

PKI Workshop – Enterprise Public Key Infrastructure & Certificate Services

Hero Section

PKI Workshop – Enterprise Public Key Infrastructure & Microsoft AD CS

Duration: [XX Hours] of Live Instructor-Led Training

Format: Live Virtual Sessions + Guided Hands-On Labs + Interactive Q&A

Instructor: Senior PKI / Windows Security Professional with Enterprise Experience

Post Training: Practical Exercises, Lab Practice, Troubleshooting Scenarios & Continued Learning Support

CTA: Talk to an Expert

CTA: Download Course PDF

Upcoming Batch Details

Training Program: PKI Workshop

Start Date: [Add Batch Start Date]

Duration: [XX Hours]

Timing (IST): [Add Timing]

Mode: Live Online Instructor-Led Training

Enrollment: Enroll Now

Course Overview

The **PKI Workshop** is a practical, instructor-led training program designed to help IT and cybersecurity professionals understand, deploy, manage, secure, and troubleshoot enterprise Public Key Infrastructure (PKI).

The workshop takes participants from the fundamentals of cryptography and digital certificates to real-world PKI architecture, Certificate Authority deployment, certificate templates, auto-enrollment, revocation mechanisms, OSCP, disaster recovery, migration, NDES, security hardening, and advanced troubleshooting.

A major focus of the program is understanding how enterprise certificate services operate in real environments. Participants will learn how to design secure Certificate Authority hierarchies, configure offline Root CAs and online Issuing CAs, manage certificate templates, automate certificate enrollment, configure certificate validation infrastructure, and diagnose common PKI issues.

The training combines conceptual understanding with practical administration so that participants understand not only **how PKI works**, but also **how to operate and maintain a production-ready PKI environment securely**.

What You Will Learn

PKI & Cryptography Fundamentals

Understand the core principles behind symmetric and asymmetric encryption, hashing, public/private key pairs, digital signatures, and certificate-based trust.

Digital Certificates & X.509

Understand the structure of X.509 digital certificates and important certificate attributes including **Key Usage (KU)**, **Enhanced Key Usage (EKU)**, **certificate validity**, **subject information**, and **trust chains**.

Enterprise CA Architecture

Learn how to design secure **two-tier and three-tier Certificate Authority architectures**, including a protected Offline Root CA and enterprise Online Issuing CAs.

Certificate Templates & Enrollment

Create and manage enterprise certificate templates and understand certificate enrollment methods including **Active Directory Auto-Enrollment**, **MMC-based enrollment**, and **web enrollment**.

Certificate Revocation & Validation

Configure and understand **Certificate Revocation Lists (CRL)**, **CRL Distribution Points (CDP)**, **Authority Information Access (AIA)**, and **Online Certificate Status Protocol (OCSP)**.

PKI Operations & Disaster Recovery

Learn how to protect and maintain PKI environments through CA backups, database protection, private-key protection, migration strategies, and recovery planning.

NDES & Network Device Certificates

Understand and configure the **Network Device Enrollment Service (NDES)** for certificate enrollment requirements involving network devices and appliances.

PKI Security Hardening

Implement administrative role separation, security auditing, access controls, operational security, and other measures required to protect critical Certificate Authority infrastructure.

Advanced PKI Troubleshooting

Use tools such as **certutil** and **certreq** to investigate certificate enrollment problems, template issues, validation errors, certificate expiration, trust-chain problems, and other common PKI failures.

Why Wiseman CyberSec

Personalized Learning Experience

We maintain focused batch sizes to encourage interaction, personalized mentorship, live troubleshooting, and proper attention to every participant.

Flexible Redo & Retake Option

Missed a session because of professional or personal commitments? Eligible learners can attend relevant sessions with upcoming batches to strengthen their understanding.

LMS Access with Recorded Sessions

Participants receive access to learning resources and recorded sessions through our LMS, allowing them to revisit important concepts and demonstrations after the live training.

Continuous Post-Training Support

Learning does not stop when the workshop ends. Participants receive continued support through dedicated communication channels, learning resources, community discussions, and mentor guidance.

Join an Active Cybersecurity Community

Become part of the Wiseman CyberSec learning community and gain access to cybersecurity discussions, expert sessions, masterclasses, podcasts, webinars, and networking opportunities.

Learn from Real Industry Professionals

Our training is delivered by professionals with practical industry exposure who focus on real enterprise architectures, operational challenges, tools, configurations, and troubleshooting scenarios.

Practical & Industry-Focused Training

The workshop focuses on practical implementation and real-world use cases rather than theory alone, helping participants understand how PKI is actually designed and managed within enterprise environments.

Who Should Enroll

Windows / Active Directory Administrators

Professionals managing Windows Server, Active Directory, Group Policy, identity infrastructure, or enterprise Windows environments who want to develop practical PKI expertise.

Identity & Access Management Professionals

IAM engineers, architects, and administrators who work with certificate-based authentication, machine identities, privileged access, authentication systems, or enterprise identity infrastructure.

Cybersecurity Engineers & Analysts

Security professionals who want to understand certificate-based security, cryptographic trust, digital identities, certificate validation, and PKI security controls.

Infrastructure & Network Engineers

Infrastructure and networking professionals responsible for servers, network devices, VPNs, wireless authentication, secure communication, or certificate-enabled infrastructure.

Security Architects & Consultants

Professionals involved in designing or reviewing enterprise security architectures who need a strong practical understanding of Certificate Authorities, trust models, certificate lifecycle management, and PKI security.

IT & Security Professionals Moving into PKI

Professionals looking to specialize in PKI, certificate services, enterprise identity security, Windows security, or cryptographic infrastructure.

Course Curriculum

Module 1: PKI Fundamentals & Cryptography

Build a strong foundation in the cryptographic principles that power Public Key Infrastructure.

Topics Covered:

- Introduction to Public Key Infrastructure
- Role of PKI in enterprise security
- Symmetric vs. asymmetric encryption

- Public and private key pairs
 - Hashing algorithms and their purpose
 - Digital signatures and certificate-based trust
 - Introduction to digital certificates
 - Understanding X.509 certificates
 - Certificate fields and attributes
 - Key Usage (KU)
 - Enhanced Key Usage (EKU)
 - Understanding Certificate Authorities
 - Root CA and Subordinate CA concepts
 - Certificate trust chains
 - Enterprise PKI trust models
 - Designing CA hierarchy baselines
-

Module 2: PKI Architecture & Certificate Authority Deployment

Learn how enterprise PKI environments are structured and how Certificate Authorities are securely deployed.

Topics Covered:

- Enterprise PKI architecture
 - Understanding Root and Issuing CAs
 - One-tier, two-tier and three-tier PKI architectures
 - Designing a secure CA hierarchy
 - Standalone vs. Enterprise Certificate Authorities
 - Building an Offline Root CA
 - Deploying an Online Issuing CA
 - Protecting the Root CA
 - CA hierarchy security considerations
 - Introduction to CAPolicy.inf
 - Configuring CAPolicy.inf
 - Customizing Certificate Authority installation settings
 - Configuring certificate policy parameters
 - Defining CA path lengths
 - Applying subordinate CA constraints
 - PKI architecture planning and deployment considerations
-

Module 3: Certificate Templates & Enrollment

Learn how certificates are requested, issued, distributed, and managed throughout the enterprise.

Topics Covered:

- Understanding certificate templates
 - Certificate template architecture
 - Managing Version 2 certificate templates
 - Managing Version 3 certificate templates
 - Managing Version 4 certificate templates
 - Creating and duplicating certificate templates
 - Configuring certificate template settings
 - Template permissions and enrollment requirements
 - User certificates
 - Computer certificates
 - Certificate enrollment workflows
 - Active Directory certificate enrollment
 - Configuring Auto-Enrollment
 - Automatic certificate deployment to users
 - Automatic certificate deployment to computers
 - Group Policy-based certificate enrollment
 - Manual certificate enrollment
 - Certificate Management Console (MMC)
 - Web-based certificate enrollment
 - Understanding certificate requests and issuance
-

Module 4: Certificate Revocation & Validation Mechanisms

Understand how systems determine whether certificates remain valid and trustworthy.

Topics Covered:

- Certificate validation process
- Understanding certificate revocation
- Certificate Revocation Lists (CRLs)
- CRL publication and management
- CRL Distribution Points (CDP)
- Designing CDP locations
- Publishing CRLs through HTTP
- High-availability considerations for CRL distribution
- Authority Information Access (AIA)
- Configuring AIA locations
- Certificate chain discovery
- Certificate chain validation
- Introduction to Online Certificate Status Protocol (OCSP)
- Understanding Online Responders

- Configuring an OCSP Online Responder
 - Near real-time certificate validation
 - CRL vs. OCSP
 - Troubleshooting certificate validation problems
-

Module 5: Advanced PKI Operations, Maintenance & Hybrid Integration

Learn how to operate, maintain, recover, migrate, and extend enterprise PKI environments.

Topics Covered:

PKI Backup & Disaster Recovery

- Understanding PKI disaster-recovery requirements
- Backing up the Certificate Authority
- CA database backup
- CA registry configuration backup
- Protecting and backing up CA private keys
- CA restoration considerations
- Developing a PKI recovery strategy

PKI Migration & Upgrade

- Planning Certificate Authority migrations
- Understanding Cryptographic Service Providers (CSP)
- Understanding Key Storage Providers (KSP)
- Migrating from legacy CSPs to modern KSPs
- PKI operating-system upgrade considerations
- Maintaining certificate trust during migrations
- PKI migration planning and validation

NDES Configuration

- Introduction to Network Device Enrollment Service
 - Understanding NDES architecture
 - NDES use cases
 - Configuring Network Device Enrollment Service
 - Certificate enrollment for network devices and appliances
 - Understanding certificate enrollment workflows involving NDES
-

Module 6: PKI Security Hardening & Troubleshooting

Learn how to securely operate PKI infrastructure and diagnose problems encountered in enterprise environments.

PKI Security & Administrative Controls

- Securing Certificate Authorities
- Administrative role separation
- CA Administrator responsibilities
- Certificate Manager / Officer responsibilities
- Segregation of administrative duties
- Principle of least privilege
- PKI administrative access controls
- Security auditing
- Logging critical Certificate Authority events
- Monitoring PKI operations
- Protecting critical CA services

Advanced PKI Troubleshooting

- PKI troubleshooting methodology
- Understanding certificate-chain failures
- Troubleshooting enrollment failures
- Troubleshooting certificate template matching
- Certificate expiration problems
- Certificate validation problems
- Revocation-checking issues
- Using `certutil`
- Using `certreq`
- Certificate store diagnostics
- Verifying certificate chains
- Investigating enrollment requests
- Troubleshooting common enterprise PKI issues

Training Format & Delivery

The **PKI Workshop** is delivered through live, instructor-led virtual sessions designed for working IT and cybersecurity professionals.

The workshop combines:

- Instructor-led conceptual sessions
- Live PKI demonstrations
- Guided configuration exercises
- Hands-on administrative activities
- Enterprise deployment scenarios
- Troubleshooting exercises
- Interactive Q&A and discussion

Participants learn each major PKI concept and then see how it is implemented and managed within an enterprise environment.

Training Mode: Live Online Instructor-Led

Duration: [XX Hours]

Schedule: [Weekend / Weekday – Add Final Schedule]

Session Timing: [Add Timing]

What to Expect

This workshop is designed to be interactive and implementation-focused rather than lecture-only.

The instructor will demonstrate the configuration and administration of enterprise PKI components while explaining the security and architectural decisions behind each configuration.

Participants will explore practical scenarios involving:

- Certificate Authority architecture
- Root and Issuing CA deployment
- Certificate templates
- Certificate enrollment
- Auto-Enrollment
- Certificate revocation
- CRL and AIA configuration
- OCSP
- PKI backup and recovery
- NDES
- Security hardening
- PKI troubleshooting

Participants will also be able to discuss their questions and real-world PKI challenges directly with the instructor.

Hands-On Experience

PKI is best understood by working directly with certificates, Certificate Authorities, trust chains, enrollment mechanisms, and validation infrastructure.

The workshop therefore places a strong emphasis on practical learning.

Participants will work through scenarios involving enterprise Certificate Authority infrastructure and learn how to:

- Understand and inspect X.509 certificates
- Build certificate trust chains
- Design a CA hierarchy
- Configure an Offline Root CA
- Work with an Online Issuing CA
- Configure CAPolicy.inf
- Create and manage certificate templates
- Configure certificate Auto-Enrollment
- Perform manual certificate enrollment
- Configure CRL Distribution Points
- Configure Authority Information Access
- Work with OCSP validation
- Understand PKI backup and recovery
- Work with NDES concepts and configuration
- Audit Certificate Authority activities
- Diagnose problems using certutil and certreq

By the end of the workshop, participants should be able to understand the complete certificate lifecycle—from certificate request and issuance through validation, renewal, revocation, expiration, and troubleshooting.

Practical & Career-Focused Learning

Enterprise PKI is an important component of identity security, authentication, encrypted communications, device security, digital signatures, and Zero Trust architectures.

This workshop is designed to help professionals build practical skills that can be applied to roles involving:

- PKI Administration
- PKI Engineering
- PKI Architecture
- Identity & Access Management
- Microsoft / Windows Security
- Active Directory Security

- Infrastructure Security
- Information Security Engineering
- Certificate Lifecycle Management
- Enterprise Security Architecture

The training also helps existing system, IAM, network, infrastructure, and cybersecurity professionals add deeper PKI expertise to their current roles.

Frequently Asked Questions

1. What is this PKI Workshop about?

The workshop covers the design, deployment, administration, security, maintenance, and troubleshooting of enterprise Public Key Infrastructure. Topics range from cryptography and X.509 certificates to Certificate Authority deployment, templates, Auto-Enrollment, CRL, AIA, OCSP, disaster recovery, NDES, hardening, and troubleshooting.

2. Who should attend this workshop?

The workshop is suitable for Windows and Active Directory administrators, IAM professionals, infrastructure engineers, network engineers, security engineers, security architects, consultants, and other IT professionals who work with or want to specialize in enterprise PKI.

3. Do I need prior PKI experience?

Prior PKI experience is not mandatory. The workshop begins with PKI and cryptography fundamentals before progressing into enterprise architecture and advanced administration.

Basic familiarity with Windows Server, Active Directory, networking, or cybersecurity will help participants follow the technical exercises more effectively.

4. Is this workshop hands-on?

Yes. The training is designed around practical demonstrations, configuration exercises, deployment scenarios, and troubleshooting activities rather than theory alone.

5. What PKI technologies and components are covered?

The workshop covers enterprise Certificate Authorities, X.509 certificates, certificate templates, Active Directory Auto-Enrollment, CRL, CDP, AIA, OCSP, CAPolicy.inf, NDES, CSP/KSP migration, and command-line utilities including certutil and certreq.

6. Will I learn how to build a Certificate Authority hierarchy?

Yes. Participants will understand secure enterprise PKI architecture, including two-tier and three-tier designs, Offline Root CAs, Online Issuing CAs, CA hierarchy planning, and CAPolicy.inf configuration.

7. Does the training cover certificate Auto-Enrollment?

Yes. The workshop covers Active Directory-based Auto-Enrollment for automatically issuing and deploying certificates to eligible users and computers.

8. Are CRL, AIA and OCSP covered?

Yes. Certificate revocation and validation are key components of the workshop. Participants will understand CRL Distribution Points, Authority Information Access, certificate-chain validation, and Online Certificate Status Protocol.

9. Does the workshop cover PKI backup and disaster recovery?

Yes. Participants will learn the major components that must be protected in a Certificate Authority environment, including the CA database, registry configuration, and CA private keys, along with recovery planning considerations.

10. Is NDES included?

Yes. The workshop introduces and covers the configuration of **Network Device Enrollment Service (NDES)** for certificate enrollment use cases involving supported network devices and appliances.

11. Will troubleshooting be covered?

Yes. Troubleshooting is an important part of the workshop. Participants will work with tools such as **certutil** and **certreq** and learn how to investigate enrollment errors, certificate-template problems, trust-chain failures, expiration problems, and certificate-validation issues.

12. Will recordings be provided?

Participants will receive access to recorded sessions and supporting learning resources through the Wiseman CyberSec learning platform, subject to the training program's applicable access policy.

13. Is post-training support available?

Yes. Wiseman CyberSec provides continued learning support through community interactions, learning resources, mentor guidance, and doubt-resolution opportunities after the training.

Closing CTA Section

Build Practical Enterprise PKI Skills

Learn how to **design, deploy, manage, secure, maintain, and troubleshoot enterprise Public Key Infrastructure** through practical instructor-led training.

Master Enterprise PKI from Fundamentals to Advanced Administration

- Understand PKI & cryptography
- Build secure CA hierarchies
- Configure certificate templates
- Implement Auto-Enrollment
- Manage CRL, AIA & OCSP
- Configure NDES
- Plan backup, recovery & migrations
- Harden Certificate Authorities
- Troubleshoot using certutil & certreq
- Learn through real-world enterprise scenarios

CTA Button: Secure My PKI Workshop Seat

Suggested Website Course Name

PKI Workshop – Enterprise PKI & Microsoft AD CS

Alternative shorter name:

Enterprise PKI Hands-On Workshop

Suggested Short Course Description

Learn how to design, deploy, manage, secure, and troubleshoot enterprise Public Key Infrastructure through hands-on training covering Certificate Authorities, X.509 certificates, certificate templates, Auto-Enrollment, CRL, AIA, OCSP, NDES, disaster recovery, migrations, security hardening, certutil, and certreq.

SEO Title

PKI Training & Workshop | Enterprise PKI & Microsoft AD CS | Wiseman CyberSec

Meta Description

Learn Enterprise PKI through live hands-on training covering Certificate Authorities, X.509 certificates, certificate templates, Auto-Enrollment, CRL, AIA, OCSP, NDES, PKI security, disaster recovery, and troubleshooting.

Suggested URL Slug

/pki-workshop/

or

/enterprise-pki-training/