

Module 5: Configuring Network Security by Using Public Key Infrastructure

Contents

Overview	1
Introduction to Public Key Infrastructure (PKI)	2
Deploying Certificate Services	10
Using Certificates	21
Managing Certificates	27
Configuring Active Directory for Certificates	33
Troubleshooting Certificate Services	35
Lab A: Installing and Configuring Certificate Services	37
Review	47



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, places or events is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2000 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, BackOffice, FrontPage, IntelliMirror, NetShow, Outlook, PowerPoint, Visual Studio, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Simulations and interactive exercises were built with Macromedia Authorware

Instructor Notes

Presentation:
90 Minutes

This module provides students with the knowledge and skills necessary to configure network security by using Public Key Infrastructure (PKI) in a Microsoft® Windows® 2000 network.

Lab:
45 Minutes

At the end of this module, students will be able to:

- Define PKI concepts.
- Deploy Certificate Services.
- Use certificates.
- Manage certificates.
- Configure the Active Directory™ directory service for certificates.
- Troubleshoot Certificate Services.

Materials and Preparation

This section provides you with the required materials and preparation tasks that are needed to teach this module.

Required Materials

To teach this module, you need the Microsoft PowerPoint® file 2153a_05.ppt.

Preparation Tasks

To prepare for this module, you should:

- Read all of the materials for this module.
- Complete the lab.
- Read the entire “Windows 2000 Certificate Services and Public Key Infrastructure” section in the Windows 2000 Server Resource Kit.
- Read the entire “Windows 2000 Choosing Security Solutions that Use Public Key Infrastructure” section in the Windows 2000 Server Resource Kit.
- Read the entire “Windows 2000 Cryptography for Network and Information Security” section in the Windows 2000 Server Resource Kit.
- Read the Public Key and Cryptography Web Workshop at <http://msdn.microsoft.com/workshop/c-frame.htm#/workshop/security/capi/pkcb/crypt1.asp>.

- Read the following white papers under **Additional Reading** on the Web page on the Student Materials compact disc:
 - *An Introduction to the Windows 2000 Public Key Infrastructure*
 - *Microsoft Windows 2000 Public Key Infrastructure*
 - *Windows 2000 Certificate Services*
- Read the following step-by-step guides at <http://www.microsoft.com/windows2000/library/technologies/security/default.asp>:
 - *Step-by-Step Guide to Administering Certificate Services*
 - *Step-by-Step Guide to Setting up a Certificate Authority*
 - *Step-by-Step Guide to Setting up Certification Authority Trust for a Domain*
 - *Step-by-Step Guide to Advanced Certificate Management*

Module Strategy

Use the following strategy to present this module:

- Introduction to Public Key Infrastructure (PKI)

Explain that the module is only intended to provide an overview of PKI concepts, and refer students to the *Public Key and Cryptography Web Workshop* at <http://msdn.microsoft.com/workshop/c-frame.htm#/workshop/security/capi/pkcb/crypt1.asp> for more information about security and cryptography. Briefly explain the difference between the use of the key pair for encryption and authentication. Use the driver's license analogy, or a similar example, to explain the role of a certification authority (CA). Explain the parent/child relationship and trust relationships established by a certificate hierarchy.

- Deploying Certificate Services

Provide examples of business cases for each of the four CA models. Do not go into detail about the advanced options for cryptographic settings. Explain that advanced settings are only modified for specific security architectures. Mention that Internet Information Services (IIS) must be installed prior to the installation of Certificate Services to use the Web components of Certificate Services. Explain the difference between the Certification Authority and the Certificates snap-in.

- Using Certificates

Explain the two methods for requesting certificates and explain that the Certificate Request wizard is only available for enterprise CAs. If time permits, show students an issued certificate and briefly explain the properties of the certificate.

- Managing Certificates

Explain the tasks that are performed to manage certificates. Emphasize that a Certificate Revocation List (CRL) must be published before revoked certificate information is available to clients. Briefly discuss certificate file formats, and show students an example of a certificate file in Windows Explorer if time permits.

- Configuring Active Directory for Certificates

Briefly discuss business cases for authenticating external users. Explain the three options for mapping accounts to certificates.

- Troubleshooting Certificate Services

Explain how to access the troubleshooting information in Windows 2000 Help. Discuss the use of the **certsrv** command for diagnostics purposes. Explain some of the problems that can affect the validity of a certificate.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

Important The lab in this module is also dependent on the classroom configuration that is specified in the Customization Information section at the end of the Classroom Setup Guide for course 2153, Implementing a Microsoft Windows 2000 Networking Infrastructure.

Lab Setup

There are no lab setup requirements that affect replication or customization.

Lab Results

There are no configuration changes on student computers that affect replication or customization.

Overview

Topic Objective

To provide an overview of the module topics and objectives.

Lead-in

In this module, you will learn about providing network security by using Public Key Infrastructure in a Windows 2000 network.

- Introduction to Public Key Infrastructure (PKI)
- Deploying Certificate Services
- Using Certificates
- Managing Certificates
- Configuring Active Directory for Certificates
- Troubleshooting Certificate Services

*****ILLEGAL FOR NON-TRAINER USE*****

Your organization's network may consist of intranets, Internet sites, and extranets—all of which are potentially susceptible to access by unauthorized individuals who may maliciously view or alter your digital information assets. A well-planned Public Key Infrastructure (PKI) can help you to secure data and distribute and manage identification credentials across your organization. The Microsoft® Windows® 2000 operating system includes a native PKI that is designed to take full advantage of the Windows 2000 security architecture.

At the end of this module, you will be able to:

- Define PKI concepts.
- Deploy Certificate Services.
- Use certificates.
- Manage certificates.
- Configure the Active Directory™ directory service for certificates.
- Troubleshoot Certificate Services.

Note This module provides an overview of PKI concepts. For more information about cryptography basics, see the Microsoft Windows 2000 Public Key Infrastructure white paper at <http://www.microsoft.com/windows2000/techinfo/planning/security/pki.asp>.

◆ Introduction to Public Key Infrastructure (PKI)

Topic Objective

To identify PKI concepts.

Lead-in

Public Key Infrastructure is a key technology used to provide network security. Windows 2000 can use public key security for encryption and authentication in areas such as smart card authentication, Encrypting File System, and IPSec.

- Public Key Encryption
- Public Key Authentication
- Certificate Authority
- Certificate Hierarchies
- Windows 2000 PKI

*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Public key cryptography is crucial for e-commerce and scenarios that require *distributed security*—security in which the participants are not part of the same network and have no common security credentials.

Public key cryptography is an important technology for e-commerce, intranets, extranets, and Web-enabled applications. The two fundamental operations associated with public key cryptography include encryption and authentication. Windows 2000 uses public key cryptography in areas such as smart card logon, Encrypting File System (EFS), and Internet Protocol Security (IPSec).

Note The PKI in Windows 2000 supports the standards developed by the Internet Engineering Task Force (IETF) and RSA Data Security, Inc. These include Public Key Infrastructure, X.509 draft standards, and Public Key Cryptography Standards, respectively.

For more information about Internet drafts and for RFCs about PKI, see www.ietf.org/.

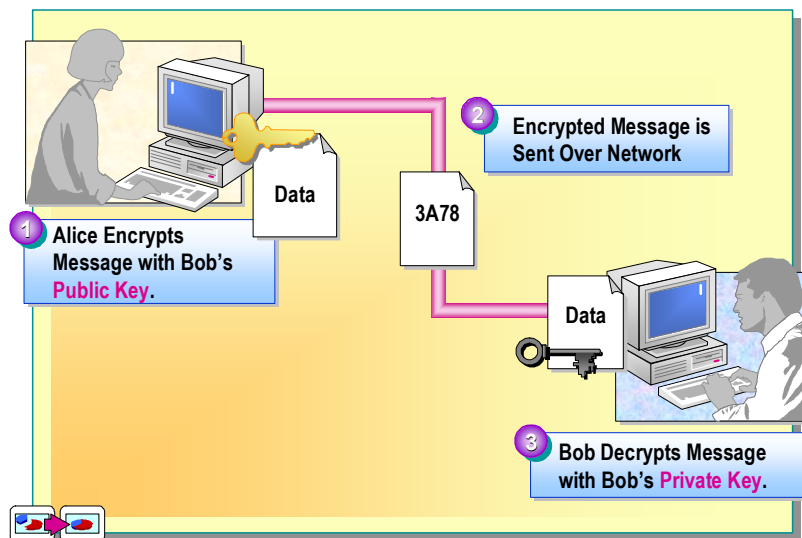
Public Key Encryption

Topic Objective

To illustrate the process of public key encryption.

Lead-in

Public key encryption uses two keys: an encryption key and a decryption key.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

Public key cryptography provides privacy through data encryption, whether the data is in the form of e-mail messages, credit-card numbers sent over the Internet, or network traffic. Because public keys can be posted freely, complete strangers can establish private communications over public networks merely by retrieving each other's public keys and encrypting the data.

Using Public Keys and Private Keys

Key Point

Public key encryption is a method of encryption that uses two keys that are mathematically related.

Public key encryption uses two keys that are mathematically related. A *key* is a random string—such as a number, ASCII value, word, or phrase—that is used in conjunction with an algorithm. For public key encryption, every user has a pair of mathematically related keys, including:

- A *private key*, which is kept confidential.
- A *public key*, which is freely given out to all potential correspondents.

Key Point

The use of keys in PKI-enabled programs that provide data encryption is typically transparent to the user.

The goal of encryption is to obscure data in such a way that it can only be read by the intended party. In a typical scenario, a sender uses the recipient's public key to encrypt a message. Only the recipient has the related private key to decrypt the message. By making your public key available, other people can send you encrypted data that can only be decrypted by using your private key. The use of keys in PKI-enabled programs that provide data encryption is typically transparent to the user.

Encrypting and Decrypting Text

The fundamental property of public key encryption is that the encryption and decryption keys are different. Encryption with a public key is a one-way function. When you encrypt a document with a public key, *plaintext* turns into *cipher text*. A decryption key, which is related but not identical to the encryption key, is needed to turn the cipher text back into plaintext. If someone intercepts an encrypted message in transmission, the message is in cipher text and is unreadable.

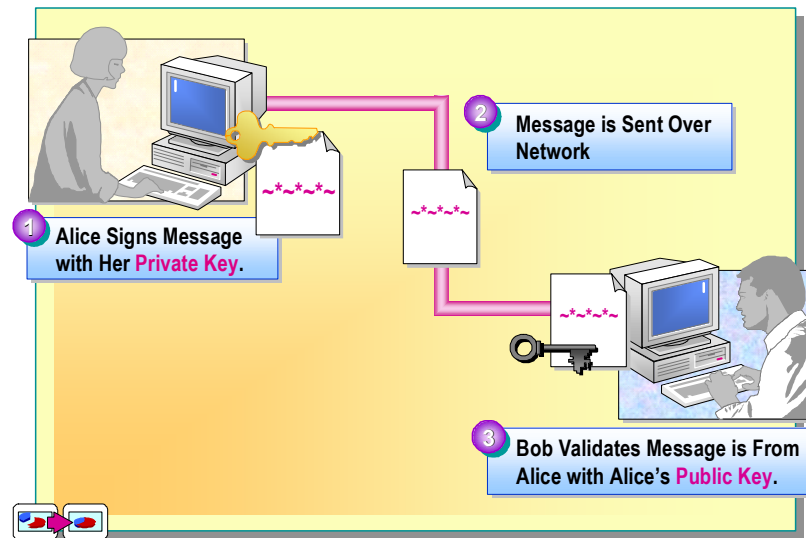
Public Key Authentication

Topic Objective

To identify the use of digital signatures and hash algorithms for public key authentication.

Lead-in

Like public key encryption, public key authentication uses a key pair.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

Public key authentication uses public key cryptography to authenticate and verify the originator of electronic data in e-mail, e-commerce, and other electronic transactions. Like public key encryption, public key authentication uses a key pair. However, instead of using the sender's private key to decrypt a message, the sender's public key is used to authenticate and validate the sender of the message. A string of characters that uniquely identifies the contents of the message is encrypted with the private key to create a *digital signature*. A digital signature swaps the role of the private and public keys.

Digital Signatures

A digital signature is a means for the originator of a message, file, or other digitally encoded information to bind his or her identity to the information. The signature itself is a sequence of bits appended to a digital document. A digital signature ensures that:

- Only someone possessing the private key could have created the digital signature.
- Anyone with access to the corresponding public key can verify the digital signature.

For example, when you visit a Web site and you are prompted to download a file, a dialog box informs you that the file has been digitally signed by an entity that you can trust. A digital signature assures you that a file or program that you are about to download has come from a reputable source.

Hash Algorithms

A digital signature uses an algorithm called a *hash algorithm*. Hash algorithms are designed to guarantee that if a single byte changes, processing the document generates a completely different hash. When a hash is encrypted by using a public key, any modification of the signed data invalidates the digital signature.

Explain that encryption provides security and confidentiality, and that digital signatures provide proof of authenticity and origination.

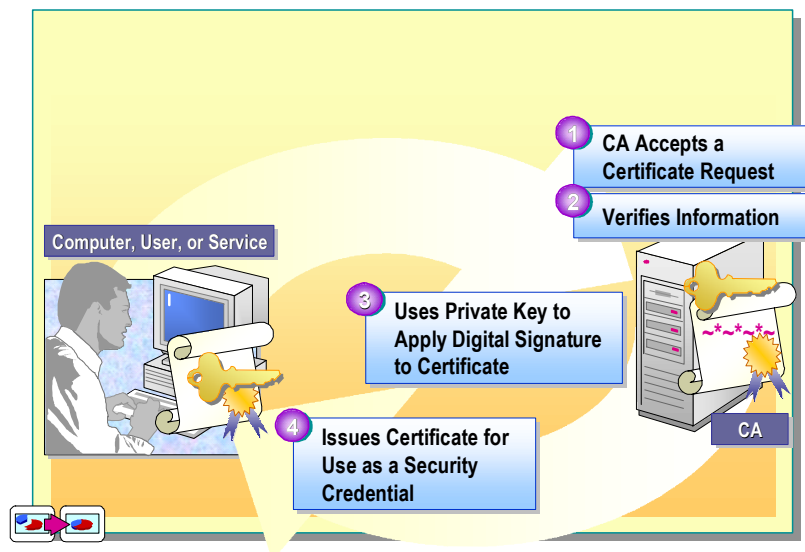
Certification Authority

Topic Objective

To illustrate the process that a CA uses to issue a certificate.

Lead-in

A CA is responsible for providing and assigning the keys for encryption, decryption, and authentication.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

A certification authority (CA) is responsible for providing and assigning the keys for encryption, decryption, and authentication. A CA distributes keys by issuing *certificates*, which contain the public key and a set of attributes. A CA can issue certificates to a computer, a user account, or a service.

Certificates

Certificates are signed documents that match public keys to other information, such as a name or an e-mail address. Certificates are signed by CAs that issue certificates. A CA's signature guarantees that the public key does indeed belong to the party that presents it.

Delivery Tip

Explain that a driver's license is a real-world analogy for a digital certificate. It contains a unique key (a license number) and attributes (an expiration date, your name, address, hair color, and so on). It is issued by a trusted agency and laminated to prevent it from being tampered with.

External and Internal CAs

A CA can be an external issuing company, such as a large commercial CA that issues certificates to millions of users. Or a CA can be internal, such as a department within a company that has installed its own server for issuing and verifying certificates. Each CA decides what attributes it includes in a certificate and what mechanism it uses to verify those attributes before issuing the certificate.

Important An organization can set its own policy for its internal CA. Be aware that other organizations may have very different policies from your own organization. The use of certificates requires that you trust the policies of the organization that issues the certificates.

Additionally every CA has a certificate to confirm its own identity, issued by another trusted CA or by itself. By trusting a CA, you implicitly trust the policies and procedures that the CA has in place for confirming the identity of the entities that are issued certificates.

The Process for Issuing Certificates

The process for issuing a certificate has four basic steps:

1. The CA accepts a certificate request.
2. The CA verifies the requester's information according to the proof-of-identity requirements of the CA.
3. The CA uses its private key to apply its digital signature to the certificate.
4. The CA issues the certificate for use as a security credential within a PKI.

Certificate Revocation

A CA is also responsible for revoking certificates and for publishing a Certificate Revocation List (CRL). Revocation of a certificate invalidates the certificate as a trusted security credential before the expiration of the certificate's validity period. The following are some reasons why a certificate would be revoked prior to its expiration:

- Compromise, or suspected compromise, of the certificate subject's private key
- Discovery that a certificate was obtained fraudulently
- Change in the status of the certificate subject as a trusted entity

Note If a CA's certificate is revoked, then all certificates that the CA issued are also revoked.

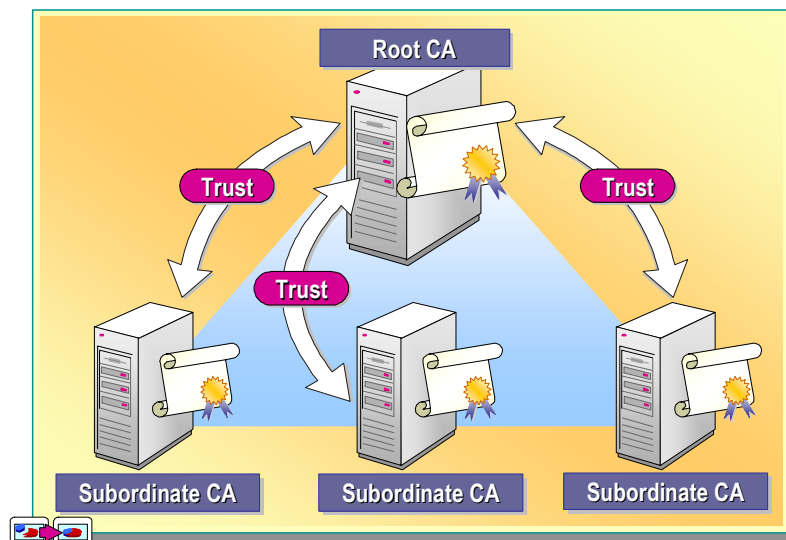
Certificate Hierarchies

Topic Objective

To identify the topics related to certificate hierarchies.

Lead-in

A certificate hierarchy is a model of trust in which certification paths are created through the establishment of parent/child relationships between CAs.



*****ILLEGAL FOR NON-TRAINER USE*****

Delivery Tip

The slide for this topic includes animation. Click or press the SPACEBAR to advance the animation.

A certificate hierarchy is a model of trust in which certification paths are created through the establishment of parent/child relationships between CAs. A root CA, the subordinate CAs that have been certified by the root, and subordinate CAs that have been certified by other subordinate CAs, form a certificate hierarchy. You can only trust root CAs, not subordinate CAs. You trust the policies and procedures defined by the root CA, because all subordinate CAs must also follow these rules.

Root CA

A *root CA*, sometimes called a root authority, is meant to be the most trusted type of CA in an organization's PKI. Typically, both the physical security and the certificate issuance policy of a root CA are more rigorous than those for subordinate CAs. If the root CA is compromised or issues a certificate to an unauthorized entity, all certificate-based security in your organization is suddenly vulnerable. Although root CAs can be used to issue certificates to end users for such tasks as sending secure e-mail, in most organizations they are only used to issue certificates to other CAs, called subordinate CAs.

Subordinate CA

A *subordinate CA* is a CA that has been certified by another CA in your organization. Typically, a subordinate CA issues certificates for specific uses, such as secure e-mail, Web-based authentication, or smart card authentication. Subordinate CAs can also issue certificates to other, more subordinate CAs.

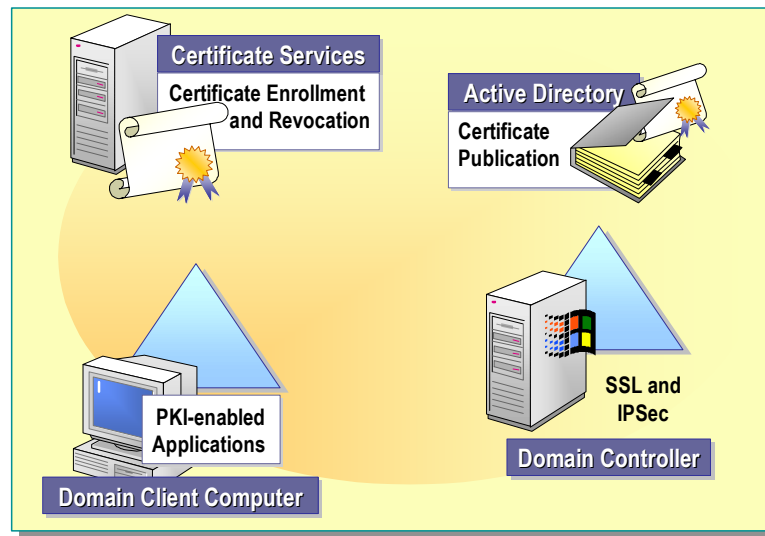
Windows 2000 PKI

Topic Objective

To illustrate the services and components that comprise a Windows 2000 PKI.

Lead-in

To use the benefits of public key cryptography, you need a supporting infrastructure.



*****ILLEGAL FOR NON-TRAINER USE*****

To use the benefits of public-key cryptography, an organization needs a supporting infrastructure. The PKI supplied by Windows 2000 consists of a set of services that are provided by a group of interconnected components. These components work together to provide public key–based security services to users and applications.

Windows 2000 PKI Primary Components

The primary components of the Windows 2000 PKI are:

- *Certificate Services*. The core operating system service that allows businesses to act as their own CAs and to issue and manage digital certificates.
- *Active Directory*. The publication service for PKI. Certification publication makes certificates and CRLs publicly available within an organization.

Note Certificates can also be published on Web pages or distributed on smart cards, disks, or compact discs. Certificate Revocation Lists are published at URLs.

- *PKI-enabled applications*. The applications that use PKI for encryption and authentication. These include Microsoft Internet Explorer, Microsoft Money, Microsoft Internet Information Services (IIS), Microsoft Outlook®, Microsoft Outlook Express, and third-party applications.

Security Protocols

In addition, Windows 2000 PKI components use industry security protocols, including:

- *Secure Sockets Layer (SSL)*. A protocol developed by Netscape Communications Corporation for ensuring security and privacy in Internet communications. SSL supports authentication of client, server, or both, in addition to encryption during a communications session.
- *Internet Protocol Security (IPSec)*. A set of protocols being developed by the IETF to support secure exchange of packets at the IP layer.
- *Transport Layer Security (TLS)*. A protocol that provides privacy and security between two applications communicating over a network.

Use of Certificates

Security services and programs in Windows 2000 use certificates to provide authentication, data integrity, and secure communications across nonsecure networks such as the Internet. Certificates provide the following:

- *Server authentication*. Uses certificates to authenticate servers to clients. E-commerce is an example.
- *Client authentication*. Uses certificates to authenticate clients to servers. Remote access functionality and smart card authentication are examples.
- *Code signing*. Uses certificates associated with key pairs to sign active content.
- *Secure e-mail*. Uses certificates associated with key pairs to sign e-mail messages.
- *EFS*. Uses two certificates associated with key pairs. One certificate is for encryption and decryption and one certificate is used for EFS recovery.
- *IPSec*. Uses certificates associated with key pairs to encrypt IP-based network traffic.

◆ Deploying Certificate Services

Topic Objective

To identify the topics related to deploying Certificate Services.

Lead-in

The first choice that you must make when deploying a PKI solution is which CA hierarchy model to use.

- **Choosing a Certificate Authority (CA) Model**
- **Installing Certificate Services**
- **Creating a Subordinate CA**
- **Backing up and Restoring Certificate Services**

*****ILLEGAL FOR NON-TRAINER USE*****

By installing Certificate Services, you can create a CA for issuing certificates that are needed to run a PKI. In Windows 2000 Server, the certification authority is one of two types: *enterprise* or *stand-alone*. Within each type, there can be a root CA and one or more subordinate CAs.

Typically, you must install an enterprise CA if you plan to issue certificates to users or computers inside a single Windows 2000 network. An enterprise CA requires that all users and computers requesting certificates have an account in Active Directory.

You must install a stand-alone CA if you plan to issue certificates to users or computers outside a single Windows 2000 network. A stand-alone CA does not require Active Directory.

Whichever type of CA you choose, backing up the CA database, certificates, and keys is essential to protecting your organization against the loss of critical data.

Note For more information about using Certificate Services as part of a PKI infrastructure, see the white paper *Windows 2000 Certificate Services* under **Additional Reading** on the Web page on the Student Materials compact disc.

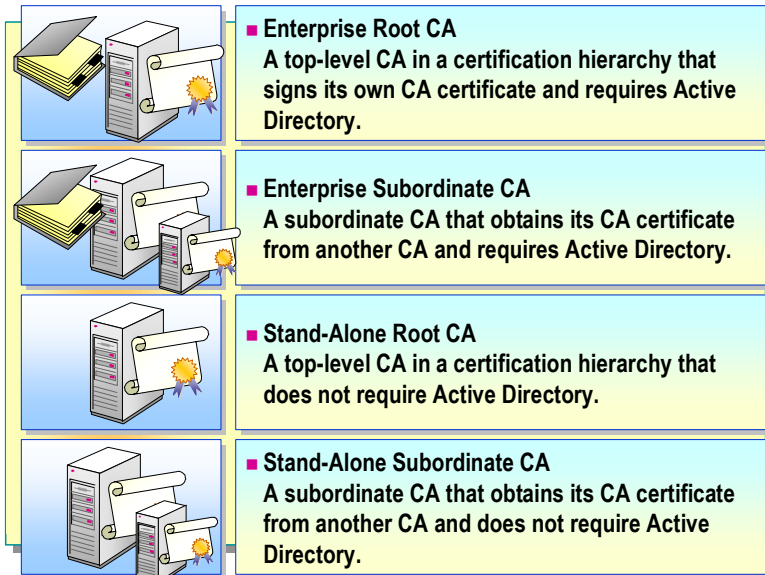
Choosing a CA Model

Topic Objective

To illustrate the CA models available for Certificate Services.

Lead-in

The first choice that you make when implementing Certificate Services is deciding which CA model to use.



*****ILLEGAL FOR NON-TRAINER USE*****

The first choice that you make when implementing Certificate Services is deciding which CA model to use. When you install Certificate Services, you can select from one of four different CA models, each of which causes the CA to have different characteristics and performance. You choose the model that you want to use, based on how you need the CA to perform, given its role in your PKI.

Enterprise Root CA

An enterprise root CA is the top-level CA in a certificate hierarchy. An enterprise root CA uses Active Directory to determine the identity of the requester and to determine whether the requester has the security permissions to request a particular certificate type. You should set up an enterprise root CA if you will issue certificates only to users and computers within your organization. Typically, the enterprise root CA issues certificates only to subordinate CAs.

Explain that these requirements are for both an enterprise root and a subordinate CA.

To install an enterprise root CA, you must have the following:

- *Active Directory.* The enterprise policy used by Certificate Services places information into Active Directory.
- *DNS Server service.* Active Directory requires the DNS service.
- *Administrative privileges on the DNS, Active Directory, and CA servers.* This is especially important because Setup modifies information in places that may require domain administrative privileges. Also, to install an enterprise CA, you must be a member of the Enterprise Admins group.

Important To publish certificates in Active Directory, the server on which the CA is installed must be a member of the Cert Publishers group.

Enterprise Subordinate CA

An enterprise subordinate CA issues certificates within an organization, but is not the most trusted CA. You can use an enterprise subordinate CA to issue certificates for specific uses, such as secure e-mail, Web-based authentication, or smart card authentication. An enterprise subordinate CA must have a parent CA.

Stand-Alone Root CA

A stand-alone root CA is the top-level CA in a certificate hierarchy. A stand-alone root CA may or may not be a member of a domain and does not require Active Directory. A stand-alone root CA can be disconnected from the network and placed in a secure area.

You should install a stand-alone root CA if you will issue certificates to entities outside your organization. Typically, a root CA only issues certificates to subordinate CAs. To install a stand-alone root CA, you must have administrative privileges on the local server.

Stand-Alone Subordinate CA

A stand-alone subordinate CA operates as a solitary certificate server within a CA trust hierarchy. You should set up a stand-alone subordinate CA if you will issue certificates to entities outside an organization.

To install a stand-alone subordinate, you must have the following:

- A parent CA, such as an external commercial CA, that will process the subordinate CA's certificate requests.
- Administrative privileges on the local server.

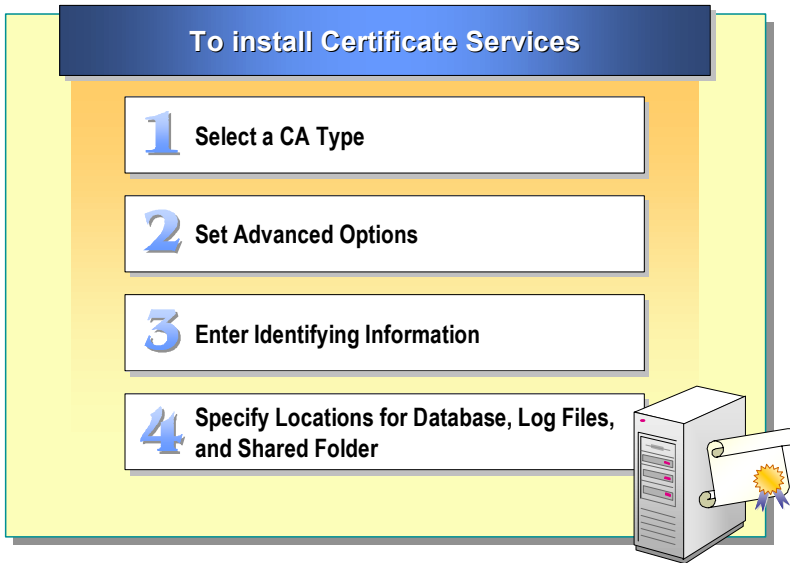
Installing Certificate Services

Topic Objective

To identify the tasks for installing Certificate Services

Lead-in

There are a number of options for installing Certificate Services.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain that although Certificate Services is a Windows 2000 service and is included with Windows 2000 server products, it is not installed by default.

Although Certificate Services is a Windows 2000 service and is included with Windows 2000 server products, it is not installed by default. You can install Certificate Services during or after Windows 2000 setup. To install Certificate Services during Windows 2000 installation, select Certificate Services from the optional components list that displays during setup. You can install Certificate Services after Windows 2000 setup, by using Add/Remove Programs in Control Panel. During Certificate Services setup, you must configure several options and settings.

Important A computer cannot be renamed, or joined to or removed from a domain after Certificate Services is installed. To perform any of these actions, you first need to remove Certificate Services from the computer.

Selecting a CA Type

First, you must select one of the following CA types: enterprise root CA, enterprise subordinate CA, stand-alone root CA, or stand-alone subordinate CA.

Setting Advanced Options

Key Point

Only modify these settings if you require specific cryptography settings.

To change default cryptographic settings, click **Advanced options**, and then select from the following settings.

Setting	Description
CSP	Use this setting to specify a third-party cryptographic service provider (CSP). The default is Microsoft Base Cryptographic Provider v 1.0. Refer to the CSP vendor's documentation for information about using the CSP with Certificate Services.
Hash algorithm	The default is SHA-1 (Secure Hash Algorithm 1).
Key length	The default key length is 512 bit when using Microsoft Base Cryptographic Providers. For a root CA, you should use a key length of at least 2048 bits. This setting is not available if you are using existing keys.
Use existing keys	Select this option when you are relocating or restoring a previously installed CA. Also, select Use the associated certificate to ensure that the CA has a certificate that is identical to the previous CA.

Entering Identifying Information

Enter the required information to identify your CA, according to the following guidelines:

Field	Description
CA name	The name to identify the CA object that will be created in Active Directory. Active Directory object names are limited to 64 characters by the Lightweight Directory Access Protocol (LDAP) standard. Refer to Windows 2000 Help for information about names with special characters.
Country/Region	The two-character country/region code, as required by the X.500 Naming Scheme standard. For example, the country/region code for the United States is US, and the code for Germany is DE.
Valid for	The field can be set only for a root CA. The validity duration you choose for the CA determines when the CA expires. Typically, a time period of two years is recommended.

Specifying Locations for the Database and Log Files

Certificate Services uses local storage for its database, configuration data, backup data, and log files. You can specify locations for the database and log files during CA setup. By default, the certificates that a CA issues are stored in *systemroot\System32\CertLog*. You can improve performance by storing the files on different physical hard drives.

You can also store configuration data in a shared folder. By default, the shared folder is *systemroot\CACConfig*.

You can also specify a shared folder where the CA stores information about the CA and its root CA certificate. Create the shared folder if you want to allow users to retrieve information about the CA and the root CA certificate from a shared folder instead of using a Web browser to retrieve this information. If you specify a shared folder, Certificate Services shares the folder and assigns to it the name *CertConfig*.

To use the Web components of Certificate Services, you must install IIS first.

Installation Components

Certificate Services adds the following components after installation:

- *Certification Authority*. A console for managing CAs on servers on which Certificate Services is installed. You access Certification Authority through the **Administrative Tools** menu. You use Certification Authority to issue certificates, revoke certificates, change policy settings, view a list of certificates issued, and to perform other administrative tasks.
- *Certificates*. A snap-in that you add to Microsoft Management Console (MMC) to manage existing certificates for user accounts, computers, and services.
- *Certificate Services Web enrollment support*. Web pages provided for users and administrators to request certificates. These Web pages are located at <http://server/certsrv>, where *server* is the name of the server running Windows 2000 that hosts the CA.

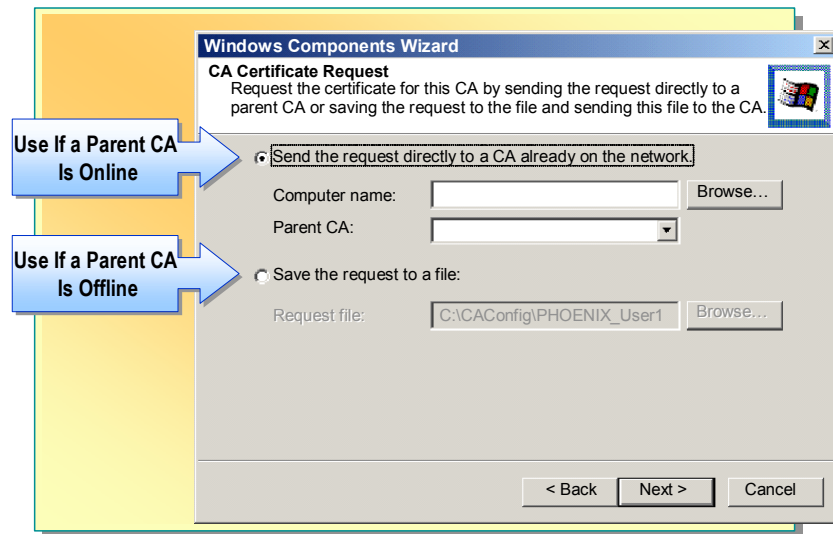
Creating a Subordinate CA

Topic Objective

To illustrate the interface for obtaining a CA certificate request during setup.

Lead-in

A subordinate CA is certified by either another CA in your organization or a commercial CA.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

When you install a subordinate CA, you will need to obtain a certificate from a parent CA.

A subordinate CA must be associated with a CA that processes the subordinate CA's certificate requests. Depending on the type of CA, this can be another CA in your organization or an external third-party CA. Typically, a subordinate CA issues certificates for specific uses, such as secure e-mail, Web-based authentication, or smart card authentication. Subordinate CAs can also issue certificates to other, more subordinate CAs. When you install a subordinate CA, you must obtain a certificate from a parent CA.

Obtaining a Certificate for a Subordinate CA

To obtain a certificate if a parent CA is available online:

1. On the **CA Certificate Request** page, click **Send the request directly to a CA already on the network**.
2. In the **Computer Name** box, type or browse to the name of the computer on which the parent CA is installed.
3. In the **Parent CA** list, click the name of the parent CA.

To obtain a certificate if a parent CA is not available online:

On the **CA Certificate Request** page, click **Save the request to a file**. In the **Request file** box, type the path and file name of the file that will store the request. You then must obtain the certificate from the parent CA. As a minimum, the file from the parent CA should contain the subordinate CA's certificate and the full certification path.

Installing a Certificate from a File

When you create a certificate request file during installation of a subordinate CA, you must submit the file to your parent CA. Your parent CA will provide you with a certificate for this file. After you receive your certificate, you must install the certificate.

To install a certificate from a file:

1. Open Certification Authority from the **Administrative Tools** menu.
2. In the console tree, click the name of the CA.
3. On the **Action** menu, point to **All Tasks**, and then click **Install CA Certificate**.
4. Locate the certificate file received from the parent CA, click this file, and then click **Open**.

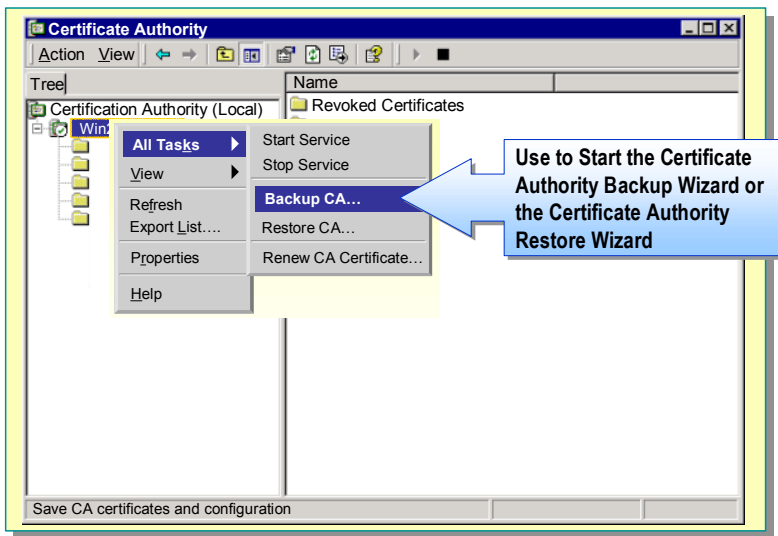
Backing Up and Restoring Certificate Services

Topic Objective

To identify the topics related to backing up and restoring Certificate Services.

Lead-in

You need to protect the CA and its operational data from accidental loss due to hardware or storage media failure.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Use the Certification Authority snap-in to back up data when you do not want to back up the entire server.

The purpose of performing backup and restore operations is to protect the CA and its operational data from accidental loss due to hardware or storage media failure. The recommended method for backing up a CA is to use Windows 2000 Backup to back up the entire server. When backing up a server, the CA is backed up as part of the system state. It is also possible to back up and restore a CA by using Certification Authority, but this method is intended for use only when you do not want to back up the entire server on which the CA is installed.

Important Upon restoring a CA, the IIS metabase must also be restored if it has been damaged or lost. If a damaged or missing IIS metabase is not restored, IIS will fail to start, and that will result in the failure of Certificate Services to start.

Backing up a CA

How frequently you back up a CA depends on the number of certificates issued. The more certificates a CA issues, the more frequently you should back up the CA.

To back up a CA:

1. Log on to the system as a member of the Backup Operators or Administrators groups.
2. Open Certification Authority from the **Administrative Tools** menu.
3. In the console tree, click the name of the CA.
4. Right-click the name of the CA, point to **All Tasks**, and then click **Backup CA**.
5. Follow the instructions in the Certification Authority Backup wizard. They include:
 - Selecting the data to back up and specifying a backup location.
 - Providing a password to gain access to the private key and CA certificate.

Restoring a CA

To restore a CA from a backup copy:

1. Log on to the system as a member of the Backup Operators or Administrators groups.
2. Open Certification Authority.
3. In the console tree, click the name of the CA.
4. Right-click the name of the CA, point to **All Tasks**, and then click **Restore CA**.
5. Follow the instructions in the Certification Authority Restore wizard. They include:
 - Selecting the data to restore and specifying the restore location.
 - Providing a password to gain access to the private key and CA certificate.

◆ Using Certificates

Topic Objective

To identify the topics related to creating and managing certificates.

Lead-in

There are two primary ways to explicitly request certificates in Windows 2000.

- Using the Certificate Request Wizard
- Using the Certificate Services Web Pages
- Viewing Certificates

*****ILLEGAL FOR NON-TRAINER USE*****

There are two primary ways to explicitly request certificates in Windows 2000: by using the Certificate Request wizard or by using the Certificate Services Web pages. The Certificate Request wizard is only available if you are requesting a certificate from an enterprise CA. You can use the Certificate Services Web pages to request certificates from a stand-alone CA or from an enterprise CA.

Using the Certificate Request Wizard

Topic Objective

To identify the topics related to using the Certificate Request wizard.

Lead-in

The Certificate Request wizard is only available for requesting a certificate from an enterprise CA.

- Using Certificate Templates
- Requesting a Certificate

*****ILLEGAL FOR NON-TRAINER USE*****

The Certificate Request wizard is available only for requesting a certificate from an enterprise CA. When requesting a certificate, a user can select from different certificate types. The user can select from certificates types for which they have Read or Enroll permissions. After a user submits a certificate request, the request is either immediately denied or granted. If it is granted, the user is prompted to install the certificate.

Using Certificate Templates

Explain that you use the domain controller, computer, and Web server templates to issue certificates to computers.

As part of its policy settings, an enterprise CA can issue specific certificate types. The certificate types are based on *certificate templates*. Certificate templates are predefined configurations that provide common settings for the certificate request. The following are examples of some commonly used certificate templates.

Certificate Template	Description
Administrator	Allows use of a certificate for code signing, certificate trust list signing, EFS, secure e-mail, and client authentication
Domain Controller	Allows use of a certificate for client authentication and server authentication
Computer	Allows use of a certificate for client authentication and server authentication
Basic EFS	Allows use of a certificate for EFS only
EFS Recovery Agent	Allows use of a certificate for file recovery
User	Allows use of a certificate for EFS, secure e-mail, and client authentication
Web Server	Allows use of a certificate for server authentication.

Requesting a Certificate

To request a certificate by using the Certificate Request wizard:

1. Open an MMC console that contains the Certificates snap-in.
2. In the **Certificates snap-in** dialog box, select **My user account**, **Service account**, or **Computer account**, and then click **Finish**.
3. Close the **Add Stand-alone snap-in** dialog box, and then click **OK**.
4. In the console tree, expand **Certificates Current User**, **Certificates (Local Computer)**, or the node for the selected service.
5. In the console tree, click a logical store name (for example, **Personal**), right-click, point to **All Tasks**, click **Request New Certificate** to start the Certificate Request wizard, and then click **Next**.
6. On the **Certificate Template** page, select a certificate template.
7. If necessary, click **Advanced options** to specify the following information:
 - The cryptographic service provider (CSP).
 - Whether to enable strong private key protection.

Enabling strong private key protection ensures that you are prompted for a password every time the private key is used. This is useful if you want to make sure that the private key is not used without your knowledge.
 - The name of the CA that issues the certificate, if more than one CA is available.
8. Type a display name for the certificate.
9. When the Certificate Request wizard is finished, click **Install Certificate**.

Note You can automate the process of requesting, receiving, and installing a certificate by using automatic certificate settings in public key policies. This enables automatic certificate enrollment for computers associated with a Group Policy, which eliminates the need for an administrator to explicitly enroll each computer-related certificate.

Using the Certificate Services Web Pages

Topic Objective

To identify the tasks associated with the Certificate Services Web Pages.

Lead-in

Each CA that is installed on a Windows 2000–based server has Web pages that users can access to submit basic and advanced certificate requests.

- **Submitting a Certificate Request**
- **Submitting an Advanced Certificate Request**
- **Checking a Pending Request**

*****ILLEGAL FOR NON-TRAINER USE*****

Each CA that is installed on a Windows 2000–based server has Web pages that users can access to submit basic and advanced certificate requests. The Web pages are the only way that users can request certificates from a stand-alone CA. Web pages are optional for users who want to request certificates from enterprise CAs.

Submitting a Certificate Request

To submit a certificate request through the Web:

1. In Internet Explorer, connect to `http://server/certsrv` (where *server* is the name of the Windows 2000–based Web server where the CA that you want to access is located).
2. On the **Welcome** page, under **Select a task**, click **Request a certificate**, and then click **Next**.
3. On the **Choose Request Type** page, under **User certificate request**, select the type of certificate that you want to request, and then click **Next**.
4. Type your identifying information for the certificate request if necessary, and then click **Submit**.

Explain that the procedure that an administrator uses to issue a certificate will be presented later in the module.

By default, on a stand-alone CA, a certificate is not available to install until the CA has issued the certificate.

Note An enterprise CA requires the requester to be authenticated and generates a certificate based on the information in Active Directory.

Submitting an Advanced Certificate Request

Many types of certificate requests, such as those for IPSec, client authentication, and server authentication, require the submission of an advanced certificate request. To request an advanced certificate through Web-based enrollment:

1. In Internet Explorer, connect to `http://server/certsrv` (where *server* is the name of the Windows 2000–based Web server where the CA that you want to access is located).
2. On the **Welcome** page, under **Select a task**, click **Request a certificate**, and then click **Next**.
3. On the **Choose Request Type** page, click **Advanced** request, and then click **Next**.
4. On the **Advanced Certificate Requests** page, click **Submit a certificate request to this CA using a form**, and then click **Next**.
5. Type your identifying information for the certificate request if necessary, and then click **Submit**.

Important When requesting a certificate for a computer, you must select the **Store in local machine store** check box.

By default, on a stand-alone CA, a certificate is not available to install until the CA has issued the certificate.

Checking a Pending Request

To check a pending certificate:

1. In Internet Explorer, connect to `http://server/certsrv`, where *server* is the name of the Windows 2000–based Web server where the CA that you want to access is located.

Important To check a certificate by using Internet Explorer, you must use the same installation of Internet Explorer that you used to request the certificate.

2. On the **Welcome** page, under **Select a task**, click **Check on a pending certificate**, and then click **Next**.
3. Select the certificate request that you want to check, and then click **Next**.
4. Check the pending certificate requests. The status of the pending certificate requests is one of the following:
 - **Still pending.** The administrator of the CA has not yet issued the certificate. Click **Remove** to remove the certificate request.
 - **Issued.** Click **Install this certificate** to install the certificate.
 - **Denied.** Contact the administrator of the CA for further information.

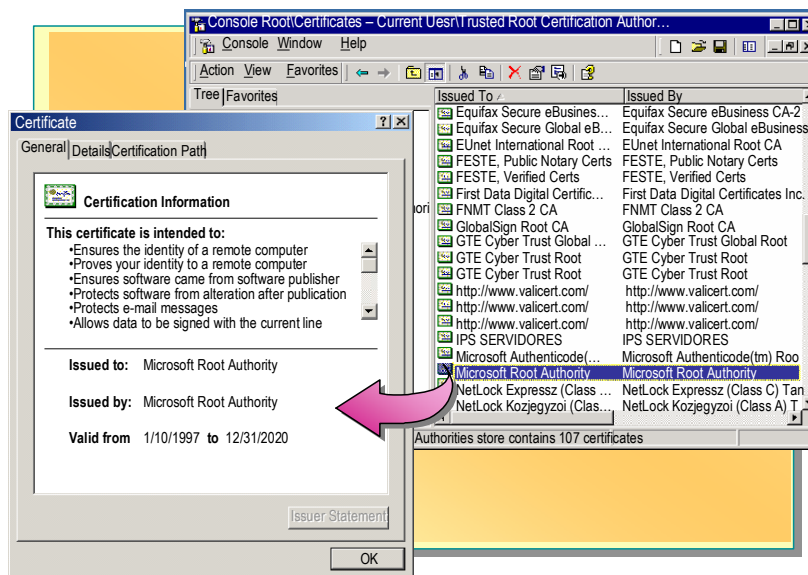
Viewing Certificates

Topic Objective

To illustrate the interface used to view certificates.

Lead-in

Windows 2000 stores certificates locally on the computer that requested the certificate.



*****ILLEGAL FOR NON-TRAINER USE*****

Explain that the user profile contains the default certificate store for a user. You can increase security by moving a user authentication certificate to a smart card.

Windows 2000 stores computer certificates locally on the computer that requested the certificate, and stores user certificates in the user's profile. The storage location is called the *certificate store*. Certificates can be displayed by purpose or by logical stores. Displaying certificates by logical stores is the Certificates default.

By opening an MMC console that contains the Certificates snap-in, you can display the certificate store for a user, a computer, or a service, as shown in the following table.

Folder name	Contents
Personal	Certificates associated with private keys to which you have access.
Trusted Root Certification Authorities	Implicitly trusted Certificate Authorities.
Enterprise Trust	Certificate trust lists. A certificate trust list provides a mechanism for trusting self-signed root certificates from other organizations and limiting the purposes for which these certificates are trusted.
Intermediate Certification Authorities	Certificates that a CA issues to a subordinate CA. The subordinate CA could also receive a certificate from either trusted root CAs or other intermediate CAs.
Active Directory User Object	Certificates associated with your user object and published in Active Directory.
REQUEST	Pending or rejected certificate requests.
SPC	Certificates from import files.

You can view information about the fields, extensions, and properties that define an issued certificate by double-clicking any certificate displayed in the certificate store.

◆ Managing Certificates

Topic Objective

To identify the topics related to exporting and importing certificates.

Lead-in

The Certificates snap-in provides administrative tools to manage certificates.

- Issuing Certificates
- Revoking Certificates
- Publishing a Certificate Revocation List
- Importing and Exporting Certificates

*****ILLEGAL FOR NON-TRAINER USE*****

In addition to storing certificates, the Certificates snap-in provides administrative tools to issue, revoke, and publish a CRL, and import and export certificates. Administrators can use the Certificates snap-in to manage certificates for themselves and other users, a computer, or a service.

Issuing Certificates

Topic Objective

To identify the tasks related to issuing certificates.

Lead-in

When a user submits a certificate request to a stand-alone CA, it is considered pending until the administrator of the CA approves or rejects the request.

- Rejecting a Certificate Request
- Issuing a Certificate Request

*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

An administrator only needs to review certificates on a stand-alone CA that is configured to have every incoming certificate request marked as pending.

When a user submits a certificate request to a stand-alone CA, the request is considered pending until the administrator of the CA approves or rejects it. The user must access the Certificate Services Web pages to check the status of pending certificates.

Note The following procedure applies *only* to a stand-alone CA that is configured to mark every incoming certificate request as pending.

Reviewing Pending Certificate Requests

To review pending certificate requests:

1. Open Certification Authority.
2. In the console tree, click **Pending Requests**.
3. In the details pane, examine the certificate request by noting the values for requester's name, e-mail address, and any other fields that you consider critical information for issuing the certificate, and then perform one of the following:

To	Do this
Reject the certificate request	Right-click the certificate request, point to All Tasks , click Deny , and then click Yes .
Issue the certificate	Right-click the certificate request, point to All Tasks , and then click Issue .

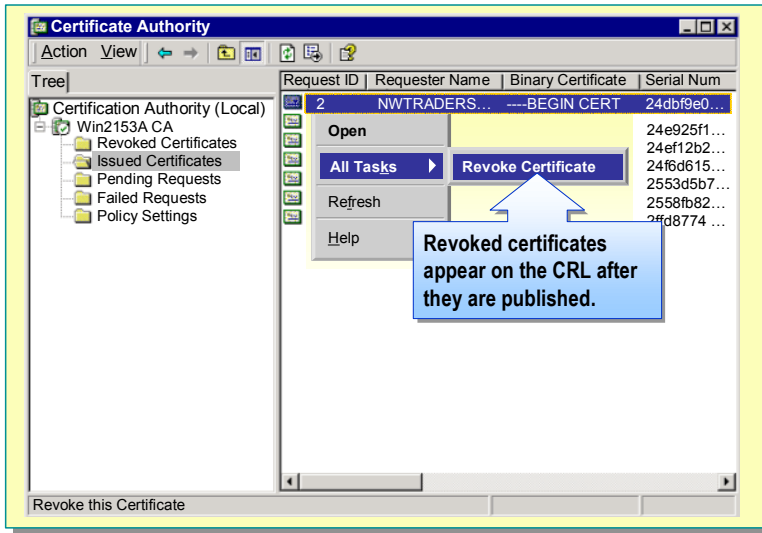
Revoking Certificates

Topic Objective

To illustrate the interface used for revoking certificates.

Lead-in

To maintain the integrity of an organization's PKI, the administrator of a CA may need to revoke certificates before they expire.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

You must publish a CRL to revoke a certificate. Revoking a certificate is not sufficient to make this information available.

To maintain the integrity of an organization's PKI, the administrator of a CA may need to revoke certificates before they expire. For example, certificates may need to be revoked if the recipient of a certificate leaves an organization, if the private key of a certificate is compromised, or if a security event affects the validity of a certificate.

An administrator revokes certificates in Certification Authority. After a certificate is revoked, it is moved to the Revoked Certificates folder. The revoked certificate will appear on the CRL the next time the CRL is published.

To revoke an issued certificate:

1. Open Certification Authority.
2. In the console tree, click **Issued Certificates**.
3. In the details pane, click the certificate that you want to revoke, right-click the certificate, point to **All Tasks**, and then click **Revoke Certificate**.
4. In the **Reason code** list, select one of the following, and then click **Yes**.
 - **Unspecified**
 - **Key Compromise**
 - **CA Compromise**
 - **Affiliation Changed**
 - **Superseded**
 - **Certificate Hold**

A certificate marked Certificate Hold can be unrevoked, left on Certificate Hold until the certificate expires, or have the reason code changed later.

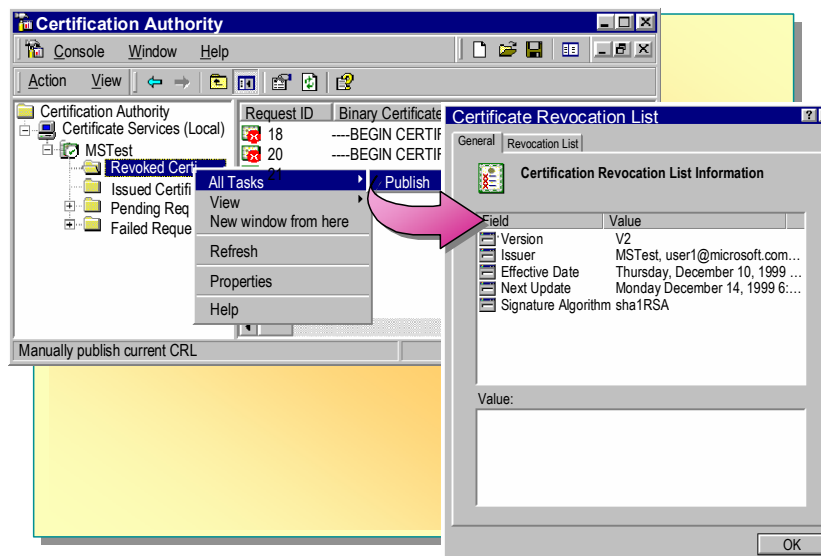
Publishing a Certificate Revocation List

Topic Objective

To illustrate the interfaces for publishing a CRL.

Lead-in

You can publish a CRL automatically or on demand.



*****ILLEGAL FOR NON-TRAINER USE*****

Key Point

Clients that have a cached copy of the previously published CRL continue to use it until its validity period has expired, even though a new CRL has been published.

A CA automatically publishes an updated CRL at an interval of time specified by the administrator of the CA. You can also publish a CRL on demand by using the CRL Publishing wizard. If you manually publish a CRL in the middle of a scheduled publish period, the CRL will still be automatically republished at the end of the current publish period.

Important Clients that have a cached copy of the previously published CRL continue to use it until its validity period has expired, even though a new CRL has been published.

To manually publish the CRL:

1. Open Certification Authority.
2. In the console tree, right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**.
3. Click **Yes** to overwrite the previously published CRL.

The CRL is published in *systemroot\system32\CertSrv\CertEnroll*. If Active Directory is available, the CRL is also published in Active Directory.

To view the newly published CRL, right-click **Revoked Certificates**, and then click **Properties**.

Importing and Exporting Certificates

Topic Objective

To identify the topics related to importing and exporting certificates.

Lead-in

The Certificates snap-in provides administrative tools for importing and exporting certificates, including certification paths and private keys, if needed.

- **Examining Certificate File Formats**
- **Importing a Certificate**
- **Exporting a Certificate**

*****ILLEGAL FOR NON-TRAINER USE*****

The Certificates snap-in provides administrative tools for importing and exporting certificates, including certification paths and private keys. You can import a certificate from another user, computer, or CA. Or, you can export a certificate for use on another computer. You can export certificates to or import certificates from several standard certificate file formats.

Examining Certificate File Formats

You can import and export certificates in the following formats:

- *Personal Information Exchange (PKCS #12)*. Enables the transfer of certificates and their corresponding private keys from one computer to another or from a computer to removable media. If a certificate was issued from a Windows 2000–based CA, the private key for that certificate is only exportable if one of the following is true:
 - The certificate is for EFS or EFS recovery.
 - The certificate was requested through the Advanced Certificate Request Web page with the **Mark keys as exportable** check box selected.
- *Cryptographic Message Syntax Standard (PKCS #7)*. Enables the transfer of a certificate and all of the certificates in its certification path from one computer to another, or from a computer to removable media.
- *DER Encoded Binary X.509*. Supports interoperability for CAs that are not on Windows 2000–based servers. DER certificate files use the .cer extension.
- *Base64 Encoded X.509*. Supports interoperability for CAs that are not on Windows 2000–based servers. Base64 certificate files use the .cer extension.

Importing a Certificate

When you import a certificate, you copy the certificate from a file that uses a standard certificate storage format to a certificate store for your user account or your computer account.

To import a certificate:

1. Open an MMC console that contains the Certificates snap-in.
2. In the console tree, expand **Personal**, and then click **Certificates** below it.
3. Right-click **Certificates**, point to **All Tasks**, and then click **Import**.
4. Provide the following information in the Certificate Import wizard:
 - Specify the name of the file to import.
 - If the file is a PKCS #12 file, type the password used to encrypt the private key. If you want the private key to be exportable, select the appropriate check box, and then select to enable strong private key protection, if necessary.
 - Select the appropriate check box either to automatically place the certificate in a predefined certificate store or to specify another storage location.

Exporting a Certificate

When you export a certificate, you are copying the certificate from its certificate store to a file that uses a standard certificate storage format.

To export a certificate:

1. Open an MMC console that contains the Certificates snap-in.
2. In the console tree, expand **Personal**, and then click **Certificates** below it.
3. Right-click **Certificates**, point to **All Tasks**, and then click **Export**.
4. Provide the following information in the Certificate Export wizard:
 - Select **No, do not export the private key**.

Note This option appears only if the private key is marked as exportable and you have access to the private key.

- Select the file format that you want to use to store the exported certificate.
- If you are exporting the certificate to a PKCS #7 file, you also have the option to include all certificates in the certification path.
- Specify the name of the file to export.

After the Certificate Export wizard is finished, the certificate will remain in the certificate store. If you want to remove the certificate from the certificate store, you must delete it manually.

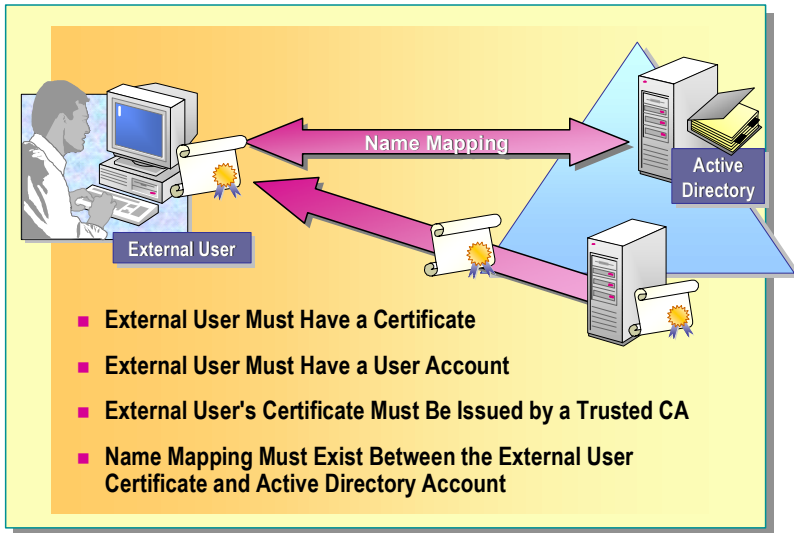
Configuring Active Directory for Certificates

Topic Objective

To identify the tasks related to configuring Active Directory for certificates

Lead-in

Your organization may need to support authentication of external users who do not have an account in Active Directory.



*****ILLEGAL FOR NON-TRAINER USE*****

Your organization may need to support authentication of external users—individuals who do not have an account in Active Directory. Authenticating external users requires the following:

- The external user must have a certificate.
- The external user must have a user account.
- The external user's certificate must be issued by a CA that is trusted by, or listed in the certificate trust list for, the site, domain, or organizational unit in which you have created the user account.
- You must create a *name mapping* between the external user certificate and the Active Directory account that you have created for authenticated access.

Any external user whose client program presents a mapped certificate can then access the permitted locations published on the appropriate Web site for your organization. The authentication process is transparent to the external user.

Setting Up a CA Trust

If your organization has its own Windows 2000 enterprise root CA and uses Active Directory, Windows 2000 automatically distributes the root certificates. Distribution of any other root certificates requires Group Policy.

Note For more information about setting up a CA trust, see the white paper *Windows 2000 Certificate Services*, under **Additional Reading** on the Web page on the Student Materials compact disc.

Mapping Accounts to Certificates

1. Open Active Directory Users and Computers from the **Administrative Tools** menu.
2. Click **Active Directory Users and Computers**. On the **View** menu, click to select **Advanced Features**.
3. In the console tree, double-click the domain name.
4. Click the container where the user account is located.
5. In the details pane, right-click the user account to which you want to map a certificate, and then click **Name Mappings**.
6. On the **X.509 Certificates** tab, click **Add**.
7. In the **Add Certificate** dialog box, type the name and path of the .cer file that contains the certificate that you want to map to this user account, click **Open**, and then do one of the following:

To	Do this
Map the certificate to one account (one-to-one mapping)	Confirm that both the Use Issuer for alternate security identity and the Use Subject of alternate security identity check boxes are selected.
Map any certificate that has the same subject to the user account, regardless of the issuer of the certificate (many-to-one mapping)	Clear the Use Issuer for alternate security identity check box and confirm that the Use Subject of alternate security identity check box is selected.
Map any certificate that has the same issuer to the user account, regardless of the subject of the certificate (many-to-one mapping)	Clear the Use Subject of alternate security identity check box and confirm that the Use Issuer for alternate security identity check box is selected.

Troubleshooting Certificate Services

Topic Objective

To identify the tasks related to troubleshooting Certificate Services.

Lead-in

There are important troubleshooting tasks for administering Certificate Services.



Reviewing Event Logs



Using Diagnostics Mode



Troubleshooting a CA



Confirming the Validity of a Certificate

*****ILLEGAL FOR NON-TRAINER USE*****

Determining the validity of the certificates issued is an important troubleshooting task for administering Certificate Services. Troubleshooting may also involve verifying the public/private key combination.

Reviewing Event Logs

The first step in troubleshooting Certificate Services is to review the Windows 2000 event logs for any indication of what the problem is.

Using Diagnostics Mode

You can obtain detailed diagnostics information about Certificate Services by running Certificate Services in diagnostics mode.

Note For more information about diagnostics mode, see “Troubleshooting under Certificate Services” in Windows 2000 Help.

Troubleshooting a CA

If you cannot access the Certificate Services Web pages, or you cannot create certificates by using the Web pages, check the authentication methods for your Web server.

Note For more information about troubleshooting a CA, see “Troubleshooting under Certificate Services” in Windows 2000 Help.

Confirming the Validity of a Certificate

The **Certificate** dialog box lists the details of the certificates, including any problems with the certificates.

To confirm the validity of a certificate:

Open an MMC console that contains the Certificates snap-in, and then double-click the certificate.

Possible problems include:

- *Certificate was created by a nontrusted CA.* If a nontrusted CA has issued the certificate, you must add the CA to the list of trusted CAs.
- *Certificate has expired.* If the CA has expired, you must renew it.
- *Certificate has been revoked.* If the certificate has been revoked, contact an administrator for the CA that issued the certificate to determine why the certificate was revoked, and then request a new certificate. If a CA certificate is revoked, then any CAs that stem from that CA are also revoked.

Lab A: Installing and Configuring Certificate Services

Topic Objective

To introduce the lab.

Lead-in

In this lab, you will create a stand-alone CA



*****ILLEGAL FOR NON-TRAINER USE*****

Explain the lab objectives.

Objectives

After completing this lab, you will be able to:

- Install a stand-alone CA.
- Request a certificate from a CA.
- Issue a certificate.

Prerequisite

Before working on this lab, you must have knowledge about the roles that CAs have in Windows 2000.

Key Points

The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Lab Setup

To complete this lab, you need the following:

- A computer running Windows 2000 Advanced Server that is configured as a domain controller
- A partner with a similarly configured computer

Important One computer will hold a stand-alone root CA, and the other computer will hold a stand-alone subordinate CA. The computer of the student with the higher student number will act as the stand-alone root CA; the computer of the student with the lower student number will act as the stand-alone subordinate CA. Determine the role that your computer will have before you start the lab.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Scenario

Your organization requires business partners to access a database of product specifications at Northwind Traders over the Internet. You must ensure that the information remains confidential. To ensure security of the network traffic between the computers that will communicate across the Internet, you will use certificates to encrypt IP traffic between these computers. Northwind Traders' specifications for a PKI structure call for a stand-alone root CA and stand-alone subordinate CAs. You must install the required CAs. You must also ensure that all computers that communicate with each other across the Internet have a valid certificate so that all IP traffic between these computers can be encrypted.

Estimated time to complete this lab: 45 minutes

Exercise 1

Creating a Stand-Alone Root CA

Scenario

Northwind Traders requires a stand-alone root CA. This CA will be at the top of the certification chain for other CAs that will issue certificates for Northwind Traders.

Goal

In this exercise, you will create a stand-alone root CA.

Tasks	Detailed Steps
 Complete the following procedure only on the computer that will hold the root CA.	
1. Create a stand-alone root CA that has the name of your computer.	- Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. - In Control Panel, double-click Add/Remove Programs. - In Add/Remove Programs, click Add/Remove Windows Components. - In the Windows Components wizard, on the Windows Components page, select the Certificate Services check box. - In the Microsoft Certificate Services message box, click Yes, and then click Next. - On the Certification Authority Type page, verify that Stand-alone root CA is selected, and then click Next. - On the CA Identifying Information page, enter the following information: CA name: <i>server CA</i> (where <i>server</i> is the name of your computer) Organization: the name of your company or organization Organizational unit: the name of your organizational unit or department City: the name of your city State or province: the name of your state or province Country/region: the two-letter code of your country or region E-mail: your e-mail address CA description: Certification Authority for Windows 2000 class Valid for: 2 Years - Click Next. - On the Data Storage Location page, click Next. - In the Microsoft Certificate Services dialog box, click OK to stop Internet Information Services. - In the Files Needed dialog box, type \\London\Setup\Winsrc and then click OK. - When the configuration process is complete, click Finish. - Close all open windows.

Exercise 2

Creating a Stand-Alone Subordinate CA

Scenario

Northwind Traders requires a stand-alone subordinate CA. This CA will issue certificates for Northwind Traders that business partners can use to connect securely to your network.

Goal

In this exercise, you will create a stand-alone subordinate CA.

Tasks	Detailed Steps
 Complete the following procedures only on the computer that will hold the subordinate CA. Ensure that your partner has completed the preceding exercise before you continue.	
1. Add your partner's CA as a trusted root CA.	- Log on as administrator@domain.nwtraders.msft (where <i>domain</i> is the name of your domain) with a password of password. - Click Start, and then click Run. - In the Open box, type http://partner_server/certsrv (where <i>partner_server</i> is the name of your partner's computer), and then click OK. - If the Internet Connection wizard appears, complete the wizard by specifying that you want to connect through a local area network (LAN). Accept the defaults for a LAN connection, and do not set up an Internet mail account. - In Internet Explorer, on the Welcome page, click Retrieve the CA certificate or certificate revocation list, and then click Next. - On the Retrieve The CA Certificate or Certificate Revocation List page, click Install this CA certification path. - In the Root Certificate Store dialog box, click Yes. - When the CA Certificate Installed page appears, close Internet Explorer.
2. Create a stand-alone subordinate CA that has the name of your computer. Make the subordinate CA a subordinate of your partner's root CA.	- In Control Panel, double-click Add/Remove Programs. - In Add/Remove Programs, click Add/Remove Windows Components. - In the Windows Components wizard, on the Windows Components page, select the Certificate Services check box. - In the Microsoft Certificate Services message box, click Yes, and then click Next. - On the Certification Authority Type page, select the Stand-alone subordinate CA check box, and then click Next.

(continued)

Tasks	Detailed Steps
2. (continued)	f. On the CA Identifying Information page, type the following information: CA name: <i>server CA</i> (where <i>server</i> is the name of your computer) Organization: the name of your company or organization Organizational unit: the name of your organizational unit or department City: the name of your city State or province: the name of your state or province Country/region: the two-letter code of your country or region E-mail: your e-mail address CA description: Certification Authority for Windows 2000 class Valid for: determined by parent CA g. Click Next. h. On the Data Storage Location page, click Next. i. On the CA Certificate Request page, in the Computer name box, type <i>partner_server</i> (where <i>partner_server</i> is the name of your partner's computer), and then press TAB. j. Click Next. k. In the Microsoft Certificate Services dialog box, click OK to stop Internet Information Services. l. In the Files Needed dialog box, type <code>\\London\Setup\Winsrc</code> and then click OK. m. Read the text in the Microsoft Certificate Services message box, and then click OK. n. Read the text in the Microsoft Certificate Services message box, and then click OK. o. When the configuration process is complete, click Finish.
	Complete the following procedure only on the computer that holds the root CA. Ensure that your partner has completed the preceding procedure before you continue.
3. Issue a certificate for a subordinate CA on the root CA.	a. Open Certification Authority from the Administrative Tools menu. b. In the console tree, expand <i>server CA</i> (where <i>server</i> is the name of your computer), and then click Pending Requests. c. In the details pane, right-click your partner's certificate request, point to All Tasks, and then click Issue. d. In the console tree, click Issued Certificates, and then verify that the certificate for your partner's CA has been issued. e. Minimize Certification Authority.
	Complete the following procedure only on the computer that holds the root CA. Ensure that your partner has completed the preceding procedure before you continue.

(continued)

Tasks	Detailed Steps
4. Install a certificate for the subordinate CA.	a. Open Certification Authority from the Administrative Tools menu. b. In the console tree, right-click <i>server CA</i> (where <i>server</i> is the name of your computer), point to All Tasks, and then click Install CA Certificate. c. In the Select file to complete CA installation dialog box, click Cancel. d. In the CA Certificate Request dialog box, in the Computer Name box, verify that the name of your partner's computer appears. e. In the Parent CA box, click <i>partner_server CA</i> (where <i>partner_server</i> is the name of your partner's computer), and then click OK.  The CA installation completes and the CA starts. f. Minimize Certification Authority.

Exercise 3

Requesting a Computer Certificate

Scenario

After all of the CAs in your organization have been configured, you must assign a computer certificate that allows encrypting of all IP traffic to each computer.

Goal

In this exercise, you will request a computer certificate for your computer.

Tasks	Detailed Steps
Complete the following procedure on both student computers.	
1. Use Internet Explorer to request an IPSec certificate for your computer from the CA on your computer.	a. Click Start, and then click Run. b. In the Open box, type http://server/certsrv (where <i>server</i> is the name of your computer), and then click OK. c. If the Internet Connection wizard appears, complete the wizard by specifying that you want to connect through a LAN. Accept the defaults for a LAN connection, and do not set up an Internet mail account. d. In Internet Explorer, on the Welcome page, verify that Request a certificate is selected, and then click Next. e. On the Choose Request Type page, click Advanced request, and then click Next. f. On the Advanced Certificate Requests page, verify that Submit a certificate request to this CA using a form is selected, and then click Next. g. On the Advanced Certificate Request page, enter the following information: Name: your name E-mail: your e-mail address Company: the name of your company or organization Department: the name of your department City: the name of your city State or province: the name of your state or province Country/Region: the two-letter code of your country or region. h. Under Intended Purpose, click IPSec Certificate. i. Under Key Options, select the Use local machine store check box, and then click Submit. j. When the Certificate Pending page appears, minimize Internet Explorer.

(continued)

Tasks	Detailed Steps
2. Use Certification Authority to issue the certificate that you requested.	a. Restore Certification Authority. b. In the console tree, expand <i>server</i> CA (where <i>server</i> is the name of your computer) if necessary, and then click Pending Requests. c. On the Action menu, click Refresh. d. In the details pane, right-click your certificate request, point to All Tasks, and then click Issue. e. In the console tree, click Issued Certificates, and then verify that the certificate for your computer has been issued. f. Close Certification Authority.
3. Use Internet Explorer to install the certificate that you issued.	a. Restore Internet Explorer. b. In the Address box, type http://server/certsrv (where <i>server</i> is the name of your computer), and then press ENTER. c. On the Welcome page, click Check on a pending certificate, and then click Next. d. On the Check On A Pending Certificate Request page, verify that the certificate request that you submitted is listed, and then click Next. e. On the Certificate Issued page, click Install this certificate. f. When the Certificate Installed page appears, close Internet Explorer.

(continued)

Tasks	Detailed Steps
4. Create an MMC console that contains the Certificates snap-in for your computer, and then confirm that the IPsec certificate has been issued to your computer.	a. Click Start, and then click Run. b. In the Open box, type mmc and then click OK. c. Maximize the Console Root window. d. In the Console1 – [Console Root] window, on the Console menu, click Add/Remove Snap-in. e. In the Add/Remove Snap-in dialog box, click Add. f. In the Add Stand-alone Snap-in dialog box, click Certificates, and then click Add. g. In the Certificates snap-in dialog box, click Computer account, and then click Next. h. In the Select Computer dialog box, verify that Local computer is selected, and then click Finish. i. Click Close to close the Add Stand-alone Snap-in dialog box. j. Click OK to close the Add/Remove Snap-in dialog box. k. On the Console menu, click Save As. l. Save the console file as Computer Certificates in the default location. m. In the console tree, expand Certificates, expand Personal, and then under Personal, click Certificates. n. On the Action menu, click Refresh. o. In the details pane, right-click the certificate that you issued to name (where name is your name), and then click Open. p. In the Certificate dialog box, verify that the certificate is intended to allow secure communication on the Internet and that the certificate is valid, and then click OK. q. Close Computer Certificates without saving changes.

Exercise 4

Removing Certificate Services

Scenario

The computers that host the CA at Northwind Traders will be removed from the network and replaced with other computers. After explaining to management that you should remove the current certification path from all computers in your company as soon as new CAs have been established, you proceed to remove all existing CAs.

Goal

In this exercise, you will remove Certificate Services from your computer.

Task	Detailed Steps
1. Remove Certificate Services.	- In Control Panel, double-click Add/Remove Programs. - In Add/Remove Programs, click Add/Remove Windows Components. - In the Windows Components wizard, on the Windows Components page, clear the Certificate Services check box, and then click Next. - When the configuration process is complete, click Finish. - Close all open windows, and then log off.

Review

Topic Objective

To reinforce module objectives by reviewing key points.

Lead-in

The review questions cover some of the key concepts taught in the module.

- Introduction to Public Key Infrastructure (PKI)
- Deploying Certificate Services
- Using Certificates
- Managing Certificates
- Configuring Active Directory for Certificates
- Troubleshooting Certificate Services

*****ILLEGAL FOR NON-TRAINER USE*****

1. Which of the following functions can a PKI perform?
 - a. Authentication of the originator of a message or a computer.
 - b. Confirmation of the physical location of a computer.
 - c. Confidentiality of a message.
 - d. Confirmation of the security privileges that a user has.

A and C.

2. What needs to be present before you can install an enterprise subordinate CA?

In a domain, you must have Active Directory and an enterprise root CA. On a stand-alone computer, you need only an enterprise root CA.

3. What are the methods for requesting a certificate, and which types of CAs support each of them?

The Certificate Request wizard and the Certificate Services Web pages. Enterprise CAs support both types. Stand-alone CAs only support the Web pages.

4. You revoke a certificate, but it does not appear in the CRL. What is the problem?

The time interval specified for publishing the CRL has not elapsed. To make the updated the CRL immediately available, you must publish the CRL manually.

5. You have requested a certificate from a stand-alone CA. What must you do before you can use the certificate?

You must wait for an administrator to issue the certificate. Then you must check the pending certificate and install the certificate.