Mastering Windows Server 2012 & PKI & Certificate Services ADCS

Description

Install, configure, test and manage PKI with Active Directory in your own environment.

Get hands-on experience and knowledge to create secure solutions using PKI, SmartCards CLM and more.

During three days of instructor-led training you will build solutions for smart cards, encryption, secure access and other exciting applications together with Hasain Alshakarti, one of the world’s foremost experts on PKI. He will show you effective methods, helpful tools and products required.

Get a grip of certificate lifecycle management using proprietary Truesec-tools and other suitable products for the administration of smart cards and certificates. Install, configure, test, and manage PKI with Active Directory, basic PKI expertise in design, standards and safety requirements in your own environment.

New features in Windows Server 2012 will be covered. Active Directory Certificate Services (ADCS) in Windows Server 2012 provides multiple new features and capabilities such as:

- Virtual Smart Cards
- Key-Based Renewal Support
- Version 4 Certificate Templates
- PowerShell Deployment and Management

This popular class address those that intend to implement a PKI solution. All trainings are based on self-perceived real life scenarios.

Objectives:

Understand and plan, install and manage PKI and ADCS in your own environment.

After completing this course, 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

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

Configuring Certificate Template
• 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 publishers

PreRequisites

Basic understanding of Active Directory administration and system security.

$2495.00 List Price

3 Days Course

Class Dates

Request a Date or a Private Class below.
Tag: Windows Server

Related Classes

CompTIA Security+

Certified Security Awareness Principles