PKI Fundamentals

a practical introduction to cryptography

A comprehensive, scenario-driven introduction to the concepts, components, and real-world usage of Public Key Infrastructure (PKI). This course blends cryptography theory with the techniques necessary to operate a functioning certification authority using Microsoft Active Directory Certificate Services. Participants gain the practical knowledge required to deploy, run, and maintain PKI in enterprise environments.

Overview:

- **Duration:** 3 (extendable to 4 days with optional modules, longer labs, and extended Q&A)
- **Teaching format:** online or on-site, suitable for groups up to 8 participants
- **Target Audience:** system or network administrators, security engineers, and all specialists responsible for PKI-enabled services in a Microsoft-centric on-prem or cloud environment
- **Prerequisites:** working knowledge of Windows Server, including Active Directory Domain Services

Goals:

- Understand the foundations of modern cryptography and its security goals
- Explain PKI components, trust models, and certificate life-cycle concepts
- Install, operate, and manage Microsoft AD CS in an enterprise environment
- Secure practical workloads such as IIS, VPN, Wi-Fi, EFS, email signing/encryption, and code-signing
- Work confidently with external CAs and OpenSSL for cross-platform certificate requests

Deliverables:

Training delivery includes preparation of hosting environment for hands-on labs, one per each attendee. Attendees also receive access to sample code, a list of reference resources, and transcript of code written in class. Classes are not recorded.

Pricing terms:

Training delivery is priced based on group size and includes trainer fee, courseware, hosting for the hands-on labs. Some customizations may incur an additional development charge. Travel expenses are billed as agreed before commencement of contract.

Course outline:

Chapter 1: Cryptography Fundamentals

- Recognizing security goals and threats
- Understanding real-world use cases

Chapter 2: PKI Concepts and Trust Models

- Components of PKI
- Common and rare types of trusts

Chapter 3: Understanding Certificates

- Certificate structure, fields, extensions
- Navigating certificate chains and troubleshooting trust
- Public standards, file formats, OIDs

Chapter 4: Getting Started with CAs

- Self-signed certificates and their role
- Using external CAs vs. internal issuance
- Importance of writing Certificate Policies

Chapter 5: Deploying AD CS

- Designing a two-tier PKI hierarchy
- Certificate templates
- Enrollment workflows: manual, Web Enrolment, GPO, and auto-enrollment
- Certificate life-cycle management

Chapter 6: Maintaining AD CS

- Health monitoring
- Key archival and recovery
- CA backup/restore procedures

Chapter 7: Practical Applications

- Web Servers
- Authentication
- Networking: VPNs, 802.1X
- File Encryption
- Email and Document Security
- Code Signing

Customization:

Topics listed can be modified to suit the needs of the attendees or class hours. This course is extremely flexible and can be adjusted to include, for example: OpenSSL on Linux and Windows, deep-dives into AD DS maintenance best-practices. Time can be allotted for a troubleshooting session of customer's existing PKI deployment. Additional topics may be added, provided available development time.

About the trainer

Paul "Dash" Wojcicki-Jarocki

With over two decades of experience in the Microsoft ecosystem, Paul is a trainer and consultant specializing in cloud infrastructure, automation, and deployment. Paul has designed and built solutions for enterprises across EMEA, often for the public and military sectors. As a Microsoft Certified Trainer, he delivers bespoke training, and has presented at industry-leading events (Microsoft Ignite, PowerShell+DevOps Global Summit, MCT Summit).