interface

We teach. You do.

ISC2

PKI300: Mastering Windows Server 2016 & PKI & Certificate Services ADCS

Renowned instructor Hasain Alshakarti demystifies PKI in this 3-Day class! This is an experiential course where you'll learn by actually deploying PKI - creating secure solutions using Public Key Infrastructure (PKI), SmartCards CLM and more. This live class is available virtually with RemoteLive™ or locally at our Phoenix, AZ location.

$2,495.00

- 3 Days
- Experiential class - learn by doing!
- Taught by Hasain Alshakarti

Upcoming Dates

Course Description

Get hands-on experience building secure solutions for Smart Cards, encryption, Secure Access and other exciting applications with Hasain Alshakarti, one of the world's foremost experts on PKI. He will show you effective methods, helpful tools and products required – all based on real-world scenarios.

Get a grip on Certificate Lifecycle Management using proprietary products to administrator smart cards and certificates. Install, configure, test, and manage PKI with Active Directory. The course will provide basic PKI expertise in design, standards and safety requirements when implementing PKI in your own environment.

New features in Windows Server 2016 will be covered. Active Directory Certificate Services (ADCS) in Windows Server 2016 provides many new features and capabilities such as Virtual Smart Cards, Key-Based Renewal Support, Version 4 Certificate Templates, and PowerShell Deployment and Management.

About the Instructor:

Hasain Alshakarti is a world leading IT security expert with a strong focus on networks, PKI and certificates. He's a senior IT security consultant at TrueSec with deep experience of numerous design projects, audits as well as advanced implementation projects and penetration testing of systems.

For his hard, solid achievements over the years, Hasain has been rewarded "Sweden's leading IT security expert" and Microsoft Most Valuable Professional(MVP) in Enterprice security multiple times. He is a sought after speaker and extremely popular instructor at various events worldwide.

Hasain is also an active member of Microsoft Extended Experts Team(MEET) and one of the few that successfully combines his expertise in application development and IT technology.

Course Outline

Overview of Public Key Infrastructure

- Introduction to PKI

- Introduction to Cryptography
- Certificates and Certification Authorities

Designing a Certification Authority Hierarchy

- Identifying CA Hierarchy Design Requirements
- Common CA Hierarchy Designs
- Documenting Legal Requirements
- Analyzing Design Requirements
- Designing a CA Hierarchy Structure
- Identifying Applications and Certificate Holders
- Identifying Technical and Business Requirements
- Designing a CA Hierarchy

Creating a Certification Authority Hierarchy

- Configuring CAPolicy.inf
- Creating an Offline CA
- Validating Certificates
- Planning CRL Publication
- Defining CRL and AIA Publication Settings
- Publishing the CRL and AIA Information
- Validating the PKI Health of your CA Hierarchy

Managing a Public Key Infrastructure (PKI)

- Introduction to PKI Management
- Managing Certificates
- Managing Certification Authorities
- Planning for Disaster Recovery
- Role Separation
- Restricting Certificate Managers
- Enabling Certificate Services Auditing

Configuring Certificate Templates

- Introduction to Certificate Templates
- Designing and Creating a Certificate Template
- Publishing a Certificate Template
- Managing Changes in a Certificate Template
- Delegating Certificate Template Administration Permissions
- Superseding a Certificate Template

Configuring Certificate Enrollment

- Introduction to Certificate Enrollment
- Enrolling Certificates Manually
- Autoenrolling Certificates

Key Archival and Recovery

- Introduction to Key Archival and Recovery
- Implementing Key Archival and Recovery

PKI Trust Between Organizations

- Introduction to Advanced PKI Hierarchies
- Qualified Subordination Concepts
- Configuring Constraints in a Policy.inf File
- Implementing Qualified Subordination

Deploying Smart Cards

- Introduction to Smart Cards
- Enrolling Smart Card Certificates
- Deploying Smart Cards
- Smart Card Enrollment Agent Requests
- Planning for Re-enrollment

Securing Web Traffic by Using SSL

- Introduction to SSL Security
- Enabling SSL on a Web Server
- Implementing Certificate-based Authentication
- Certificate Mapping in Active Directory
- Certificate Mapping in IIS

Configuring BitLocker Recovery

- Introduction to BitLocker Recovery
- Configuring BitLocker recovery
- Recovering BitLocker volumes

Code Signing

- Introduction to Code Signing
- Implementing code signing templates
- Managing trusted publisher

Audience

The audience for this class is the IT professional working in computer security. Roles that will benefit from this class include Security Architect, IT Security Manager, and Security Specialist that currently or plan to work directly with certificates and public key infrastructure.

Prerequisites

Some experience with Windows Server is required. General understanding and experience in IT security is necessary to understand the advanced concepts covered in this course.

What You Will Learn

After completing this hands-on PKI and Active Directory training, you will be able to:

- Describe PKI and the major components of a PKI.
- Design a certification authority (CA) hierarchy to meet business requirements.
- Install Certificate Services to create a CA hierarchy.

- Perform certificate management tasks, CA management tasks, and plan for disaster recovery of Certificate Services.
- Create and publish a certificate template, and replace an existing certificate template.
- Enroll a certificate manually, auto-enroll a certificate, and enroll a smart card certificate.
- Implement key archival and recovery in ADCS.
- Configure trust between organizations by configuring and implementing qualified subordination.
- Deploy smart cards in a Windows environment.
- Secure a Web environment by implementing SSL security and certificate-based authentication for Web applications.
- Implementing and managing Certificate based BitLocker Data Recovery
- Implement and use code signing.