

**Module 1: Overview of Public Key Infrastructure**

This module explains the basic concepts of a public key infrastructure (PKI) and its components. It also provides an overview of the topics that will be explained in-depth in the course.

**Lessons**

- Introduction to PKI
- Introduction to Cryptography
- Certificates and Certification Authorities

**Lab A: Identifying Trusted Root CAs**

- Creating a Custom MMC
- Viewing CA Certificates in Certificates MMC
- Analyzing CA Certificate Distribution Methods

After completing this module, students will be able to:

- Describe PKI and its basic components.
- Describe how symmetric and public key encryption works.
- Define the role of certificates and CAs in a PKI.

**Module 2: Designing a Certification Authority Hierarchy**

This module introduces students to designing a CA hierarchy. It explains the major tasks that are involved, including identifying business and legal requirements and planning a Certification Authority (CA) hierarchy structure.

**Lessons**

- Identifying CA Hierarchy Design Requirements
- Common CA Hierarchy Designs
- Documenting Legal Requirements
- Analyzing Design Requirements
- Designing a CA Hierarchy Structure

**Lab A: Designing a CA Hierarchy**

- Identifying Applications and Certificate Holders
- Identifying Technical and Business Requirements
- Designing a CA Hierarchy

After completing this module, students will be able to:

- Identify technical and business requirements for designing a CA hierarchy.
- Describe common CA hierarchy designs.
- Describe policies and documents for specifying the legal requirements of a CA hierarchy design.
- Identify the impact of design requirements and determine design changes to a CA hierarchy design.
- Design a CA hierarchy to meet business requirements.

### **Module 3: Creating a Certification Authority Hierarchy**

This module explains how to create a CA hierarchy based on a CA hierarchy design. Students also learn how to install Certificate Services, validate a certificate, and publish a certificate revocation list (CRL) and an Authority Information Access (AIA).

#### **Lessons**

- Creating an Offline CA
- Validating Certificates
- Planning CRL Publication
- Installing a Subordinate CA

#### **Lab A: Installing an Offline CA**

- Configuring CAPolicy.inf for installing the Offline Root CA
- Installing the Offline Root CA

#### **Lab B: Publishing CRLs and AIAs**

- Defining CRL and AIA Publication Settings
- Publishing the CRL and AIA Information
- Adding the Web Server to Local Intranet Sites

#### **Lab C: Implementing a Subordinate Enterprise CA**

- Installing the Subordinate Enterprise CA
- Validating the PKI Health of your CA Hierarchy

After completing this module, students will be able to:

- Create an offline root CA.
- Design an infrastructure to validate certificates.

- Design an infrastructure to publish CRLs.
- Install a subordinate CA.

**Module 4: Managing a Public Key Infrastructure**

This module explains how to manage a PKI by managing certificates and CAs. Students also learn how to recover a PKI in the event of a failure.

**Lessons**

- Introduction to PKI Management
- Managing Certificates
- Managing Certification Authorities
- Planning for Disaster Recovery

**Lab A: Enabling Role Separation**

- Defining CA Administrators and Certificate Managers
- Restricting Certificate Managers
- Generating Certificate Requests
- Testing CA Administrator Tasks
- Testing Certificate Manager Tasks
- Enabling Certificate Services Auditing

**Lab B: Backing Up and Restoring a Certification Authority**

- Determining Backup Privileges
- Backing Up Certificate Services
- Removing the CA's Private Key from the CA Certificate Store
- Restoring the System State Backup

After completing this module, students will be able to:

- Describe the use of roles in PKI management.
- Perform certificate management tasks.
- Perform CA management tasks.
- Plan for disaster recovery of Certificate Services.

**Module 5: Configuring Certificate Templates**

This module introduces students to certificate templates and how to design them. Students also learn about creating, publishing, and changing certificate templates.

**Lessons**

- Introduction to Certificate Templates
- Designing and Creating a Certificate Template
- Publishing a Certificate Template
- Managing Changes in a Certificate Template

**Lab A: Delegating Certificate Template Management**

- Delegating Certificate Template Administration Permissions

**Lab B: Designing a Certificate Template**

- Reviewing an Existing Certificate Template
- Designing the Custom Code Signing Certificate Template

**Lab C: Configuring Certificate Templates**

- Creating a Certificate Template
- Publishing a Certificate Template
- Enrolling the Certificate Template
- Superceding a Certificate Template

After completing this module, students will be able to:

- Describe the function of certificate templates in a Windows Server 2003 PKI.
- Design and create a certificate template.
- Publish a certificate template.
- Replace an existing certificate template with an updated certificate template.

**Module 6: Configuring Certificate Enrollment**

In this module, students learn about the various methods of enrolling certificates. Students can either process the certificate requests manually or automatically, depending upon the approval requirement from the certificate manager.

**Lessons**

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

**Lab A: Enrolling Certificates**

- Choosing an Enrollment Method
- Enrolling Computer Certificates by Using the Certificate Enrollment Wizard
- Creating a User Certificate Template that Enables Autoenrollment
- Deploying the Certificates by Using Autoenrollment

After completing this module, students will be able to:

- Select the appropriate certificate enrollment method for a given scenario.
- Enroll certificates manually.
- Autoenroll certificates.
- Enroll smart card certificates.

**Module 7: Configuring Key Archival and Recovery**

This module describes the importance of creating a strategy for data and key recovery and explains the key archival and recovery process. Students also learn how Windows XP and Windows Server 2003 enhance data protection and data recovery.

**Lessons**

Introduction to Key Archival and Recovery

Implementing Manual Key Archival and Recovery

Implementing Automatic Key Archival and Recovery

**Lab A: Configuring Key Recovery**

- Publishing the Key Recovery Agent Certificate Template
- Enrolling the Key Recovery Agent Certificates
- Implementing Key Recovery on an Enterprise CA
- Creating an Archive-enabled Certificate Template
- Acquiring an ArchiveEFS Certificate
- Performing Key Recovery

After completing this module, students will be able to:

- Describe the key archival and recovery process in a Windows Server 2003 PKI.
- Implement manual key archival and recovery.
- Implement automatic key archival and recovery.

### **Module 8: Configuring Trust Between Organizations**

Students learn how to extend an organization's PKI trust hierarchy to other organizations. By extending the trust hierarchy, an organization's certificates can be used and trusted across organizations for purposes like secure e-mail messages, client authentication, and server authentication.

#### **Lessons**

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

#### **Lab A: Implementing a Bridge CA**

- Creating a Qualified Subordination Signing Certificate Template
- Configuring a Policy.inf File
- Requesting a Qualified Subordination Signing Certificate
- Generating a Cross Certification Authority Certificate for the Bridge CA
- Modifying the Policy.inf File on the Bridge CA
- Creating the Cross Certification Authority Certificate
- Publishing the Bridge CA Cross Certification Authority Certificates
- Issuing Certificates that Meet Qualified Subordination Constraints

After completing this module, students will be able to:

- Describe advanced PKI hierarchies.
- Describe how constraints are used in qualified subordination.
- Configure a policy.inf file to implement qualified subordination constraints.
- Implement qualified subordination between CA hierarchies.

**Module 9: Deploying Smart Cards**

In this module, students learn how smart cards provide secure storage for data and also support authentication of users. Students also learn how to configure and deploy smart cards in a Windows Server 2003 PKI environment.

**Lessons**

- Introduction to Smart Cards
- Enrolling Smart Card Certificates
- Deploying Smart Cards

**Lab A: Deploying Smart Cards**

- Modifying and Publishing the Enrollment Agent Certificate Template
- Acquiring the Enrollment Agent Certificates
- Creating a Custom Smart Card Certificate
- Enabling the Downloading of Unsafe Microsoft ActiveX® Controls
- Performing Smart Card Enrollment Agent Requests
- Configuring a Certificate to Require a Smart Card Signature during Autoenrollment
- Signing an Autoenrollment Certificate Request with a Smart Card
- Planning for Re-enrollment

After completing this module, students will be able to:

- Describe the use of smart cards for authentication in a Windows Server 2003 PKI environment.
- Deploy smart cards for authentication in a Windows Server 2003 PKI environment.

**Module 10: Securing Web Traffic by Using SSL**

This module explains how to secure a Web environment by implementing SSL security and certificate-based authentication for Web applications.

**Lessons**

- Introduction to SSL Security
- Enabling SSL on a Web Server
- Implementing Certificate-based Authentication

**Lab A: Deploying SSL Encryption at a Web Server**

- Enabling SSL Encryption in IIS
- Securing the Security Virtual Folder
- Enabling Certificate Mapping in Active Directory
- Enabling Certificate Mapping in IIS

After completing this module, students will be able to:

- Describe how security is implemented in a Web environment.
- Configure IIS to implement SSL security.
- Implement certificate-based authentication for Web applications.

**Module 11: Configuring E-mail Security**

In this module, students learn how to implement secure e-mail messages in an Exchange 2003 environment.

**Lessons**

- Introduction to E-mail Security
- Configuring Secure E-mail Messages
- Recovering E-mail Private Keys
- Migrating a KMS Database to a CA Running Windows Server 2003

**Lab A: Securing E-mail Messages in Exchange Server 2003**

- Creating Exchange Server 2003 Mailboxes
- Creating and Publishing S/MIME Certificate Templates
- Configuring Outlook 2002
- Sending Secure E-mail Between Organizations

After completing this module, students will be able to:

- Describe how e-mail security is implemented by a server running Exchange in a Windows Server 2003 environment.
- Securing e-mail messages in an Exchange 2003 environment.
- Recover e-mail private keys.
- Migrate a Key Management Service (KMS) database to a Windows Server 2003 Enterprise Edition enterprise CA.

**Contact the training coordinator for pricing and details at 613-563-NOVA (6682) Ext:267 Or  
[training@novaknowledge.com](mailto:training@novaknowledge.com)**

Nova Knowledge Solutions can also customize this course to topics of your choice which will reduce the course cost.