architecture & CA deployment**

- Two-tier and three-tier hierarchy design
- Offline Root, Issuing CA and CAPolicy.inf

PRACTICAL FOCUS

Deploy and validate the CA hierarchy.

SESSION 3 | 3 HOURS | MODULE 3**Templates & enrollment**

- Template versions 2, 3 and 4; permissions
- MMC, auto-enrollment and Web Enrollment

PRACTICAL FOCUS

Create templates and test certificate delivery.

SESSION 4 | 3 HOURS | MODULE 4**Revocation & validation**

- CRL/CDP and highly available publication
- AIA discovery and OCSP Online Responder

PRACTICAL FOCUS

Validate chains, publication and revocation.

SESSION 5 | 3 HOURS | MODULE 5**Operations, recovery & NDES**

- CA backup, recovery and OS migration
- CSP-to-KSP transition; NDES/SCEP flow

PRACTICAL FOCUS

Review recovery controls and NDES integration.

SESSION 6 | 3 HOURS | MODULE 6**Hardening & troubleshooting**

- Role separation, auditing and permissions
- certutil and certreq diagnostic workflows

PRACTICAL FOCUS

Investigate certificate and enrollment failures.

Applied learning experience

Each 3-hour session combines concepts, instructor demonstrations and guided practice. The sequence builds from cryptographic foundations to deployment, certificate lifecycle management, secure operations and diagnosis.

TOOLS AND INTERFACES

Active Directory Certificate Services | MMC certificate consoles | PowerShell | certutil | certreq | Online Responder | NDES

YOUR CAPABILITY AFTER THE WORKSHOP

Operate PKI with stronger judgement

A clear operational foundation for Microsoft enterprise certificate services.

1

Interpret certificates

Read core X.509 fields, KU/EKU, algorithms, validity and trust-chain relationships.

2

Design the hierarchy

Explain offline-root separation and make informed two-tier or three-tier architecture decisions.

3

Control enrollment

Build purpose-specific templates and select secure manual or automatic delivery methods.

4

Validate trust

Assess CRL, AIA and OCSP health and understand how clients discover validation data.

5

Protect operations

Plan CA backup, migration, NDES integration, role separation and audit evidence.

6

Diagnose failures

Use certutil and certreq to investigate enrollment, template, chain and expiration problems.



WISEMAN CYBERSEC
BE WISE, BE SECURE

Ready to build trusted infrastructure?

Enterprise PKI & Microsoft AD CS
18-Hour Intensive Hands-On Workshop

CONNECT WITH WISEMAN CYBERSEC

www.wisemancybersec.com | info@wisemancybersec.com