Faysal Aziz

Enterprise PKI and Certificate Lifecycle Management: Foundations and Practice

Build practical foundations. Design enterprise trust. Automate certificate operations.

FA-0833 · 3 days

Cybersecurity · DevOps, Cloud & Infrastructure

Strengthen infrastructure foundations before practising enterprise PKI, AD CS, certificate lifecycle automation and operational recovery.

Introduction

Enterprise certificate management depends on more than issuing certificates. Teams must understand where certificates are deployed, who owns them, how applications use them, and what happens when renewal or deployment fails. Across Windows, Linux, network devices, and cloud services, these responsibilities connect infrastructure operations with security policy, application availability, and governance.

This course develops the practical foundations and architectural understanding needed to manage that lifecycle. It begins with a focused refresher on networking, server operations, command-line tools, and HTTPS troubleshooting. This helps participants strengthen supporting skills before progressing into enterprise PKI, Microsoft AD CS, Windows/IIS operations, and certificate lifecycle automation. Guided work in prepared environments reinforces the connection between certificate issuance, application deployment, and operational verification.

Participants explore how certificate discovery, inventory, enrollment, renewal, revocation, and audit fit into an enterprise CLM architecture. Additional depth covers CA integration, enrollment protocol selection, private key protection, automation failure handling, and hybrid infrastructure dependencies. The emphasis is on repeatable workflows that reduce manual effort, establish ownership, and improve service reliability.

The course follows vendor-neutral principles applicable across enterprise CLM platforms such as AppViewX, CyberArk/Venafi, Keyfactor, and DigiCert. Microsoft AD CS and EJBCA provide practical integration context. The initial refresher supports participants with uneven technical foundations while

retaining the working administration experience needed for the course.

Learning outcomes

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

- Apply networking, server administration, and diagnostic skills to certificate operations.
- Inspect certificates, CSRs, keys, and trust chains using Windows and Linux tools.
- Explain enterprise PKI hierarchies, certificate profiles, and trust distribution.
- Design the components, integration flows, and trust boundaries of an enterprise CLM architecture.
- Perform enrollment, deployment, renewal, and validation in prepared AD CS/IIS and Linux environments.
- Explain EJBCA and third-party CA integration through connectors, protocols, and APIs.
- Select appropriate uses for ACME, SCEP, EST, and domain-based autoenrollment.
- Establish certificate discovery, inventory, ownership, and monitoring processes.
- Develop renewal and deployment workflows with validation, retries, rollback, and escalation.
- Define HSM, key management, revocation, RBAC, and audit requirements.
- Plan a phased hybrid CLM implementation with measurable operational benefits.

Prerequisites

- Working experience administering Windows or Linux, including independently managing files, accounts, permissions, and services.
- Ability to connect to remote systems and follow administrative instructions.
- 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. Infrastructure and Troubleshooting Refresher

1. DNS resolution, ports, firewalls, and connectivity checks
2. HTTPS connections and TLS termination points
3. Windows and Linux service administration
4. File permissions, service identities, and administrative access

5. PowerShell, shell commands, and diagnostic output
6. System logs and structured troubleshooting

2. PKI and Certificate Operations Foundations

1. Public and private keys, signatures, and CSRs
2. X.509 fields, SANs, key usage, and extended key usage
3. Root and issuing CAs, trust chains, and trust anchors
4. Public and private PKI trust models
5. PEM, DER, and PKCS#12 formats
6. Certificate inspection and key matching
7. Windows, Linux, and application trust stores

3. Enterprise CLM Architecture

1. Certificate lifecycle stages and ownership
2. CA, registration authority, and CLM responsibilities
3. Discovery, inventory, policy, and workflow services
4. CA connectors, deployment agents, and gateways
5. Identity, secrets management, CMDB, ITSM, and SIEM integrations
6. Trust boundaries, service identities, and connector security
7. Availability, recovery, and platform evaluation criteria

4. Microsoft AD CS and Windows/IIS Operations

1. Enterprise CA hierarchy and enrollment architecture
2. Certificate templates, profiles, and permissions
3. Subject naming, SAN controls, and approval policies
4. Group Policy autoenrollment and renewal
5. Windows certificate stores and private key access
6. Certificate requests, imports, and PFX protection
7. IIS HTTPS bindings, SNI, and certificate rebinding
8. Enrollment, renewal, and deployment diagnostics

5. Third-Party CA Integration and Enrollment Protocols

1. EJBCA architecture and certificate profile concepts

2. Third-party CA connectors and API authentication
3. Policy and profile mapping across CAs
4. ACME accounts, challenges, issuance, and renewal
5. SCEP enrollment and bootstrap controls
6. EST authentication, enrollment, and reenrollment
7. Protocol selection and interoperability constraints

6. Certificate Discovery and Inventory Management

1. Network, endpoint, store, and CA discovery
2. Discovery scope, access controls, and visibility gaps
3. Certificate identity and deployment instance reconciliation
4. Application ownership and CMDB relationships
5. Expiry, algorithm, and policy risk classification
6. Monitoring, escalation, and inventory reconciliation

7. Automated Renewal and Deployment

1. Request, approval, issuance, and deployment orchestration
2. Renewal windows, rekeying, and scheduling
3. Windows/IIS and Linux service automation
4. API, scripting, and configuration management integration
5. Credential and private key handling
6. Idempotency, retries, and concurrent operations
7. Service activation and endpoint verification
8. Rollback, exception queues, and audit evidence

8. HSM and Enterprise Key Management

1. CA signing keys and application private keys
2. HSM trust boundaries and integration concepts
3. PKCS#11 and Windows cryptographic providers
4. Key generation, exportability, custody, and rotation
5. Dual control and separation of duties
6. Backup, recovery, and key destruction

9. Revocation and Certificate Incident Response

1. CRL publication and distribution dependencies
2. OCSP and client validation behaviour
3. Revocation limitations and short-lived certificates
4. Private key compromise and emergency replacement
5. Chain, hostname, expiry, and key mismatch diagnosis
6. Failed renewal and stale deployment investigation

10. Governance and Hybrid CLM Adoption

1. RBAC, least privilege, and approval boundaries
2. Certificate policies and time-bound exceptions
3. Audit records, reporting, and operational runbooks
4. On-premises, cloud, and segmented network patterns
5. Load balancer, container, and application integration concepts
6. Hybrid architecture review and recovery dependencies
7. Phased automation priorities and team responsibilities
8. Automation coverage, renewal success, and service reliability metrics

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