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 2016 is required. General understanding and experience in IT security is necessary to understand the advanced concepts covered in this course.

WHAT YOU WILL LEARN

» 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 & enroll a smart card certificate.
» Implement key archival & 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.

“Interface never disappoints – first class all the way.”

Interface Student
Phoenix, AZ

$2495.00
• 3-Day Course

QUESTIONS?
Call 602-266-8585
PKI300: Mastering Windows Server 2016 & PKI & Certificate Services ADCS

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