CONCEPT

Public Key Infrastructure (PKI) Training: Certificate Lifecycle, HSMs and Applied Cryptography



Public Key Infrastructure (PKI) Training: Certificate Lifecycle, HSMs and Applied Cryptography

Introduction:

Public Key Infrastructure PKI training on certificate lifecycle, HSMs and applied cryptography is a one-week course for security architecture, infrastructure, identity and e-service teams, ending in a PKI Design and Certificate Management Policy. Expired certificates that halt e-services, poorly guarded issuing keys and weak revocation checking leave organisations unable to prove which servers, devices and documents to trust. Participants already run servers, directories or security controls at work, and learn through hands-on labs with certificate authorities, key stores and validation tools. CoreConcept Training Center delivers this course in public key infrastructure.

Course Objectives:

- Select symmetric ciphers, key pairs, hash functions and signature schemes suited to each protection need in a system design
- Design a root and issuing certificate authority hierarchy with registration authority roles, a certificate policy and a CPS
- Operate certificate enrolment, renewal and revocation with CRL and OCSP checking and ACME automation across large server estates
- Specify hardware security module use, key ceremonies and key rotation schedules that protect issuing and signing keys
- Apply certificates to code signing, signed document validation and device identity while preparing audit evidence for trust services
- Produce a PKI Design and Certificate Management Policy with a crypto-agility and post-quantum migration inventory for a case organisation

Target Audience:

- Security architecture staff who define encryption, signing and trust requirements for new systems and e-services
- Infrastructure and server operations staff who install, renew and troubleshoot TLS certificates and load balancers
- PKI and certificate authority operations staff who issue, revoke and audit certificates and guard CA keys
- Identity and directory staff who rely on certificates for smart cards, device authentication and federation trust
- E-service and application delivery staff who sign code, documents and transactions in citizen and customer channels

Course Outline:

Day 1: Applied Cryptography Foundations and Certificate Estate Assessment

- Symmetric Ciphers and Authenticated Encryption Modes for Data Protection
- RSA and Elliptic Curve Key Pairs for Asymmetric Operations
- Hash Functions, Message Authentication Codes and Integrity Checks
- Digital Signature Creation and Verification Using Private and Public Keys
- Certificate Estate Discovery Scan and Current-State Trust Inventory

Day 2: PKI Architecture, Certificate Policy and Trust Models

- X.509 Certificate Fields, Extensions and Path Validation Rules
- Root, Policy and Issuing CA Hierarchy Design Options
- Registration Authority Vetting Workflows and Validation Authority Roles
- RFC 3647 Certificate Policy and CPS Document Structure
- Offline Root Key Ceremony Planning with M of N Custodians

Day 3: Certificate Lifecycle Operations, HSMs and Key Management

- Certificate Enrolment Requests, CSR Generation and Issuance Approval Steps
- ACME Protocol Automation for TLS Certificate Renewal at Scale
- CRL Publication and OCSP Responder Design for Revocation Checking
- Hardware Security Module Partitioning, Backup and FIPS 140 Validation
- SP 800-57 Key States, Cryptoperiods and Rotation Schedules

Day 4: Code Signing, Device Identity, Trust Services and Crypto-Agility

- Code Signing Certificates, Timestamping and Software Release Pipelines
- Signed Document Validation Reports and Long-Term Signature Preservation
- Device and IoT Certificate Provisioning at Manufacture and Onboarding
- Baseline Requirements Audit Readiness for Publicly Trusted TLS Issuance
- SP 800-131A Algorithm Transitions and Post-Quantum Migration Inventory

Day 5: Lab Work and the PKI Design and Certificate Management Policy

- Case Organisation Brief Covering E-Services, Devices and Internal Applications
- Lab Build of a Two-Tier CA Hierarchy and HSM Plan
- Certificate Expiry Outage Root Cause Review and Renewal Runbook
- Revocation and Compromise Response Playbook for Issuing CA Keys
- PKI Design and Certificate Management Policy Completion and Peer Review

Skills You Will Gain:

- Cryptographic Primitive Selection
- CA Hierarchy Architecture
- Certificate Policy and CPS Authoring
- Certificate Lifecycle Automation
- Revocation Service Design
- HSM Key Custody
- Code and Document Signature Validation
- Crypto-Agility Planning

Why Attend This Course:

- Deliver a PKI Design and Certificate Management Policy to the security architecture board and the infrastructure head for approval
- Decide which systems need a private issuing CA, a publicly trusted certificate or an HSM-protected signing key
- Avoid service outages from expired certificates and the cost of reissuing trust after an unprotected CA key is exposed
- Coach server, application and identity colleagues on enrolment, renewal and revocation routines using the lab runbooks

Conclusion:

Once participants return, the security architecture board can use the PKI Design and Certificate Management Policy to approve the CA hierarchy, HSM purchases and certificate ownership across e-services, servers and devices. Infrastructure and application owners gain one renewal and revocation routine instead of ad hoc fixes. After the first full renewal cycle or the first external audit, the unit should review expiry incidents, revocation response times and the cryptographic inventory, then adjust key lengths, automation coverage and the migration plan.

Frequently Asked Questions FAQ:

What should participants know before Public Key Infrastructure PKI training?

Participants should already administer servers, directories, applications or security controls and understand basic networking and TLS connections. No mathematics beyond everyday arithmetic is needed; cryptographic concepts are explained through hands-on lab tasks with certificate authorities, key stores and validation tools.

How does Public Key Infrastructure PKI training differ from an electronic signature law or identity management course?

This course builds and runs the trust technology itself: key pairs, certificate authorities, HSMs, revocation services and certificate automation. Legal recognition of electronic signatures and identity governance processes are covered only where they depend on certificates.

Why do Public Key Infrastructure PKI teams need crypto-agility?

Algorithms and key lengths are retired over time, and certificate validity periods keep shortening. A crypto-agile PKI keeps an inventory of where each algorithm is used and automates reissuance, so the organisation can change algorithms or migrate toward post-quantum schemes without service outages.

What do participants take back from Public Key Infrastructure PKI training?

Each participant takes back a PKI Design and Certificate Management Policy for a case organisation, covering the CA hierarchy, HSM and key ceremony plan, certificate lifecycle routines, revocation design and a crypto-agility inventory that can be adapted to their own estate.