Report Number: C4-059R-00

Guide to the Secure Configuration and Administration of Microsoft® Windows® 2000 Certificate Services

(Checklist Format)

Network Applications Team
of the
Systems and Network Attack Center (SNAC)

Author:
Sheila Christman

Updated: July 3, 2001
Version 2.0.1

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2KGuides@nsa.gov

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- This document may contain recommended settings for the system Registry. Windows 2000 Certificate Services can be severely impaired or disabled with incorrect changes or accidental deletions when using a Registry editor (Regedt32.exe or Regedit.exe) to change the system configuration.
- Currently, there is no **undo** command for deletions within the Registry. Registry editor prompts the user to confirm the deletions if **Confirm on Delete** is selected from the options menu. When a key is deleted, the message does not include the name of the key being deleting. Therefore, check selection carefully before proceeding.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of April 30, 2001. See Microsoft's web page for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Acknowledgements

Some parts of this document were drawn from Microsoft copyright materials with their permission.

Trademark Information

Microsoft, MS-DOS, Windows, Windows 2000, Windows NT, Windows 98, Windows 95, Windows for Workgroups, and Windows 3.1 are either registered trademarks or trademarks of Microsoft Corporation in the U.S.A. and other countries.

All other names are registered trademarks or trademarks of their respective companies.

Table of Contents

Warnings ..... **iii**

Acknowledgements ..... **v**

Trademark Information ..... **vi**

Table of Figures ..... **viii**

Table of Tables ..... **ix**

Introduction **1**

Getting the Most from this Guide *2*

Commonly Used Names *2*

About the Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Service *3*

An Important Note About Operating System Security *3*

Chapter 1 Windows 2000 Certificate Services **5**

Pre-Installation Considerations *5*

Installation *6*

Root CAs *7*

Subordinate CAs *12*

Renewing CA Certificates *16*

Chapter 2 Managing Certificates with the MMC **18**

Certificate Services Snap-Ins *18*

Certificate Store and Active Directory *20*

Certificate Revocation Lists (CRLs) *27*

Chapter 3 Additional Security Issues **30**

Antiviral Program *30*

Audits *30*

Certificate Service Web Pages *31*

Chapter 4 Backups **36**

Backup Procedures *36*

Appendix A Further Information **40**

Table of Figures

Figure 1 Choosing Stand-alone Root CA for Certification Authority Type 7
Figure 2 Stand-Alone Certificate – Advanced Options 9
Figure 3 Stand-Alone - CA Identifying Information 10
Figure 4 Stand-Alone - Data Storage Location 11
Figure 5 Choosing Subordinate CA 12
Figure 6 Subordinate CA - Advanced Options 13
Figure 7 Subordinate CA - Identifying Information 14
Figure 8 Subordinate CA - Data Storage Location 14
Figure 9 Renewing CA Certificate 17
Figure 10 Certification Authority Snap-In 17
Figure 11 Slecting Certificate Templates 18
Figure 12 Setting Security Permissions for CA Control 19
Figure 13 Adding Certificate Snap-in 20
Figure 14 Selecting Account for Certificate Management 21
Figure 15 Creating Separate Snap-ins 21
Figure 16 Selecting File to Import in the Certificate Import Wizard 22
Figure 17 Selecting Location for Certificate Store 22
Figure 18 Deleting Untrusted CA 23
Figure 19 Expanding Personal Folder 23
Figure 20 Selecting a Certificate Template 25
Figure 21 Delegating Control of Templates 26
Figure 22 Delegating Control of the Following Objects 27
Figure 23 Sample Data for Filtering Information 31
Figure 24 Sample Screens on Certificate Service Web Pages 32
Figure 25 Example of Advanced Certificate Request 33
Figure 26 Securing Certificate Service Web Pages 34
Figure 27 Selecting Items to Back-up 37
Figure 28 Selecting a Password for CA Backup 38
Figure 29 Completion of CA Backup Wizard 38

Table of Tables

Table 1 Summary of Certificate Server Documentation.....1
Table 2 Permissions on Certificate Directories 3
Table 3 Details of “Advanced Options” for Root CA 8

This Page Intentionally Left Blank

Introduction

This document is one of two documents that describe how to securely install, configure, and administer the Windows 2000 Certificate Services. The focus of these documents is security-relevant information pertaining to the installation and administration of the service. Although Microsoft's Internet Information Service (IIS) is required to enable users to request certificates through web pages, this document does not provide instructions for securely installing and managing IIS. That information, along with detailed information on using certificates with Internet Information Service, can be found in the document entitled *Secure Installation and Configuration of Microsoft's Internet Information Service 5.0*.

This document is intended for the reader who is already familiar with public key cryptography but needs to understand how to install, configure, and administer Microsoft's Certificate Services in a more secure manner. The information presented here is written in a direct and concise manner in deference to this intended audience. A brief description of public key cryptography is given as background information.

Some Certificate Services' security issues and corresponding configuration and administrative actions are very specific to the way the product is being used. For this reason, it is difficult in some areas to recommend specific, concrete actions. Instead, a summary is offered which describes the concerns and recommends solutions that the administrator must tailor to his/her own environment.

It is also important to realize that many organizations have developed policies regarding the structure and administration of certificate services. Given the wide audience intended for this document, those specific policies could not be considered. It is up to the reader to apply these recommendations in light of local policy.

Summary of Certificate Server Documentation		
Document	**Contents**	**Target audience**
Guide to the Secure Configuration and Administration of Microsoft's Windows 2000 Certificate Services	• A detailed look at the secure installation and configuration of Certificate Services in Windows 2000 and a description of how these services can be used in the Windows 2000 environment.	• Knowledgeable Windows 2000 administrators who may be new to Microsoft's Certificate Services
Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services (Checklist Format – this document)	• A secure installation and configuration guide in checklist format with no detailed explanations	• Windows 2000 administrators who are familiar with Microsoft's Certificate Services

Table 1 Summary of Certificate Server Documentation

PLEASE NOTE THAT THESE DOCUMENTS ASSUME THAT THE READER IS A KNOWLEDGEABLE WINDOWS 2000 ADMINISTRATOR. A knowledgeable Windows 2000 administrator is defined as someone who can create and manage accounts and groups, understands how Windows 2000 performs access control, understands how to set account policies and user rights, is familiar with how to setup auditing and read audit logs, etc. These documents do not provide step-by-step instructions on how to perform these basic Windows 2000 administrative functions. It is assumed that the reader is capable of implementing basic instructions regarding Windows 2000 administration without the need for detailed instructions.

WARNING: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to the Microsoft Windows 2000 Certificate Service and its implementation.

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 or network security.

Getting the Most from this Guide

The following list contains suggestions to successfully secure the configuration and administration of Windows 2000 Certificate Service according to this guide:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Omitting or deleting steps can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system before implementing any of the recommendations in this guide
- Follow the security settings that are appropriate for your environment.

Commonly Used Names

Throughout this guide the network name "xtest.gov" and will be used in the examples, screenshots, and listings.

WARNING: It is extremely important to replace "xtest.gov" with the appropriate network name for the networks being secured. These names are not real networks and have been used for demonstration purposes only.

About the Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Service

This document consists of the following chapters:

Chapter 1, "Windows 2000 Certificate Services,"

Chapter 2, "Managing Certificates with the MMC,"

Chapter 3, "Additional Security Issues,"

Chapter 4, "Backups,"

Appendix A, "Further Information," contains a list of resources referenced in this guide

An Important Note About Operating System Security

It is very important to keep track of permissions on Certificate directories. The default settings should be changed to reflect the following. Think carefully before granting others access to these directories. The more access given, the more likely it is that there could be a compromise.

Directory	User/Group	Permissions
%Systemroot%\system32\Certsrv	Administrators	Full Control
	Authenticated Users	Read&Execute, List Folder Contents, Read
	System	Full Control
%Systemroot%\system32\CertLog	Administrators, Security group (could be Enterprise Admins), System	Full Control
Specified Shared Folder location	Administrators, System, Enterprise Admins	Full Control

Table 2 Permissions on Certificate Directories

File permissions, registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on Certificate Services security.

The recommended source of information for how to securely configure the Windows 2000 server and workstation is NSA's Windows 2000 security guide. This guide is comprised of a series of documents covering various aspects of Windows 2000 security, which is available on the same media as this document, or can be obtained by calling 1-800-688-6115. It is important to implement this guide on the server running Certificate Services.

This Page Intentionally Left Blank

Chapter

1

Windows 2000 Certificate Services

Microsoft Windows 2000 Certificate Services offers an integrated public key infrastructure (PKI) that enables the secure exchange of information across the Internet, extranets, and intranets. PKI refers to a system of digital certificates and certificate authorities (CAs) that verify and authenticate the validity of each party involved in an electronic transaction. Certificate Services, when implemented, help eliminate the threats to computer systems by providing authentication, non-repudiation, and integrity security services. The installation instructions provided in this document assume the recommended PKI hierarchy (stand-alone root CAs and subordinate enterprise CAs).

Pre-Installation Considerations

- Invoke the Windows 2000 Operating System security guidelines. File permissions, Registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on Certificate Services security.

- Check for hotfixes/patches and install them as directed, along with the latest service pack available from Microsoft. Available patches can be found at the Microsoft Download Center at http://www.microsoft.com/downloads. At the time of this writing, Microsoft had released no hotfixes or patches for Windows 2000 Certificate Services.

Prior to configuring the Certificate Services, determine the hierarchy of the PKI. The number of CAs will depend on the size of the user community being serviced.

- Implement a three-tier hierarchy consisting of at least one root CA that only issues intermediate subordinate CA certificates. Implementing a three-tier CA hierarchy will provide flexibility and insulate the root CA from attempts to compromise its private key by malicious individuals. In small intranets, a two-tier hierarchy may be implemented as long as all CAs are located in a physically protected environment.

- Place the root CA machine where it will be physically secure; i.e., behind a locked door where only authorized personnel can gain physical access to it. Ideally, the root CA will have no network connectivity and will not be a member of any domain. During installation, the root CA may have network connectivity to ease the administrative burden of publishing the root certificate to Active Directory. Once installed, however, the root CA should be removed from the network.

- Determine how many CAs will be needed to issue end-entity certificates. Consider having more than one CA available for enrollment into a forest, ensuring at least one CA is always available to process requests.

- Determine the number of intermediate subordinate CAs needed to issue certificates to the CAs providing end-entity certificates.

- Determine who in the enterprise will be permitted to enroll for certificates.

- Determine the types of certificates each CA will issue (user, client authentication, certificate trust list signing, secure e-mail, etc.). The available templates offered by a CA will depend on the types of certificates the administrator permits the CA to issue. The Microsoft Management Console Help utility has a comprehensive list of certificate templates with a description of the type of certificate the template represents. (Perform a search on "Certificate Templates" to access this table.)

Answer the following questions to determine which policy module to choose when installing each of the CAs in the enterprise.

- Will you maintain your own root CA or require services from an external CA? When you choose to trust a root certificate, you are also choosing to trust certificates signed by that root. Maintaining your own stand-alone root CA provides more control over its security.

- Are the services required to support users and computers outside of a Windows 2000 domain? A stand-alone policy module is required for a CA that supports an environment that is not entirely Windows 2000.

- Are the services required for a Windows 2000 domain (intranet) only? If so, implement the enterprise policy module on all subordinate CAs.

Installation

Two choices for a policy module are available during the installation of Certificate Services: enterprise policy and stand-alone policy. A custom policy module can also be created; however, you must install the stand-alone policy first, and then replace it with the custom policy module. The *Microsoft Platform Software Development Kit* has more information on creating custom policies for CAs. The policy selected will determine how the CA will process certificate requests, issue certificates, revoke certificates, and publish CRLs. The two policies also differ in how they handle interaction with Active Directory, authentication, and the use of templates.

The CAs' private keys provide the basis for trust in the certification process. For this reason, cryptographic hardware modules may be used to provide tamper-resistant key storage and to isolate the cryptographic operations from other software running on the server. Cryptographic hardware modules greatly reduce the likelihood of a CA's key being compromised.

Use hardware modules to secure signing keys of at least the root CAs. Prior to using a cryptographic service provider (CSP) other than the software CSPs included with Windows 2000, confirm with the vendor that it can work with Microsoft's Certificate Services. If it does, ask the vendor for documentation explaining how to operate Certificate Services with their CSP.

Root CAs

(Most of this information was taken from Microsoft's "Install a stand-alone root certification authority" Help page)

These instructions assume the installation of the recommended stand-alone root CA. If your environment requires the installation of an enterprise root CA, see the other document in this set, *Guide to the Secure Configuration and Administration of Windows 2000 Certificate Services*, for step-by-step instructions.

- Log on to the system as an Administrator, or if you have Active Directory, log on to the system as a Domain Administrator.
- Click **Start**, point to **Settings**, and then click **Control Panel**.
- Double-click **Add/Remove Programs** and then click **Add/Remove Windows Components**.
- In the Windows Components wizard, select the **Certificate Services** check box. A dialog box will appear to inform you that the computer cannot be renamed, and the computer cannot be joined to or removed from a domain after Certificate Services is installed. Click **Yes** and then click **Next**.
- Click **Stand-alone root CA**. (See **Figure 1**).

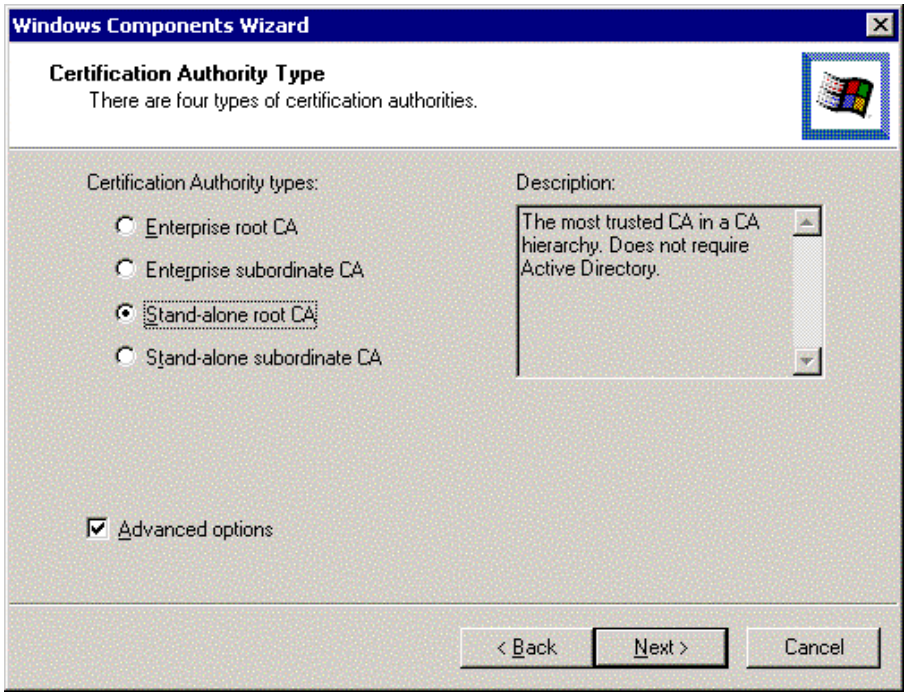


Figure 1 Choosing Stand-alone Root CA for Certification Authority Type

- Select the **Advanced options** check box to specify the options listed in .

Table 3 Details of "Advanced Options" for Root CA

Advanced option	Comment
Cryptographic service provider (CSP)	The default is the Microsoft Base Cryptographic Provider, however, it is recommended that the optional High Encryption package be installed on all CAs and the Microsoft Enhanced Cryptographic Provider v1.0 be used instead. Other enhanced CSP options are available after the installation of the High Encryption package and may also be used if they are appropriate for your configuration. Certificate Services does support third party CSPs, but you must refer to the CSP vendor's documentation for information about using their CSP with Certificate Services.
Hash algorithm	The default is SHA-1.
Existing keys	If you select this option, you can use an existing public key and private key pair instead of generating new ones. This is generally not recommended, but is useful if you are relocating or restoring a previously installed CA.
Key length	The default key length using the Microsoft Base Cryptographic Provider is 512 bits. Default key lengths for other CSPs vary. In general, the larger the key length, the more secure the key is. The High Encryption pack enables the CA to issue certificates with larger key lengths than those provided by default. Keep in mind, however, key lengths larger than 2048 take longer to generate and may have an impact on network performance. A CA should use the largest key length available that is compatible with the hardware configuration and the applications being used. Be aware that some hardware devices and older applications may not support very long key lengths (i.e., 4096 bits). For example, space limitations on some smart cards prevent the use of key lengths greater than 2048 bits. (This option is not available if you select to use existing keys).

- Change the default Key length to the longest key length available for your configuration (See Key length comment in **Table 3** above). Click **Next**. (See **Figure 2**).

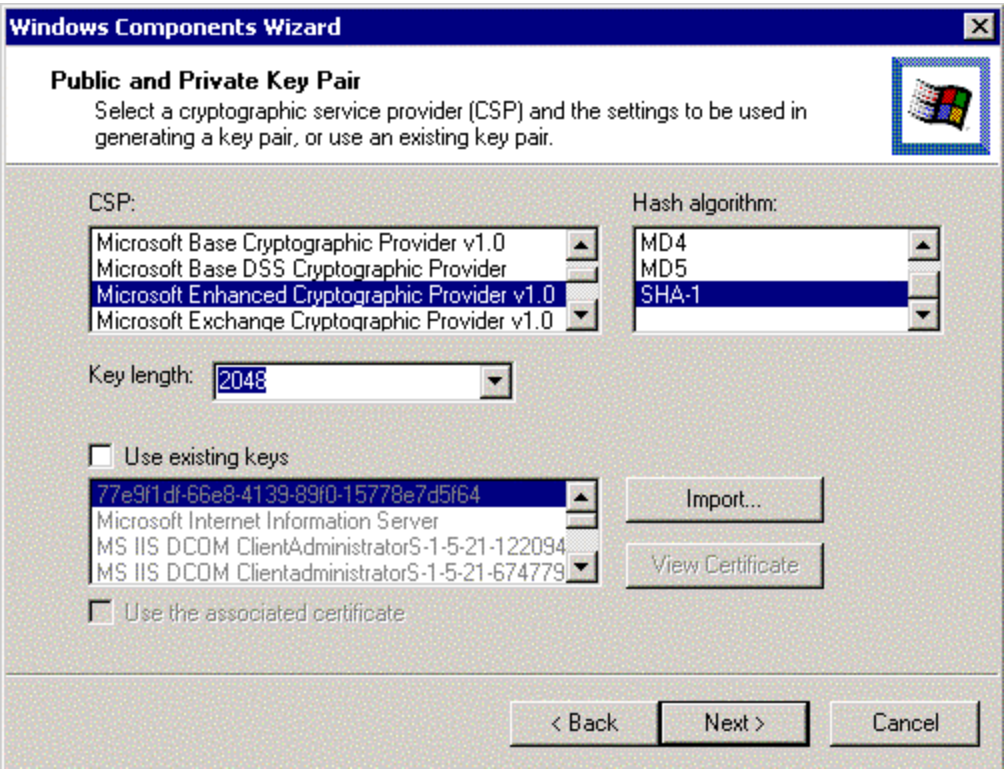


Figure 2 Advanced Options

NOTE: If a stand-alone root CA is installed with access to Active Directory, it is added to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. However, *it does not use Active Directory to verify a requester's credentials*. Therefore, do NOT change the default action (pending) of the CA upon receiving certificate requests. If the requests were not marked as pending, the trusted root stand-alone CA would automatically issue certificates without verifying the identity of the requester.

- Type the name of the certification authority and other necessary information. None of this information can be changed after the CA setup is complete. CA names are bound into their certificates and cannot change. When naming the CA, consider factors such as organizational naming conventions and future requirements. (See **Figure 3**).

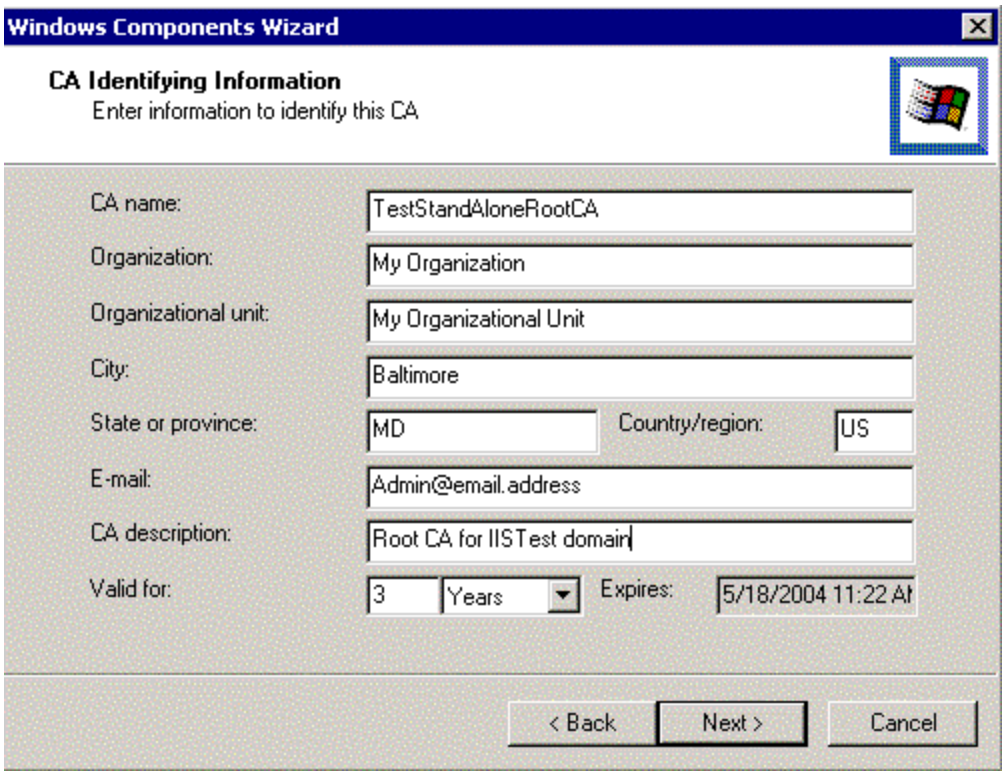


Figure 3 Stand-Alone - CA Identifying Information

- In **Validity duration**, specify the validity duration for the root CA. Click **Next**. The validity duration you choose for the CA will determine when the CA "expires." (Recommend setting this to 5 years for low assurance CAs and 3 years for medium to high assurance CAs. Information on renewing CAs will be discussed later in this document.)

- Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**. If Active Directory is available and you have Write permission to Active Directory, then specifying the shared folder is optional; however, it is recommended. (See **Figure 4**).

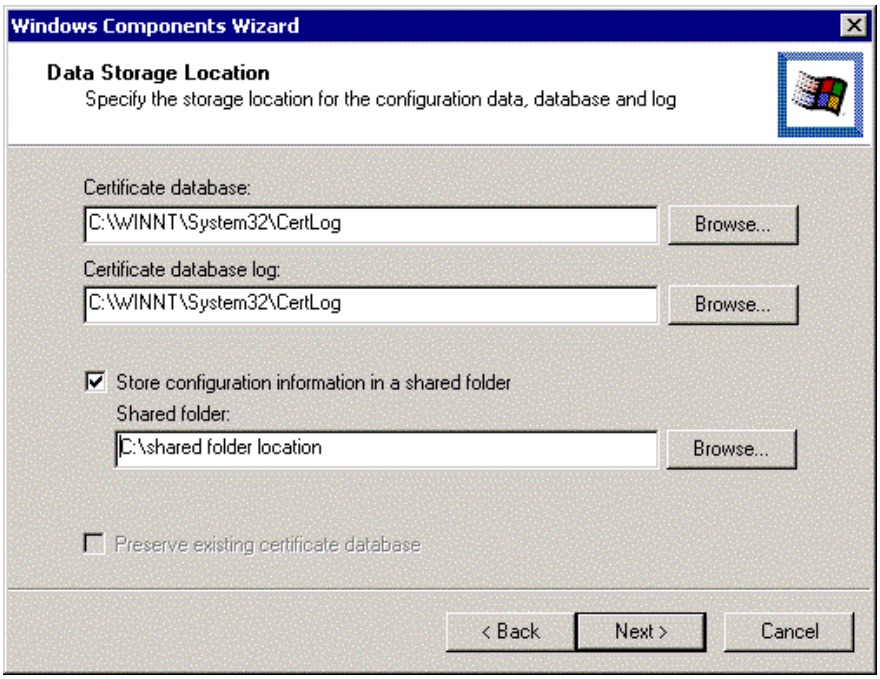


Figure 4 Stand-Alone - Data Storage Location

- If the World Wide Web Publishing Service is running, you will receive a request to stop the service before proceeding with the installation. Click **OK**.
- If prompted, type the path to the Certificate Services installation files.
- Change the URL location of the CRL distribution point. It is necessary to do this because the offline root CA's default CRL distribution points are not accessible to users on the network. If left this way, certificate revocation checking would fail.
- Open **Certification Authority snap-in**
- Highlight the CA. Select **Properties** from the Action menu.
- On the Policy Module tab, select **Configure**.
- Under CRL Distribution Points on the X.509 Extensions tab, select **Add**.
- Enter the name of the new CRL distribution point. (Information on specifying URL names can be found on the Microsoft Help pages.)
- Stop and restart Certificate Services.
- Enforce a two-person control on all actions taken on the CA through your security policy, i.e., dual-combo locks.

Subordinate CAs

(Most of this information was taken from Microsoft's "Install an [enterprise/stand-alone] subordinate certification authority" Help page. Follow the same instructions for Enterprise and Stand-alone.)

- Log on to the system as a Domain Administrator.
- Click **Start**, point to **Settings**, and then click **Control Panel**.
- Double-click **Add/Remove Programs** and then click **Add/Remove Windows Components**.
- In the Windows Components wizard, select the **Certificate Services** check box. A dialog box will appear to inform you that the computer cannot be renamed, and the computer cannot be joined to or removed from a domain after Certificate Services is installed. Click **Yes** and then click **Next**.
- Click desired subordinate CA type, i.e., Enterprise or Stand-alone subordinate CA. (See **Figure 5**).

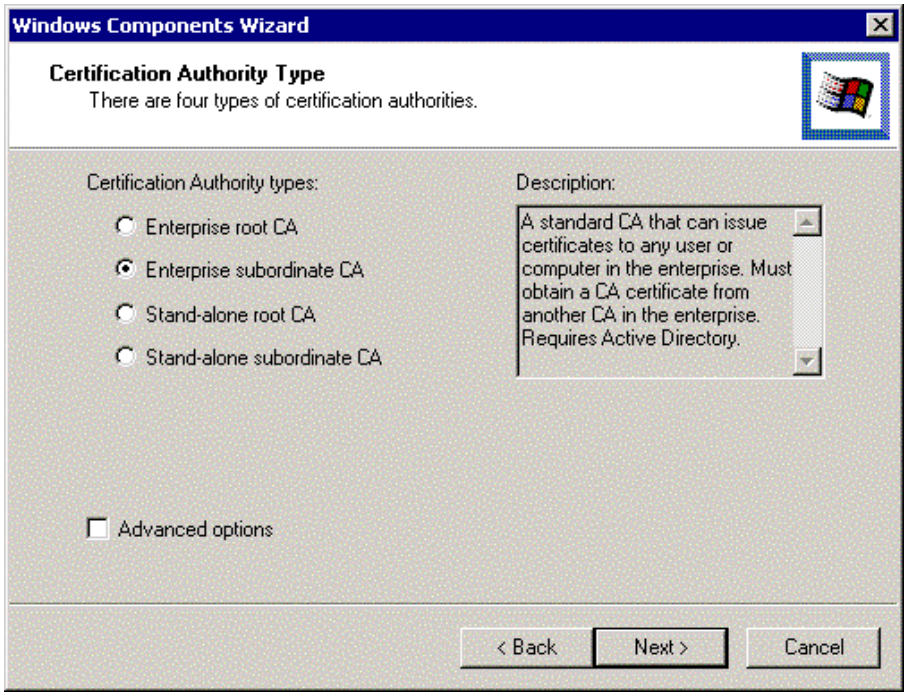


Figure 5 Choosing Subordinate CA

- Select the **Advanced options** check box and apply the desired settings. (Refer to **Table 3** to determine the appropriate settings for these fields.). Click **Next**.

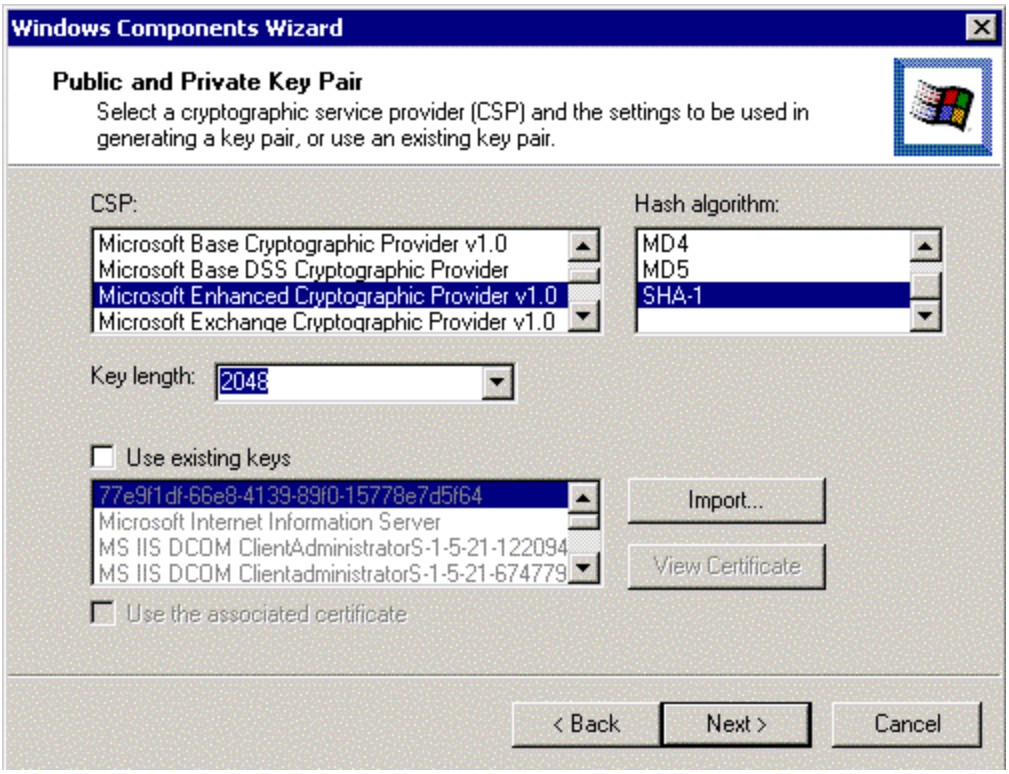


Figure 6 Subordinate CA - Advanced Options

- Type in the name of the CA and other necessary identifying information. (See **Figure 7**). None of this information can be changed after the CA setup is complete. CA names are bound into their certificates and cannot change. When naming the CA, consider factors such as organizational naming conventions and future requirements. Click **Next**.

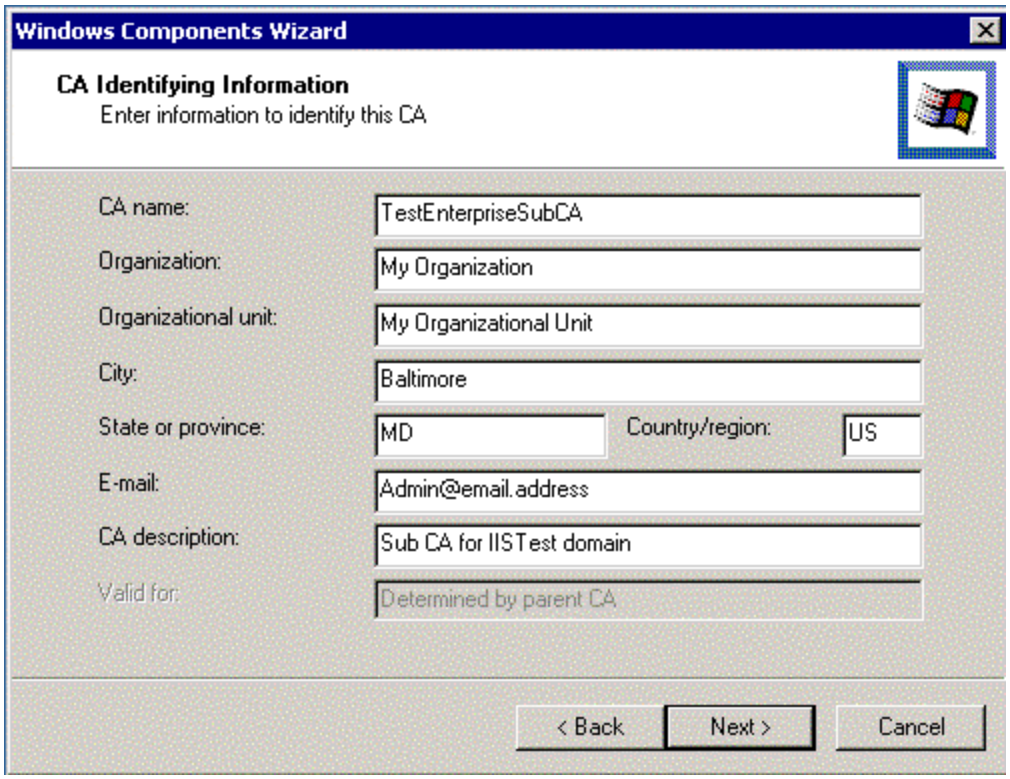


Figure 7 Subordinate CA - Identifying Information

- Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**. (See **Figure 8**).

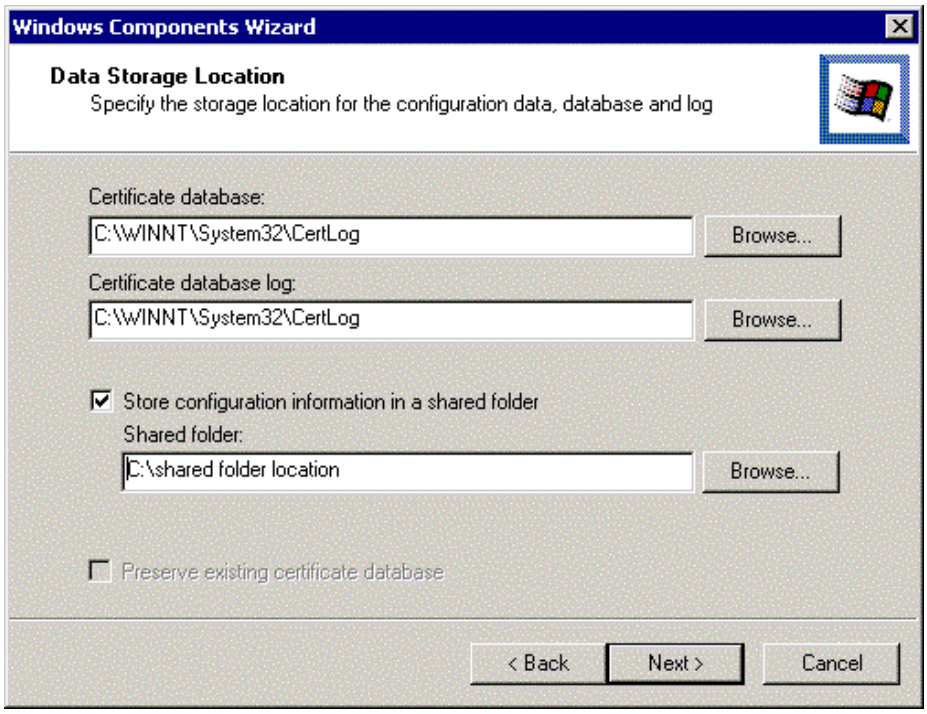


Figure 8 Subordinate CA - Data Storage Location

The enterprise subordinate CA selection requires that the host computer be a member of a domain and that it use Active Directory. The administrator who is installing an enterprise CA must have Write permission to Active Directory. If you have Write permission to Active Directory, then specifying the shared folder is optional; however, it is recommended.

- ❑ Obtain the certificate for the subordinate CA. For instructions on how to do this, see the note below.
- ❑ If the World Wide Web Publishing Service is running, the system will request that you stop the service before proceeding with the installation. Click **OK**.
- ❑ If prompted, type the path to the Certificate Services installation files.

NOTE: To obtain the certificate for a subordinate CA, submit a certificate request to a parent CA. The procedure for doing so depends on whether or not the parent CA is available online.

<u>If a parent CA is available online:</u>

- ❑ Click **Send the request directly to a CA already on the network**.
- ❑ In **Computer Name**, type the name of the computer on which the parent CA is installed.
- ❑ In **Parent CA**, click the name of the parent CA.

<u>If a parent CA is not available online:</u>

- ❑ Click **Save the request to a file**.
- ❑ In **Request** file, type the path and file name of the file that will store the request.
- ❑ Obtain this subordinate CA's certificate from the parent CA.

The procedure for doing this will be unique to the parent CA. At a minimum, the parent CA should provide a file containing the subordinate CA's newly issued certificate and, preferably, its full certification path.

If you get a subordinate CA certificate that does *not* include the full certification path, the new subordinate CA you are installing must be able to build a valid CA chain when it starts. Thus, you must place the parent CA's certificate in the Intermediate Certification Authorities certificate store of the computer (if the parent CA is not a root CA), as well as the certificates of any other intermediate CA in the chain. You must also place the certificate of the root CA in the chain into the Trusted Root Certification Authorities store. These certificates should be installed in the appropriate certificate store before you install the CA certificate on the newly created subordinate CA. Follow the instructions described in the Certificate Store and Active Directory section of this document to install required parent CA certificates. The following describes the steps for installing the subordinate CA's certificate once all the CA certificates in the chain have been installed:

- Open **Certification Authority** snap-in.
- In the console tree, click the **name of the CA**.
- On the **Action** menu, point to **All Tasks**, and then click **Install CA Certificate**.
- Locate the certificate file received from the parent CA, click this file and then click **Open**.

Two global security groups are used for managing Certificate Services -- Cert Publishers and Enterprise Admins. These groups are used to define permissions on objects related to Certificate Services. Members can be added to these groups the same way members are added to any other group in Windows 2000.

- Determine who will be trusted to manage CAs within the enterprise and add those users to the Enterprise Admins group. This group is used to delegate authority over the enterprise to selected individuals, freeing the administrator to perform other daily tasks. Examples of tasks this group can be delegated to manage include backing up, restoring, and renewing CAs within an enterprise; maintaining CA Web pages; managing CA templates; maintaining CRLs; and mapping certificates to user accounts. Assigning permissions so the Enterprise Admins group can perform specific tasks is defined later in this document.
- Place all CA servers that need to publish certificates to Active Directory in the Cert Publishers group. CAs are automatically added to the Cert Publishers group within their own domain. If a CA is required to publish certificates in another domain, it will have to be manually added to that domain's Cert Publishers group.

Renewing CA Certificates

Renewing certificates takes advantage of the inherent trust relationship of the existing certificate. It is useful to renew a certificate if the new certificate will maintain all of the same attributes as the current certificate, while extending the validity period. Below are the procedures for renewing a CA certificate:

- In the **Certificate Authority** snap-in, right-click the root CA, select **All Tasks**, **Renew CA Certificate.**
- Since Certificate Services cannot be running during this operation, you will be prompted to stop Certificate Services. Click **Yes.**
- The Renew CA Certificate window appears. Select **Yes** or **No** to generate a new key pair. Most of the time **Yes** will be selected for root and subordinate CAs. (See **Figure 9**)
- Certificate Services will then restart with a new validity date for the CA certificate.

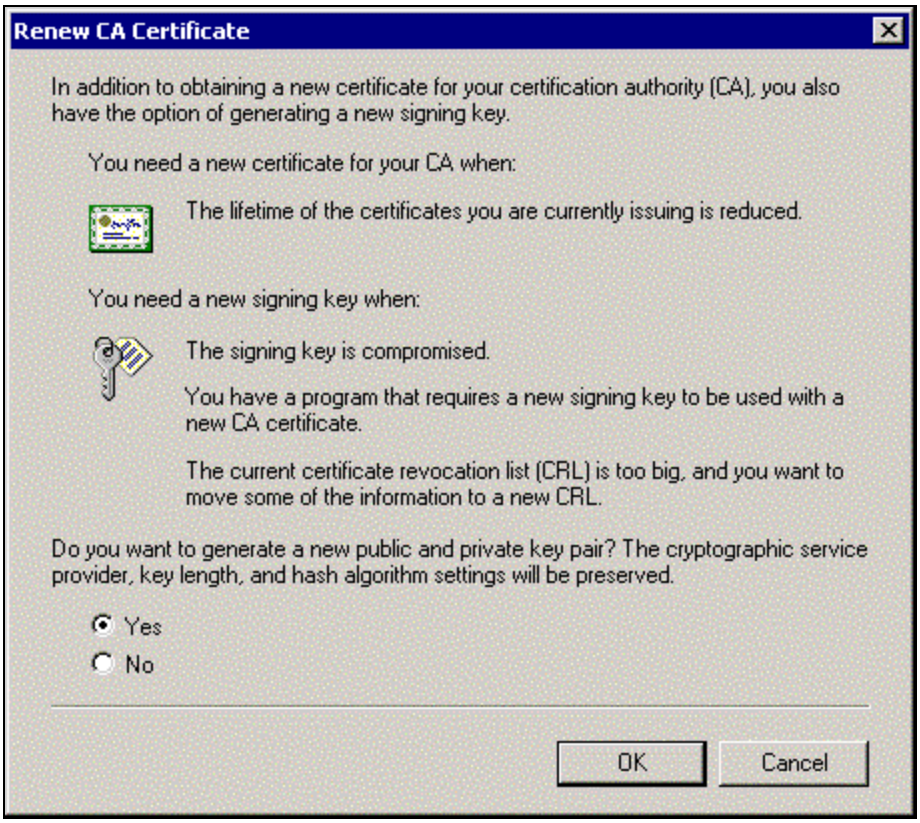


Figure 9 Renewing CA Certificate

If the CA certificate being renewed belongs to a subordinate CA, the request must be submitted to a parent CA, then the new certificate can be retrieved and installed using the same procedures for installing the initial certificate.

It is important to note that whenever a CA is renewed, all automatic certificate enrollment objects that enroll for certificates from that CA must be recreated using the same procedures described in the **Enterprise CA Templates** section of this document.

Chapter

2

Managing Certificates with the MMC

The Microsoft Management Console (MMC) provides a user interface shell application, called a console. The objective is that all management functions are accessible by a subordinate process running within a console. These processes are known as Snap-ins. The MMC itself does not provide any management behavior, but it offers a common environment for snap-ins. The result is that management and administrative control of the platform is centralized.

Certificate Services Snap-Ins

A Certification Authority snap-in and a Certificates snap-in are available for Certificate Services. During the installation of Certificate Services, a console is created with the Certification Authority snap-in loaded. This snap-in can be accessed from the **Start→Programs→Administrative Tools→Certification Authority** menu item.

The Certification Authority snap-in is used to control the types of templates the CA will make available to users, set permissions (manage, enroll, read) on the CA, and display certificate information such as issued, revoked, and pending certificates.

Figure 10 Certification Authority Snap-In

- Select the **Policy Settings** folder to view a list of templates the CA can be configured to issue.
- Delete templates the CA will not be permitted to issue by right-clicking the template you wish to remove and select **Delete.**
- Add certificate templates by right-clicking the **Policy Settings** folder and selecting **New – Certificate to Issue**. A list of templates and a description of their purpose is displayed. Select ONLY the certificate templates your CA is required to issue and click **OK**. The new template will then be displayed in the right pane of the Certification Authority window.

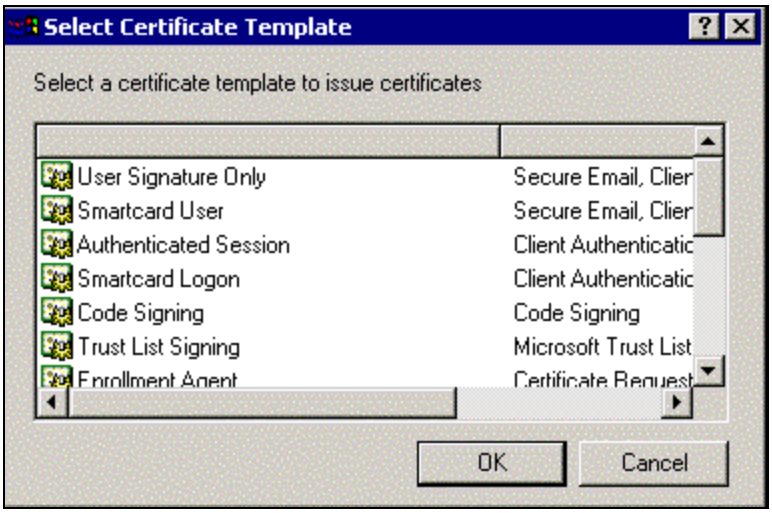


Figure 11 Selecting Certificate Templates

- Set security permissions on the CA (See **Figure 12**). Right-click the **CA name** you want to set security permissions on and select **properties**. The default permissions grant local Administrators, Domain Admins and Enterprise Admins full control over the CA (manage, enroll, and read permissions). Authenticated users are given the ability to enroll and read. Unless your security policy requires a change to this setup, these permission settings are sufficient. **ALWAYS** use the Certification Authority snap-in to set permissions on CAs. Using other tools, such as Active Directory Sites and Services snap-in, may create problems when users attempt to access the CA.

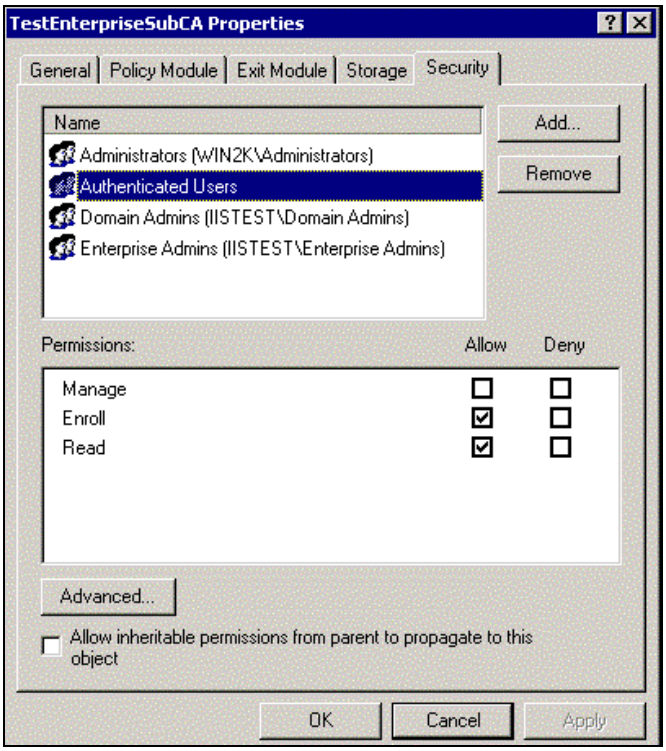


Figure 12 Setting Security Permissions for CA Control

Certificate Store and Active Directory

To view a computer's certificate store, the Certificates snap-in is used. Follow these steps to load the Certificates snap-in into a new MMC. (See **Figure 13**)

- Click **Start** Þ **Run** and type **MMC** in the **Open** box. Click **OK**
- On the Console menu, select **Add/Remove Snap-in**
- Click **Add**
- Select **Certificates** from the list of displayed snap-ins and click **Add**

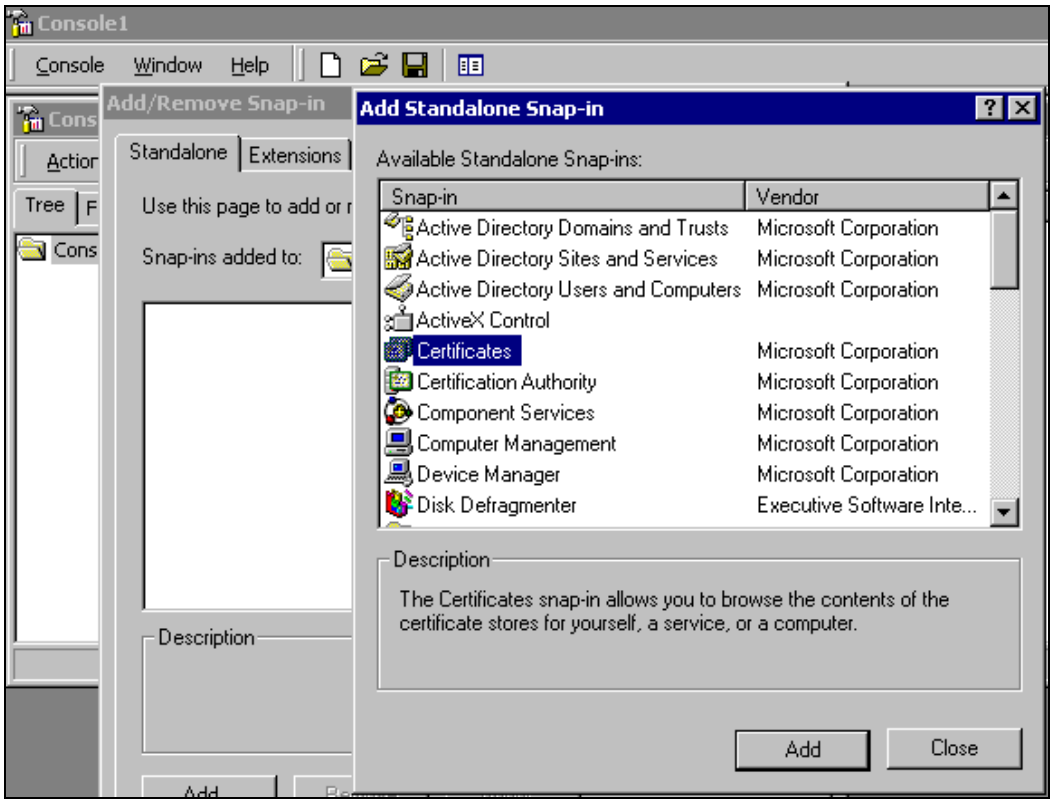


Figure 13 Adding Certificate Snap-in

A window will be displayed allowing you to choose the certificates to be managed through this snap-in. You can choose to manage user certificates, service certificates, and computer certificates (See **Figure 14**). Following this snapshot, there is an example of an MMC where **My user account** and **Computer account** have been selected, resulting in separate snap-ins (See **Figure 15**). When Computer account is selected, you have the option to choose the local machine or another machine. If another machine is selected, type in its name or click the browse button to select a computer on the network. When the snap-in is expanded, a list of available certificate stores is displayed.

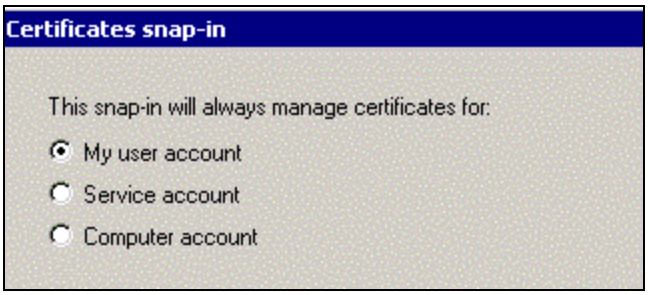


Figure 14 Selecting Account for Certificate Management

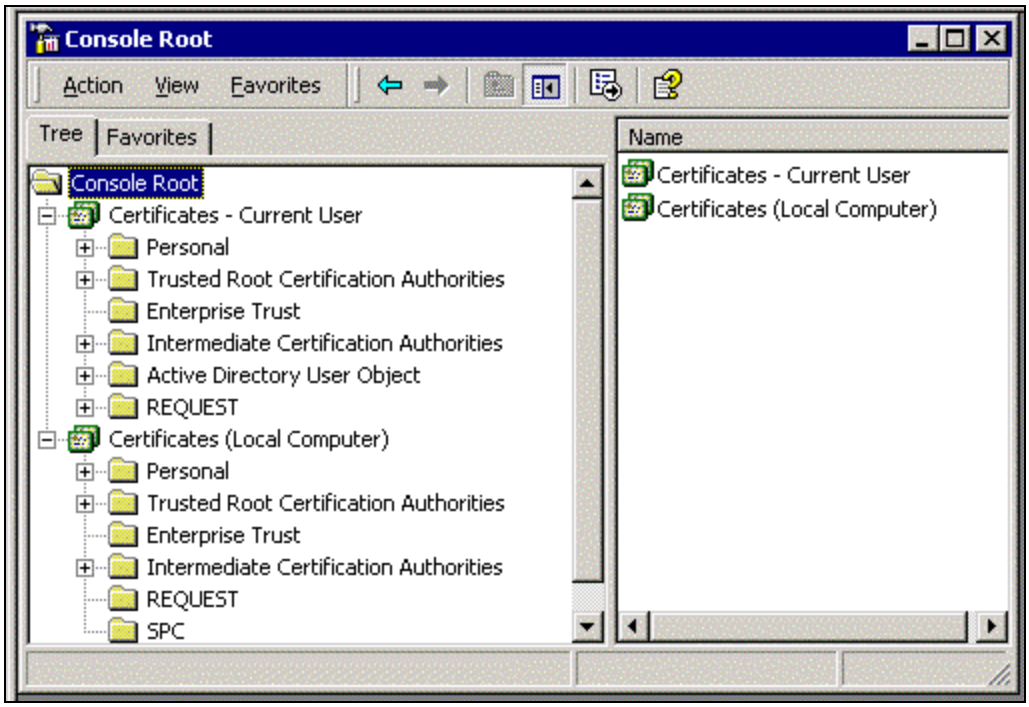


Figure 15 Creating Separate Snap-ins

This snap-in provides a means for the administrator to manage certificates. Select any container (certificate store) to display a list of certificates for that store. To install a certificate into a store:

- Right-click the store where the certificate will be placed (in this example an intermediate certificate will be placed into the Intermediate Certification Authorities store to complete a certificate chain to the root CA).
- Select **All Tasks** Þ **Import** from the pull-down menu. This starts the Import Wizard.
- Fill in the appropriate information pertaining to the certificate to install (See **Figure 16**).

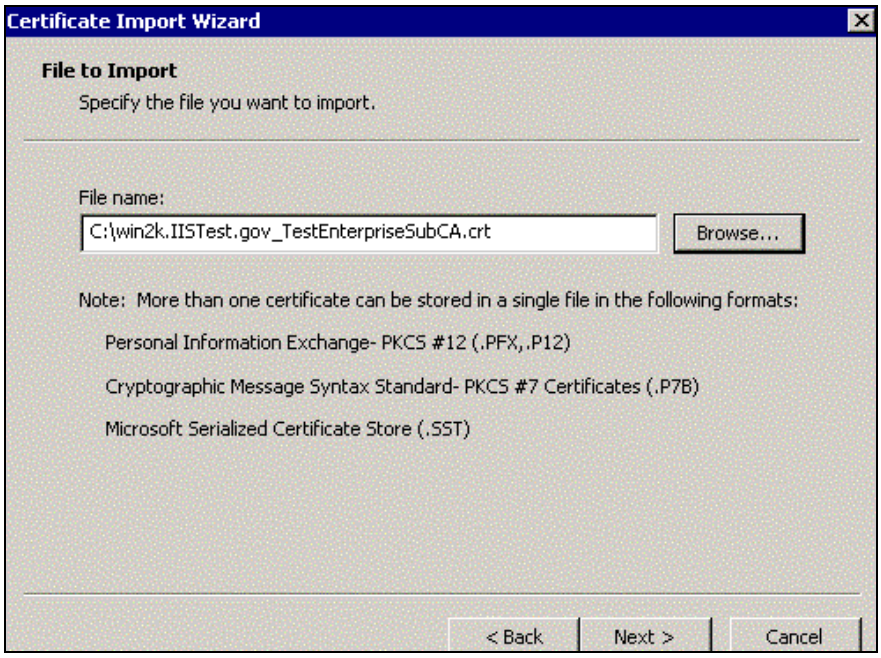


Figure 16 Selecting File to Import in the Certificate Import Wizard

- Select the appropriate Certificate Store to install the certificate (See **Figure 17**).

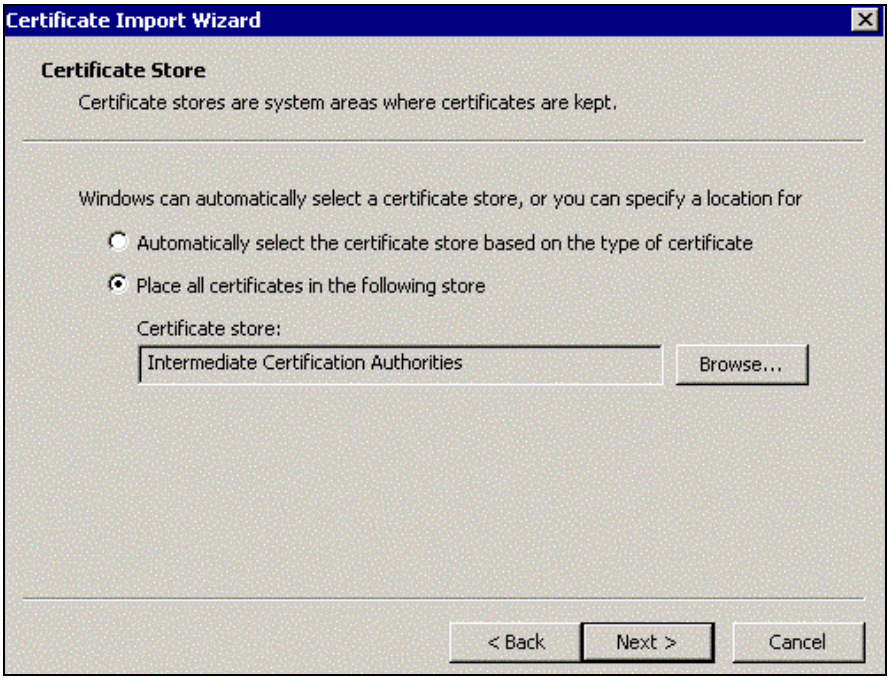


Figure 17 Selecting Location for Certificate Store

- The wizard will display the information for the Administrator to verify. **Verify** and select **Finish**. The certificate is now listed in the selected certificate store.

- In the Trusted Root Certification Authorities and Intermediate Certification Authorities stores, it is important to delete all untrusted CAs that are listed. (See **Figure 18**).

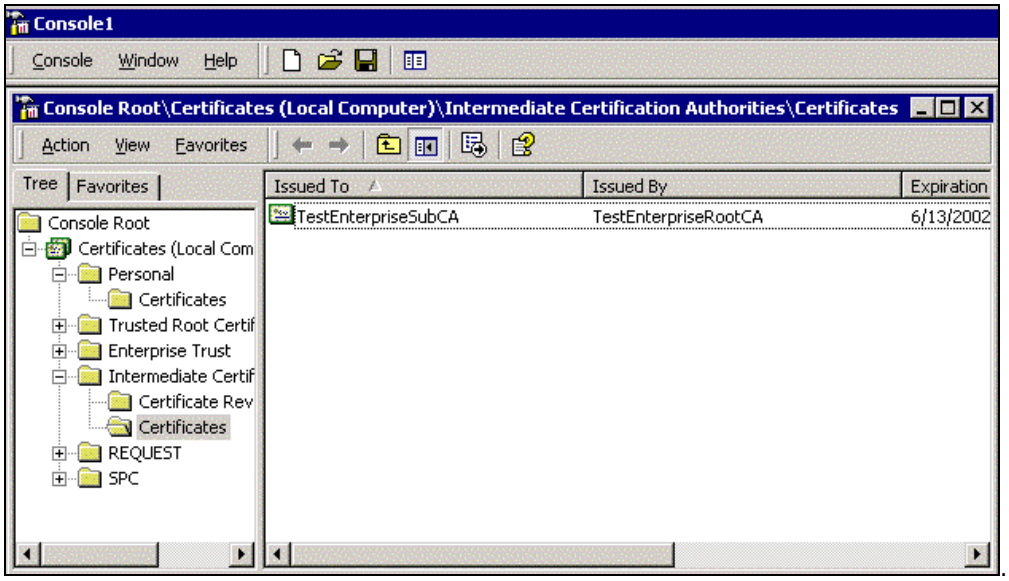


Figure 18 Deleting Untrusted CA

- Expand the **Personal** folder under the Local Computer Certificates and click the **Certificates** folder (store). All certificates issued to the local machine are listed in the right pane. Double-click any certificate in the store to view its details. (See **Figure 19**).

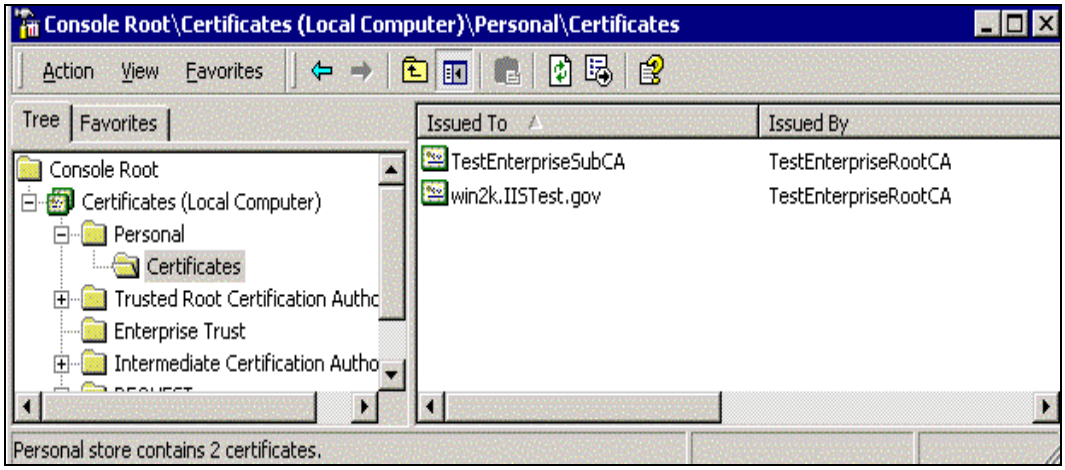


Figure 19 Expanding Personal Folder

Enterprise CA Templates

A certificate template profiles certificates based on their intended use. A certificate requester, depending on their access rights, is able to select from a variety of certificate types based on certificate templates. An enterprise CA administrator can select specific certificate types that the CA is permitted to issue using templates. Initially, only the Administrator, Domain Controller, Computer, Basic EFS, EFS Recovery Agent, User, and Web Server templates are made available to certificate requesters. The Microsoft Management Console Help utility provides a table listing other templates an administrator can choose to make available, along with their purpose and whether the type of certificate is issued to people or computers. Search for "Certificate Templates" to access the table. To make other types of certificate templates available to requesters:

- Open the **Certification Authority** snap-in
- Select ***CA* Name – Policy Settings**
- On the **Action** menu, select **New – Certificate to Issue**
- Select the new certificate template to use and click **OK**

To stop issuing certificates of a particular type:

- In the details pane of the **Policy Settings**, select the certificate template you no longer want to issue from the CA
- On the **Action** menu, select **Delete**

NOTE: The only templates that should be made available to certificate requesters are those the CA is required to issue according to the site's security policy.

Computers can be configured to automatically receive certificates using the Windows 2000 group policy service. Group policy is used to specify the number of templates that can be applied to the computer. On computer startup, the list of certificates located in the local machine "my certificate store" is compared to the templates applied by the group policy. If the computer does not have a certificate for each corresponding templates, the computer will enroll for a certificate to an enterprise CA in the forest for that template. Auto-enrollment for computers allows the administrator to request, from a single point, certificates from enterprise CAs for all computers in a domain or Organizational Unit (OU).

The setup for automatic certificate requests for computers on a Domain Controller is as follows:

- **Edit the Default Domain Policy** Group Policy Object. This can be done by right-clicking the domain node of the **Active Directory Users and Computers** snap-in and selecting **Properties.**
- Expand **Computer Configuration – Windows Settings – Security Settings – Automatic Certificate Request Settings.**

- Right-click the **Automatic Certificate Request Settings** folder, point to **New** and select **Automatic Certificate Request.**
- This launches the Automatic Certificate Request Setup Wizard. Click **Next.**
- Choose a certificate template from the list of templates. A certificate based on the selected template will be provided to a computer during the next logon. (See **Figure 20**)

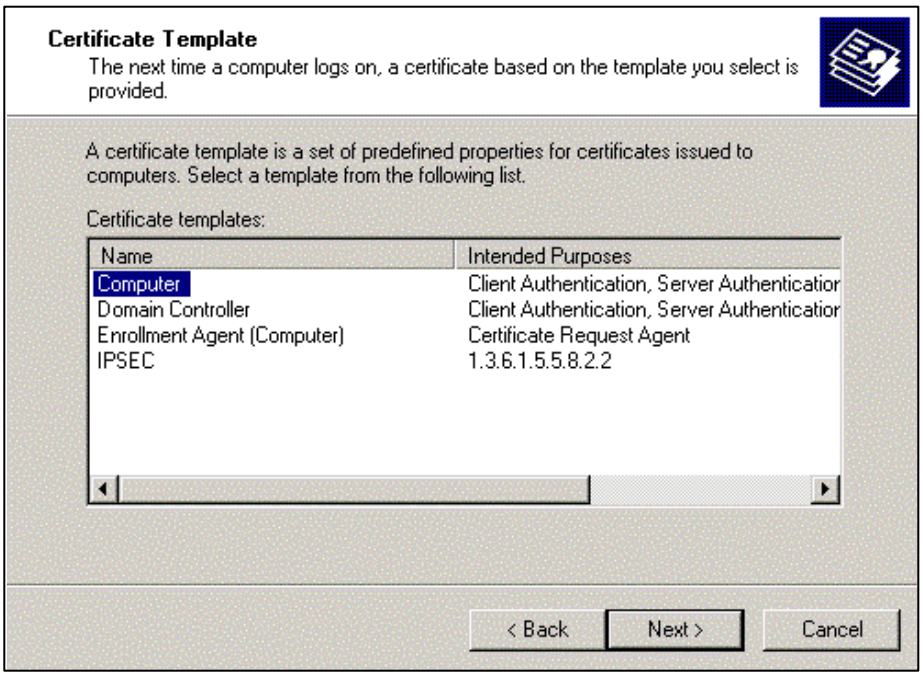


Figure 20 Selecting a Certificate Template

- Select the CA on the domain to send the certificate request. Generally, there will only be one CA on the domain, but there could be more than one CA in an enterprise. CAs not running the enterprise policy module will not be displayed. Click **Next**

- Click **Finish**. The certificate request will take place when the Group Policy Object is refreshed on the client.

Template Security

Certificate template security permissions determine who in the enterprise can enroll for the type of certificate specified by the template.

- Carefully review the list of templates and remove domain users and authenticated users from the security permissions list of those templates the CA will not be permitted to issue. This way, if one or more of these templates are inadvertently made available to users, their request to enroll for the certificate will be denied. The only reason these templates should exist on the CA is if they will be needed sometime in the future. Once again, make sure only those templates the CA is required to issue, according to the site's security policy, are made available to users.

- Look over all access to the templates to be issued by the CA to ensure the permissions are in accordance with the site's security policy.

Security permissions for certificate templates are set through the **Active Directory Sites and Services** snap-in. You must select **Show Services Node** in the **View** menu to see **Services** in the details pane. Expand **Services** – **Public Key Services** – **Certificate Templates**. Double-click each certificate template the CA will make available to users, select the **Security** tab and configure to the desired permissions.

Delegate control over the templates' container, if desired. Highlight the **Certificate Templates** container, right-click and select **Delegate Control**. The following window (See **Figure 21**) is displayed, allowing the administrator to delegate the management of the CA templates to the Enterprise Admins group, for example.

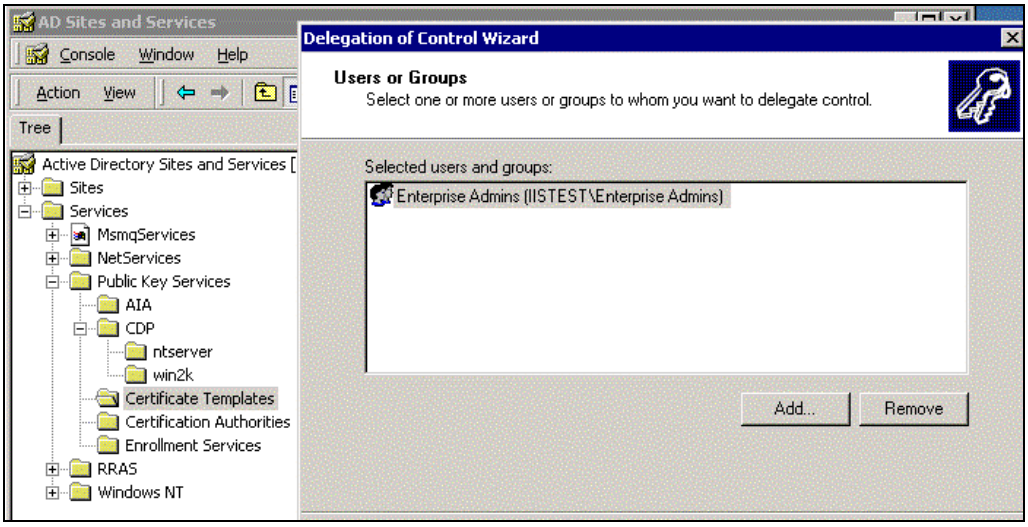


Figure 21 Delegating Control of Templates

NOTE: Although Certification Authorities and Enrollment Services are listed under Public Key Services, security permissions for these nodes MUST NOT be set using the Active Directory Sites and Services snap-in. These permissions need to be set using the Certification Authority snap-in discussed earlier. Changes made in Active Directory Sites and Services could result in problems for users when they try to access the CA.

When an administrator chooses to delegate control over a container or object, he/she can limit the control granted. A list of options are displayed allowing the administrator to select whether the **Selected users and groups** will have full control of the container and all objects in it, or only specified objects (e.g., certificationAuthority objects) (See **Figure 22**). Once that determination is made, the administrator can select the type of access to delegate. Administrators should carefully think through what they want to delegate control over, to whom, and how much access is required to accomplish the task. Do not grant more permissions than necessary.

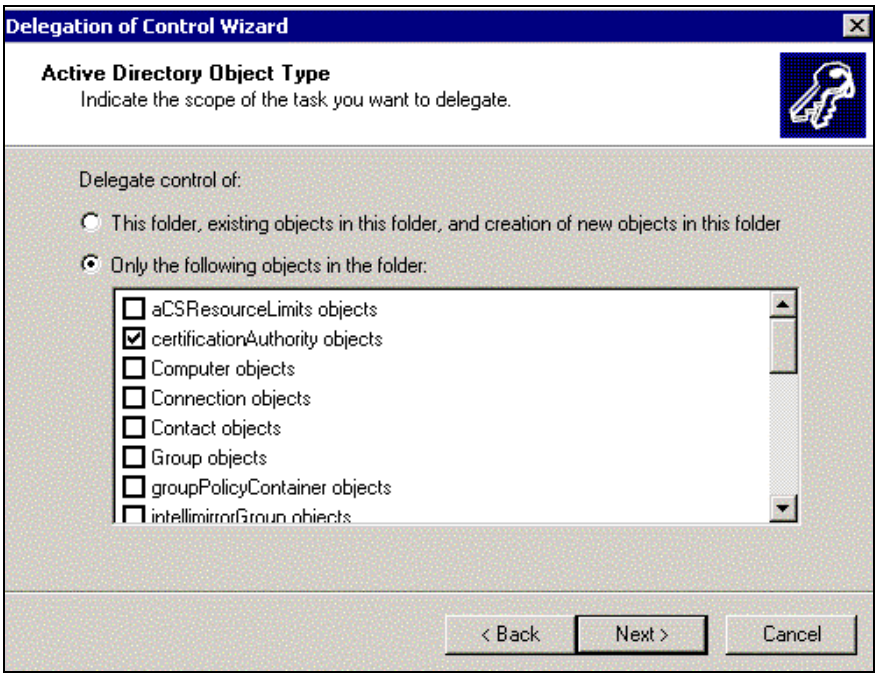


Figure 22 Delegating Control of the Following Objects

Certificate Revocation Lists (CRLs)

A certificate can become invalid if the corresponding private key has been compromised, the certificate was issued fraudulently, or there is a change in the status of the certificate subject as a trusted entity. Invalid certificates need to be revoked and placed on a CRL to be published. If a certificate is deemed invalid, this process needs to take place as soon as possible so the information can be distributed to all entities that are configured to trust the validity of the revoked certificate.

To revoke an issued certificate:

- Open the **Certification Authority** snap-in and select the **Issued Certificates** folder. A list of issued certificates is displayed in the right pane.
- Right-click the certificate to be revoked.
- Select All Tasks and click Revoke Certificate.
- Select the reason for the revocation from the drop-down list box of reason codes and click **Yes**. If the reason code selected is "**Certificate Hold**", the certificate can be unrevoked, left on "Certificate Hold" until it expires, or have the revocation reason code changed. This is the only reason code that allows an administrator to change the status of a revoked certificate. An administrator may choose to select this code if there is some question about the validity of the certificate. The certificate can remain in this state until the administrator can investigate and come to a decision regarding the certificate.
- Force the publication of a CRL by right-clicking the **Revoked Certificates** folder, select **All Tasks**, and click **Publish**. A warning will be displayed notifying the administrator that the last published CRL is still valid. Click **Yes** to publish the new CRL anyway.

To unrevoke a certificate, type the following command from a command prompt on the CA: **certutil –revoke *certificateserialnumber* unrevoke**. Double-clicking the revoked certificate and clicking the **Details** tab will display the certificateserialnumber. A list of parameters for the **certutil** command can be found in the Microsoft Help pages.

NOTE: It is important to note here that manually forcing the CRL to be published only makes the new CRL available to systems that do not have a cached copy of the previous CRL. Systems with a cached copy of the previous CRL will continue to use that CRL until it expires. Administrators should have a procedure in place to notify clients when a new CRL is published prior to the previous CRLs publication period expiration so they may retrieve the new copy. Also, manually publishing a CRL will not change the time when a CRL will be automatically published. For example, if a new CRL is published in the middle of a publication period, the CRL will still be republished at the end of the current publish period.

To obtain information about the current CRL, right-click the **Revoked Certificates** folder and select **Properties**. Click **View Current CRL**. The **General** tab provides overall identification information for the CRL. The **Revocation List** tab displays the CRL contents.

Windows 2000 CAs issue certificates with CRL distribution points as part of its content. This provides a certificate verifier with information pertaining to the location of the current CRL. A CRL file is published on the CA in *Systemroot*\System32\Certsrv\Certenroll by default. Windows 2000 supports CRL publication to Active Directory. Clients can then obtain this information from Active Directory and cache it locally to use when verifying certificates.

This Page Intentionally Left Blank

Chapter

3

Additional Security Issues

Antiviral Program

- Implement a robust anti-viral program as part of the security policy for your entire site.

There are numerous public sector sources for information on antiviral products. A suggested starting point is the International Computer Security Association at http://www.ncsa.com. This Web page contains a lot of generic information about viral solutions and hot links to the major vendors.

Audits

The Certificate Services Log and Database is useful when auditing a CA. It can be used to review queued requests and issued certificates.

- In the Certification Authority tool, beneath the CA name, right-click **Issued Certificates**.
- Select the fields to be viewed. **Request ID** must be selected. Other options are Serial Number, Certificate Effective Date, Certificate Expiration Date, and Issued Common Name. Click **OK.**
- Select **Issued Certificates** to display a list of issued certificates in the right pane.
- Right-click **Issued Certificates** and select **View – Choose Columns** to change the order of the displayed columns and add/remove columns.
- Right-click **Issued Certificates** and select **View – filter**, to display certificates based on the selected filter criteria. **Figure 23** shows an example of the data that can be set in the filter window.

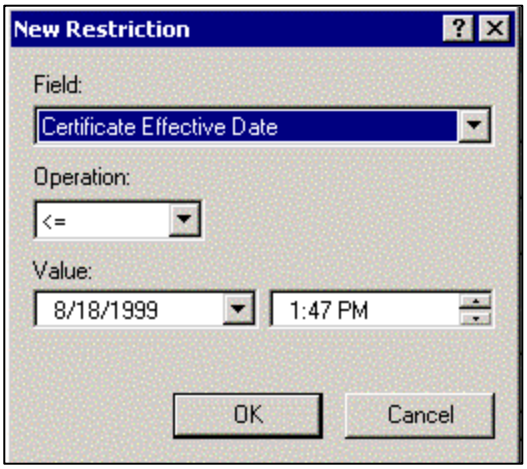
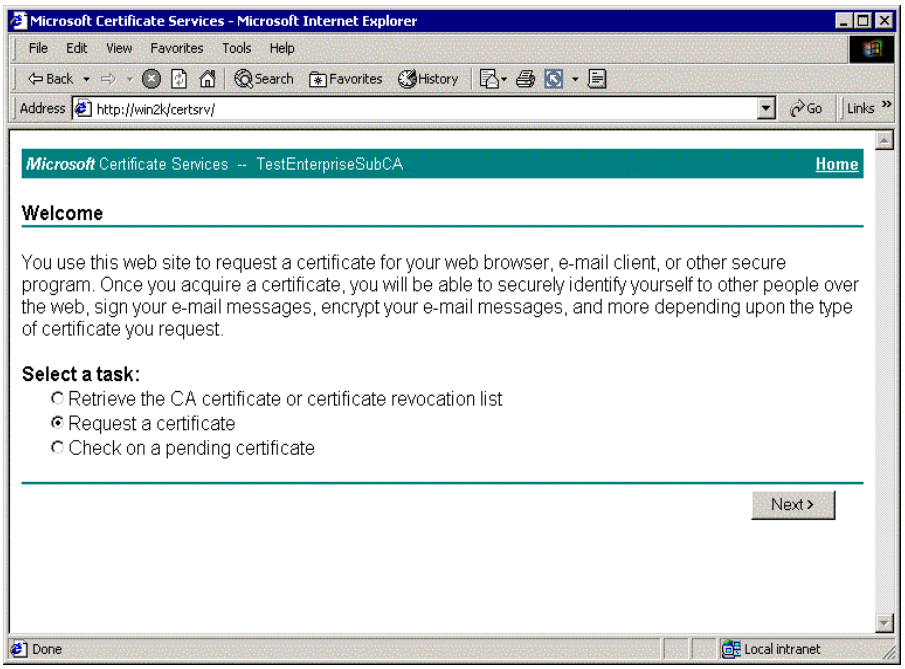


Figure 23 Sample Data for Filtering Information

Certificate Service Web Pages

Common tasks can be accomplished using Certificate Service Web pages. Internet Information Server (IIS) must be installed on the CA receiving requests from users through Web pages. Enterprise CAs require the requester to logon with a user ID. Once the user selects a certificate template, the CA searches the Active Directory for the requester's account and generates a certificate based on the chosen template and information in the Active Directory. As long as the requester is authorized to receive the specified certificate type AND the CA is configured to issue the certificate type, the user will be issued the certificate immediately. Stand-alone CAs do not require the requester to logon and will NOT immediately issue the certificate to the requester, but set the certificate to pending. An administrator must approve the request prior to making it available to the requester. This requires the requester to revisit the Web pages to retrieve the certificate once it has been approved. Following are examples of some typical screens a user might see when accessing Certificate Service Web pages (See **Figure 24**).



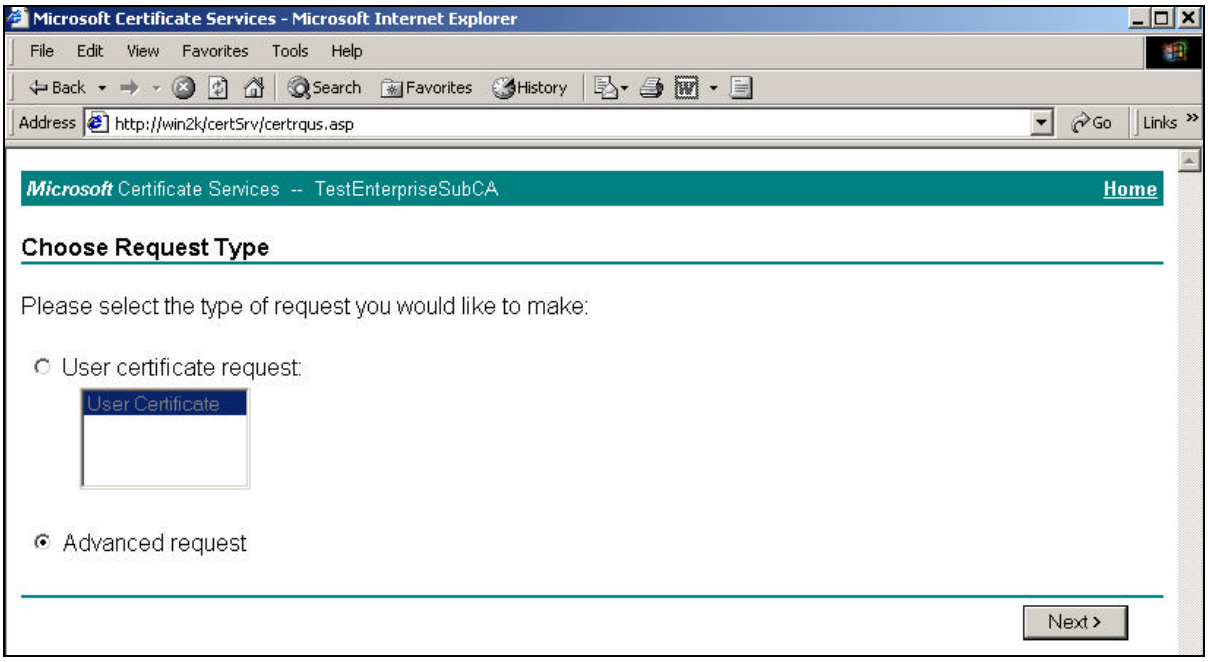
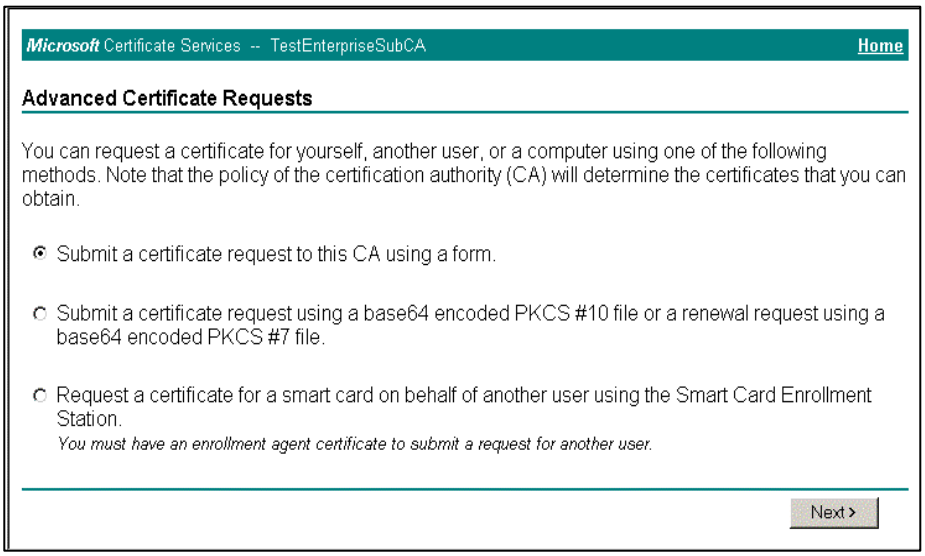


Figure 24 Sample Screens on Certificate Service Web Pages

If the CA you are requesting a certificate from implements the Stand-alone Policy module, a **User Certificate – Identifying Information** page will be displayed. Fill in the necessary information and click **Next**. Enterprise CAs will retrieve the required information from Active Directory and will prompt you to submit your request.

The following options are available when **Advanced request** is selected. (See **Figure 25**).



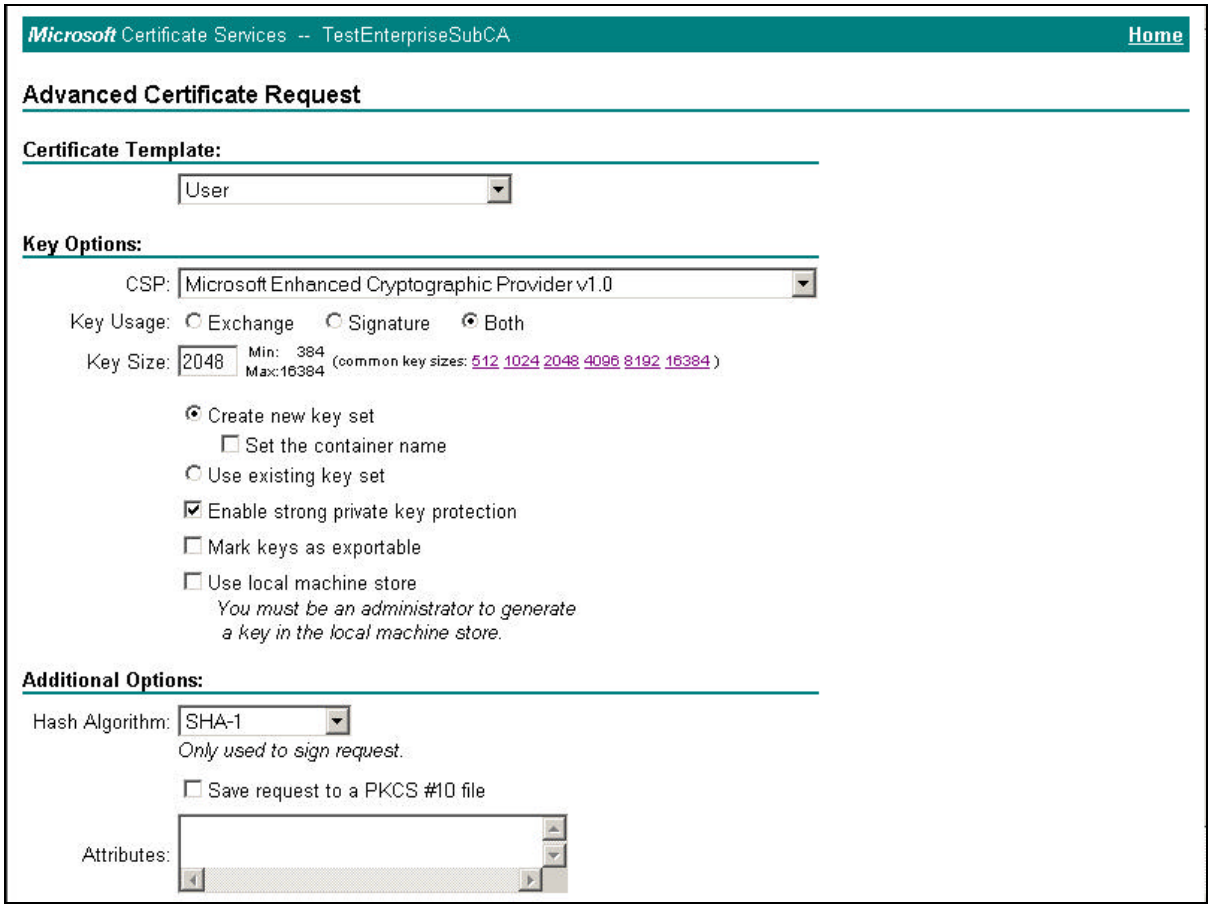


Figure 25 Example of Advanced Certificate Request

Securing Certificate Service Web Pages

Web pages on enterprise CAs must be kept secure since certificate requesters must be authenticated to the page so that it can determine the correct information to put into the requested certificate. If authentication is not set for the Web pages, a certificate will not be generated or, if a certificate is generated, it will be useless. Before following the procedures to verify the Web pages are secure, make sure you can connect to the Certificate Services Web pages. If an error occurs, check to see that the pages were installed. Also, if IIS was installed after Certificate Services, the Web pages were not installed. If the CertSrv virtual directory does not exist, run certutil –vroot from the command prompt to create it. If you have to reinstall Certificate Services, make sure **use existing keys** is selected and select the appropriate CA name from the list.

- In the ISM, expand the **Default Web site** and locate the CertSrv virtual directory
- Right-click **CertSrv** and select **Properties**
- Select the **Directory Security** tab
- Click **Edit** under the **Anonymous access and authentication control**
- Make sure **Integrated Windows authentication** is the **ONLY** option selected and click **OK,** and close all dialog boxes. (See **Figure 26**).

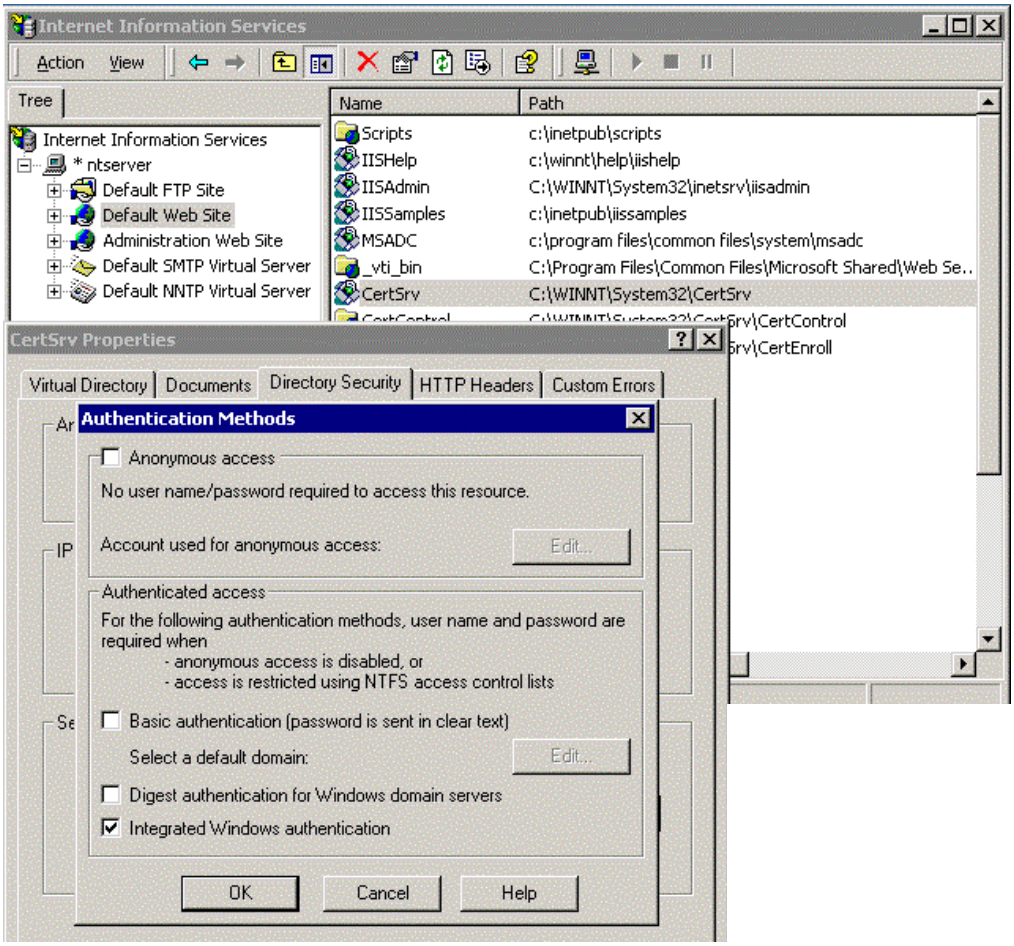


Figure 26 Securing Certificate Service Web Pages

This Page Intentionally Left Blank

Chapter

4

Backups

Backup Procedures

It is very important to include a disaster recovery policy in your site's security plan. There are several ways to backup the data on your server. Automatic backups, such as disk mirroring or disk duplexing, where there is a complete copy of the server's hard drive that can go online in the event the primary drive goes down, and manual backups. It is recommended not to rely on disk mirroring or duplexing exclusively. This strategy only protects against a single drive failure. In the event of a multiple disk failure, you must have other backups to recover. Here are some things to consider when implementing your backup strategy:

- How often does the server content change?
- How long can your site go without providing services to clients?
- Members of the Backup Operators group should have special logon accounts when performing backups. Backup privileges should not be assigned to regular user accounts.
- Consider keeping a set of backups offsite in the event of a natural disaster.
- Make a set of backups before and after any maintenance to the server providing certificate services. This includes any software or hardware changes to the system.
- It is very important that you make and TEST your backups regularly. Remember to include a strategy for backing up the Registry in your backup plan.
- Make sure that NTFS permissions are intact when a restore is done from a backup.

Backing Up Certificate Services

CAs are critical elements within a PKI. The loss of a CA due to hardware or storage media failure could result in the inability to preserve an audit trail of issued certificates and certificate requests. The ability to revoke issued and previously unrevoked certificates may also be lost. Therefore, regular backups must be performed on all CAs to ensure quick recovery in the event of a failure, preserving the stability of the PKI. The preferred method for backing up Certificate Services is to backup the entire server. However, it is possible to backup and restore a CA using the Certification Authority snap-in. This tool can be used to selectively backup keys, certificates, and the database (log of issued certificates and the queue of pending requests).

- Create a backup directory and set permissions to only allow the system and administrator's group access. At least one set of backups should be located in a directory on a remote machine not within the site to prevent the loss of backup data in the event of a natural disaster or some other type of catastrophe. If there is not a machine to backup to, store the backup on recordable media and send to an offsite storage location.

- In the **Certification Authority** tool, right click the CA to backup, select **All Tasks**, **Backup CA**

- A Certification Backup Wizard opens. Click **Next**

- Select the items to include in the backup and enter a previously created backup directory. Generally, you will want to select the **Private key and CA certificate**, and the **Issued certificate log and pending certificate request queue** options. Click **Next**. (See **Figure 27**)

- A window will display asking for a password. This password is required to protect the backup file. This password is requested when restoring the CA certificate. Click **Next.** (See **Figure 28**).

- The next window lists the options you chose to backup. Click **Finish** and the backup will take place. (See **Figure 29**).

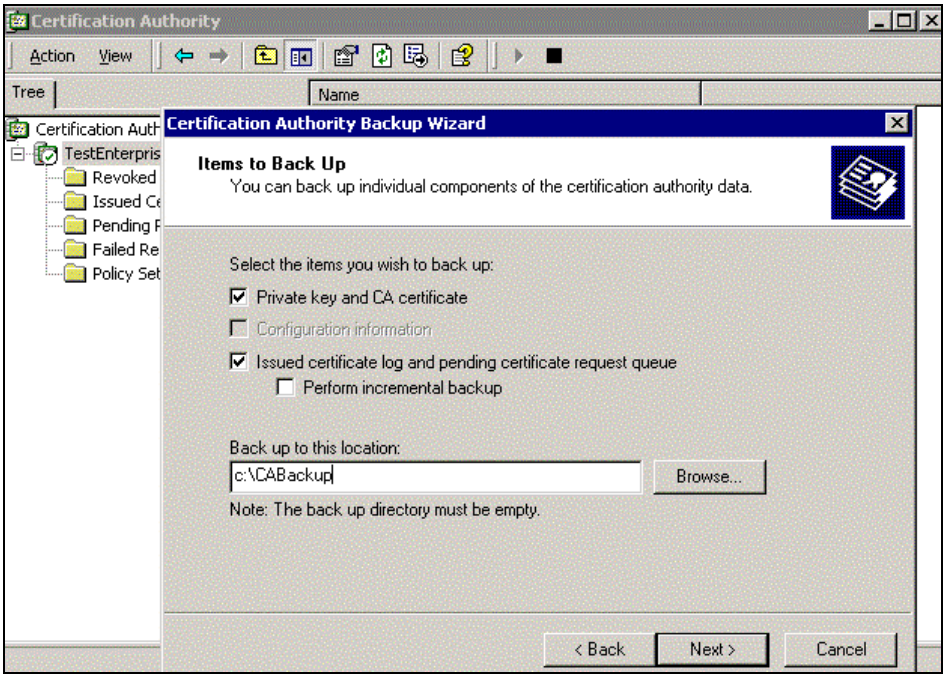


Figure 27 Selecting Items to Back-up

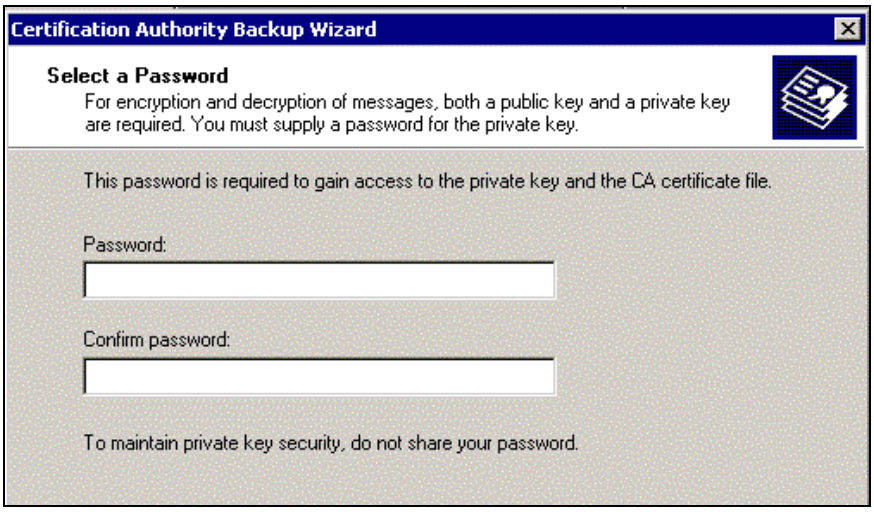


Figure 28 Selecting a Password for CA Backup

Figure 29 Completion of CA Backup Wizard

Restoring Certificate Services

The following procedures describe how to restore a backed up certificate service.

1. If Certificate Services is running, you are prompted to stop it. Click **OK**
2. The Certification Authority Restore Wizard opens. Click **Next**
3. Select the items you wish to restore (the options are the same as for backing up) and the name of the backup directory where the backup file is located. Click **Next**
4. You are prompted for the password to access the private key and the CA certificate file. Enter the password you used when backing up the CA. Click **Next**
5. A window listing the items to be restored is displayed. Click **Finish**. You are asked if you want to restart Certificate Services. If incremental backups still need to be restored, or if the IIS metabase needs to be restored, select no. Otherwise, select **Yes**.

NOTE: If a damaged or missing IIS metabase is not restored, IIS will not start and, therefore, neither will Certificate Services.

If the database logs are present at the time of the restore, the CA will be restored to the point in time of the restore. This means that the database logs will be used to apply changes to the database since the last backup. If the database logs are deleted before the restore, the CA will be restored to the point in time of the last backup.

Appendix

A

Further Information

Windows 2000 Security, Little Black Book by Ian McLean, www.coriolis.com

Microsoft's Certificate Services Help pages

www.microsoft.com/windows2000/library/howitworks - The security section of this page provides technical papers on PKI and Certificate Services

Revisions:

2.0 – Updated some screen images to reflect a different key length option because some hardware devices do not support very long key lengths. Modified recommendation on when to reuse existing keys when renewing a CA.

2.0.1 – Changed e-mail address and removed phone number from cover page

Page: 9
[TP1]I only have four chapters :-(