Faysal Aziz

# Enterprise PKI and Certificate Lifecycle Management

## Design trusted infrastructure. Automate certificate operations.

FA-0832 · 2 days

Cybersecurity · DevOps, Cloud & Infrastructure

Connect enterprise PKI architecture with practical AD CS, certificate discovery, renewal automation and cross-platform operational controls.

---

## Introduction

Certificates connect applications, servers, devices, and services through a shared foundation of trust. Managing them across an enterprise requires coordination between certificate authorities, infrastructure teams, application owners, and security operations. A certificate can be issued successfully while its deployment, ownership, renewal, or revocation remains unmanaged. These operational gaps create avoidable outages, manual work, and audit challenges.

This course brings enterprise Public Key Infrastructure (PKI) and Certificate Lifecycle Management (CLM) together through architecture, cross-platform operations, and automation. Participants explore how certificate discovery, enrollment, deployment, renewal, and governance fit into a consistent operating model across Windows, Linux, and hybrid infrastructure. Microsoft AD CS, Windows/IIS operations, and EJBCA integration provide practical context, while ACME, SCEP, EST, and API-based workflows establish the foundations for interoperable automation.

The course follows vendor-neutral principles applicable across enterprise CLM platforms such as AppViewX, CyberArk/Venafi, Keyfactor, and DigiCert. It emphasises how teams can reduce repetitive tasks, improve certificate visibility, establish clear ownership, and verify that automated workflows produce the intended operational result.

## Learning outcomes

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

- Explain enterprise PKI trust models and certificate lifecycle dependencies.
- Map the components, trust boundaries, and integrations of an enterprise CLM architecture.
- Perform certificate enrollment, deployment, and renewal operations in prepared Windows/IIS and Linux environments.
- Explain AD CS and third-party CA integration approaches.
- Select appropriate enrollment methods using ACME, SCEP, EST, and APIs.
- Define certificate discovery, inventory, ownership, and monitoring requirements.
- Design renewal and deployment automation with validation and failure handling.
- Identify key protection, revocation, RBAC, and audit controls.
- Prioritise automation opportunities and measure their operational benefits.

# Prerequisites

- Working experience administering Windows Server or Linux, including services, permissions, and system logs.
- Ability to independently troubleshoot DNS resolution, TCP connectivity, and HTTPS access.
- A laptop or workstation with a current browser, an SSH client, and a Remote Desktop client.
- Internet access permitted for the selected training tools.
- Permission and connectivity to use SSH with the designated training systems.
- Ability to establish Remote Desktop connections to the provided Windows training environment.

# Training outline

## 1. Enterprise PKI and Certificate Lifecycle Foundations

1. X.509 certificates, keys, CSRs, and certificate profiles
2. Root and issuing CAs, trust chains, and trust distribution
3. Public and private PKI
4. Certificate lifecycle stages and operational responsibilities
5. Certificate failure modes and business impact

## 2. Enterprise CLM Architecture

1. CA, registration authority, and CLM platform responsibilities
2. Discovery, inventory, policy, and workflow components
3. CA connectors, deployment agents, and gateways
4. Identity, secrets management, CMDB, ITSM, and SIEM integrations

5. Trust boundaries, connectivity, and availability
6. Vendor-neutral platform evaluation criteria

## 3. Microsoft AD CS and Windows/IIS Operations

1. AD CS hierarchy and certificate templates
2. Enrollment permissions and template security
3. Group Policy autoenrollment
4. Windows certificate stores and private key permissions
5. Certificate requests, imports, and PFX handling
6. IIS deployment, renewal, and certificate rebinding
7. Enrollment and deployment troubleshooting

## 4. Third-Party CA Integration and Enrollment

1. EJBCA and third-party CA integration concepts
2. Certificate profile and policy mapping
3. ACME enrollment and renewal
4. SCEP enrollment and bootstrap security
5. EST enrollment and reenrollment
6. API-based integration and protocol selection

## 5. Certificate Discovery and Inventory

1. Network, endpoint, certificate store, and CA discovery
2. Discovery coverage and visibility limitations
3. Certificate records and deployment instances
4. Application ownership and business service mapping
5. Expiry monitoring, policy exceptions, and escalation

## 6. Certificate Lifecycle Automation

1. Request, approval, issuance, and deployment workflows
2. Renewal windows, rekeying, and scheduling
3. Windows/IIS and Linux deployment automation
4. Service activation and endpoint verification
5. Retries, rollback, and exception handling

6. Automation credentials and private key protection
7. Team responsibilities and operational benefit metrics

## 7. Key Protection, Revocation, and Governance

1. HSM architecture and key custody
2. CA and application key management
3. Key backup, recovery, rotation, and destruction
4. CRL and OCSP operations
5. Compromise response and emergency replacement
6. RBAC, least privilege, and separation of duties
7. Approval controls, audit trails, and policy exceptions

## 8. Hybrid CLM Architecture and Adoption

1. On-premises, cloud, and segmented network integration
2. Windows, Linux, load balancer, and container certificate patterns
3. Multiple CA and trust-store coordination
4. Connector placement and recovery dependencies
5. Automation priorities and phased implementation
6. Architecture review and operational readiness

# Disclaimer

This course outline serves as a guideline for training planning and delivery. The trainer reserves the right to amend, reorder, expand, reduce, or otherwise modify the content and delivery approach as he considers appropriate, taking into account participant experience, organisational requirements, technical constraints, and available time, without prior notice.

© 2026 Faysal Aziz · Kuala Lumpur