Faysal Aziz

PKI for Infra Professionals

Build, operate, troubleshoot, and automate certificate infra in 2 days

FA-0348 · 2 days

DevOps, Cloud & Infrastructure · Automation, RPA & Power Platform

---

Introduction

Duration: 2 Days
Format: Instructor-led Training or Virtual Instructor-led Training
Audience: Linux system administrators, DevOps engineers, SREs, security engineers, infrastructure engineers, and technical leads

Certificate infrastructure has become more operational than academic. Shorter public TLS certificate lifecycles, growing automation expectations, internal service encryption, Linux trust-store management, SSH certificate use, and private CA platforms all make PKI a daily production concern rather than a background security topic.

The CA/Browser Forum has moved toward reduced public TLS certificate validity periods, making certificate lifecycle automation increasingly important. OpenSSL 3.5 is now an LTS release line, keeping OpenSSL central to Linux-based certificate operations. Modern private CA tools such as step-ca also support automated X.509 and SSH certificate management, which reflects where infrastructure teams are heading.

This course is designed for professionals. The instructor brings over 30 years of industry experience and will use real industry-demanded content instead of presenting PKI as a purely academic subject.

Learning outcomes

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

- Explain core PKI concepts, certificate chains, trust anchors, revocation, and certificate lifecycle risks.
- Build and operate a Linux-based private CA for internal infrastructure use.
- Use OpenSSL and Linux command-line tools to generate, inspect, validate, issue, and troubleshoot certificates.

- Configure Linux trust stores and validate certificate trust across common services.
- Deploy TLS certificates for Linux-based web and application services.
- Understand CRL, OCSP, ACME, SCEP, and automated certificate enrollment concepts.
- Troubleshoot certificate chain, hostname, expiration, trust-store, and revocation-related issues.
- Validate interoperability with one Windows client scenario.

Prerequisites

- Working knowledge of Linux administration
- Basic understanding of TCP/IP networking
- Familiarity with SSH and command-line operations
- Basic understanding of web servers or application services
- Some exposure to TLS, HTTPS, or certificates is helpful but not mandatory

Training outline

1. Public Key Infrastructure Fundamentals for Linux Professionals

1. PKI purpose and enterprise use cases
2. Confidentiality, integrity, authentication, and non-repudiation
3. Public key and private key concepts
4. Symmetric and asymmetric cryptography
5. Hashing and message integrity
6. Digital signatures
7. X.509 certificates
8. Certificate authorities
9. Root CAs and intermediate CAs
10. Certificate chains
11. Trust anchors
12. Public CA versus private CA
13. Internal PKI versus public Web PKI
14. Certificate policies and operational governance

2. Linux PKI Tooling and Environment Preparation

1. Linux lab architecture
2. OpenSSL installation and version validation
3. Certificate utility tools
4. Linux directory structure for PKI operations
5. Secure key storage locations
6. File permissions and ownership
7. Randomness and entropy considerations
8. Command-line certificate inspection
9. PEM, DER, CRT, CER, KEY, CSR, P12, and PFX formats
10. Certificate conversion workflows

3. Building a Linux-Based Certificate Authority

1. Root CA design
2. Offline root CA considerations
3. Intermediate issuing CA design
4. CA private key generation
5. CA certificate creation
6. OpenSSL CA configuration
7. Certificate serial number management
8. CA database structure
9. Certificate signing workflows
10. Certificate validity planning
11. Certificate extensions
12. Basic constraints
13. Key usage
14. Extended key usage
15. Subject Alternative Name handling
16. CA backup and protection considerations

4. Certificate Request and Issuance Workflows

1. Private key generation
2. Certificate signing request creation
3. CSR fields and subject naming

4. SAN-based certificate requests
5. Server certificate issuance
6. Client certificate issuance
7. Service certificate issuance
8. Wildcard certificate considerations
9. Internal naming considerations
10. Certificate renewal workflow
11. Certificate replacement workflow
12. Certificate retirement workflow

5. Linux Trust Store Management

1. Linux system trust model
2. Red Hat-based trust store management
3. Debian and Ubuntu trust store management
4. Application-specific trust stores
5. Browser trust considerations
6. Java trust store considerations
7. Container image trust considerations
8. Adding internal root CAs
9. Removing untrusted CAs
10. Trust validation with command-line tools
11. Cross-platform trust considerations

6. TLS Deployment on Linux Services

1. TLS certificate requirements
2. NGINX certificate configuration
3. Apache HTTP Server certificate configuration
4. HAProxy certificate configuration
5. System service certificate placement
6. Private key permissions
7. Certificate chain configuration
8. Full-chain certificate files
9. TLS protocol selection
10. Cipher suite considerations

11. Certificate reload versus service restart
12. Service validation with OpenSSL and curl

7. Certificate Validation, Revocation, and Status Checking

1. Chain building
2. Path validation
3. Expiration checking
4. Hostname validation
5. Trust anchor validation
6. Certificate Revocation List concepts
7. Base CRL concepts
8. Delta CRL concepts
9. CRL distribution points
10. OCSP concepts
11. OCSP responder role
12. OCSP stapling concepts
13. Revocation limitations
14. Practical revocation validation

8. Automation and Modern PKI Operations

1. Certificate lifecycle automation
2. ACME protocol concepts
3. Private ACME services
4. SCEP concepts
5. Automated enrollment design
6. Short-lived certificate strategy
7. SSH certificate concepts
8. Machine identity management
9. Service identity management
10. Certificate inventory
11. Expiration monitoring
12. Renewal alerting
13. GitOps and infrastructure automation considerations
14. Secrets management integration considerations

9. Troubleshooting PKI and TLS Issues on Linux

1. Expired certificate errors
2. Missing intermediate certificate errors
3. Incorrect certificate chain errors
4. Hostname mismatch errors
5. Untrusted root errors
6. Private key mismatch errors
7. Permission-related certificate failures
8. TLS handshake failures
9. Application trust-store failures
10. OpenSSL troubleshooting commands
11. curl troubleshooting commands
12. journalctl and service log review
13. tcpdump and packet capture basics
14. Common operational mistakes

10. Cross-Platform Client Trust Validation

1. Linux client validation
2. Windows client trust-store import
3. Browser-based certificate validation
4. Internal CA trust verification
5. HTTPS service validation from Windows
6. Certificate chain viewing on Windows
7. Common Windows client trust issues
8. Linux-to-Windows interoperability considerations

11. PKI Operational Best Practices

1. CA hierarchy design
2. Separation of root and issuing CA roles
3. Key protection practices
4. Certificate naming standards
5. Validity period standards
6. Renewal window planning
7. Revocation planning

8. Audit and logging considerations
9. Documentation requirements
10. Change control considerations
11. Incident response for CA or key compromise
12. Production readiness checklist

Disclaimer

This training outline is provided as a professional guideline for course planning and delivery. The trainer may modify, reorder, expand, reduce, or otherwise amend the topics, labs, and delivery approach at their discretion based on participant skill level, organizational requirements, technical constraints, time availability, and instructional judgment, without prior notice.

© 2026 Faysal Aziz · Kuala Lumpur