Report Number: C4-058R-00

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

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

Author:
Sheila Christman

Updated: September 29, 2000
Version 1.0

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 September 29, 2000. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system or Certificate Services.

This Page Intentionally Left Blank

Acknowledgements

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

Trademark Information

Table of Contents

Table of Figures

Table of Tables

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 Services (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.

While these documents are intended to complement the *Guide to Secure Microsoft Windows 2000 Networks*, it presents the information a little differently. 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 (This document)	• 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)	• 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 and securely configure and administer 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 “test.gov” and the subnet 192.168.0 will be used in the examples, screenshots, and listings.

WARNING: It is extremely important to replace “test.gov” and 192.169.0 with the appropriate network name and subnet 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, “References,” contains a list of resources cited.

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 Authenticated Users System	Full Control Read&Execute, List Folder Contents, Read 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 the *Guide to Secure Microsoft Windows 2000 Networks*. It is important to implement this guide on the Certificate Services server.

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. These services, when implemented, help eliminate the threats to computer systems by providing three types of security services: authentication, non-repudiation, and integrity. Windows 2000 Certificate Services has the ability to take advantage of the following resources (depending on the CA policy) to assist in implementing these security services. A detailed description of how these resources relate to Certificate Services is provided later in this document.

- The use of snap-ins – Enroll users for certificates from the CA using either the Certificate Services Web pages or the Certificates snap-in. Manage Certificate Services through the Certification Authority snap-in.
- The use of templates – Use certificate templates to help simplify the process of requesting a certificate. Templates are also used to control the kind of certificates a user can obtain from an enterprise CA.
- The use of Active Directory - Take advantage of Microsoft Active Directory for publishing trusted root certificates, issued certificates, and certificate revocation lists (CRLs).
- The use of smart cards – Ability to use smart cards to log onto a windows-based domain.

Operating System Security

Prior to installing Windows 2000 Certificate Services, invoke the Windows 2000 Operating System security guidelines contained within the *Guide to Secure Microsoft Windows 2000 Networks*. File permissions, registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on Certificate Services security.

Administrators should always 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.

Groups Used With Certificate Services

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. The Enterprise Admins group can be used to delegate authority over the enterprise to selected individuals, freeing the administrator to perform other daily tasks. The members of the group can be granted permission to manage Certificate Services within an Enterprise. Examples of such tasks 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 to allow the Enterprise Admins group to perform these tasks is discussed in the related sections within this document. Any CA server that needs to publish certificates to Active Directory must be a member of 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.

Public Key Cryptography Overview

There are two basic kinds of cryptography -- symmetric cryptography and asymmetric cryptography. In symmetric cryptography, the same secret key is used for encryption and decryption. The key must only be shared between the encrypting party and the decrypting party. If someone else is able to obtain a copy of the secret key, they can also decrypt and read the message. Security for this type of cryptography is provided through the protection of the key being used by the sender and the receiver. As long as only the sender and receiver know the secret symmetric key value, the message is protected (assuming a robust encryption algorithm is used).

Public key (or asymmetric) cryptography is based on two halves of the same key that are "mirror images" of each other and are known as a "key pair". Only one of the two halves of the key pair is required to encrypt a message with the corresponding half used for decryption. In public key cryptography, one half of the key pair is assigned to an individual who keeps it secret. This is called the "private key". The other half is published in a public directory where all users can access it and is referred to as the "public key". The sender encrypts a message with the public key of the receiver, which is retrieved from a public directory. The receiver uses the private component of his key pair, which only he has access to, to decrypt the message. Security is provided through the protection of this private key.

Public Key Cryptography can also be used to provide three other very important security services:

Authentication: a security mechanism that provides assurance that a message was actually sent by the person indicated in the "from:" field.

Non-repudiation: a security mechanism that provides assurance that a sender of a message cannot later deny having sent it and the recipient cannot deny that it was received.

Data Integrity: a security mechanism that provides assurance that a message has not been modified during transit.

These security mechanisms are typically provided via use of a hash in conjunction with public key cryptography. A hash is an encoding scheme that is quick to compute. It results in a relatively short numeric representation of the message that was hashed. Hashes have two important characteristics that allow their use for authentication, non-repudiation and data integrity.

First, a hash is a one-way function -- this means that one cannot retrieve the message from the hash. Second, a hash has a low probability of collisions meaning that even a minor change in a message will result in a change of the hash value.

A process that uses a hash in conjunction with public key cryptography to provide these security services is called “signing”.

When a user signs a message, a hash of the message is calculated and then encrypted using the sender's *private* signing key. This encrypted hash is known as the “digital signature”. The original plaintext message, the digital signature, and the sender's signing certificate (which contains the sender's public signing key) are sent to the recipient.

On the receiving end, the digital signature is decrypted using the sender's public signing key that was sent along with the message in the form of the certificate.

Additionally, the receiving client generates a hash on the plaintext message so it can be compared with the hash that was just decrypted. If the two hashes are the same the message must have originated from the sender, since he/she is the only one who holds the private component of this key pair (providing authentication and non-repudiation), and the message must be the same as was sent (providing data integrity).

In this example the sender’s public key was transmitted along with the message. How does one prevent an unscrupulous user from simply generating his own key pairs and masquerading as someone else? Trust of keys is established via the use of a certificate.

A certificate is a user's public key that has been digitally signed by a trusted authority called a Certification Authority (CA). When a certificate is received, its digital signature is checked to insure that someone the recipient trusts issued it.

Certificate Chaining

To be considered valid, all certificate chains must validate to a trusted root certificate. During a CA installation, these root certificates are distributed in one of three ways:

- The Certificate Import Wizard of the Certificates snap-in can be used by an administrator to manually add the root certificate to the local machine (described in the Certificate Services Snap-Ins section of this document).

- A domain administrator can distribute any root certificate to groups of computers within the forest using the public key group policy. If an external CA only needs to be trusted by a small number of computers within the enterprise, group policy can be used to apply the desired settings to only those computers requiring the trust.

- Automatically added from Active Directory as a result of a domain administrator installing a CA or added by using the DSStore tool.

In a CA hierarchy, several layers of CAs will exist. Part of the chain validation process involves retrieving and analyzing all intermediate certificates (subordinate CA certificates) in a certificate chain. It is possible that the client is missing all or part of the certificate chain used to validate a leaf certificate. Authority Information Access (AIA) locations, published in certificates by the enterprise CA, are used to tell the verifier of a certificate where to retrieve a CA’s certificate. An AIA typically uses LDAP, HTTP, or FILE uniform resource identifiers (URIs) to point to locations where the intermediate certificates reside.

Smart card logon uses X.509 version 3 certificates as an alternative to using passwords for the Kerberos authentication process. In order for smart card logon to work, both the domain controller and the client must have valid certificates from Windows 2000 enterprise CAs. The smart card certificate must be issued by an enterprise CA within the forest. Each certificate in the certificate chain must be accessible. This means the certificates must reside on the local machine or accessible through the network and revocation information must be reachable. All revocation information must be time valid. Certificates in the certificate chain cannot be listed on the CRL. Both certificates must chain to trusted root certificates. The smart card certificate must be based on the SmartCard Logon or SmartCard User certificate template. If any of these requirements are not met, the logon will fail.

Public Key Cryptography Standards (PKCS)

RSA Laboratories, in collaboration with Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell and Sun, developed a family of standards describing data structures used with public key cryptography. These standards, identified by numbers 1-15, describe the syntax for digitally signing a message, encrypting a message, and ensuring a requester has an appropriate private key. A Windows 2000 Certificate Services CA uses the following PKCS numbers:

- PKCS #1 – describes how digital signatures are constructed using the RSA public key algorithm in conjunction with hash algorithms. It also describes how to represent RSA public keys and private keys. This standard is used in conjunction with PKCS #7 for defining how to construct signed messages.
- PKCS #7 – describes how digital signatures and encryption are applied to any block of data. It also describes how other attributes, such as the message signing time, can be included in the message and protected by the same signature. A special form of a PKCS#7 message, *degenerate message*, is used for transporting certificates and CRLs. This standard also specifies how data can be encrypted using a symmetric-key algorithm to encrypt data and an RSA public key for encrypting the symmetric keys.
- PKCS #10 – describes how to construct a certificate request message. A certificate request consists of a public key and an optional set of attributes, such as the distinguished name or the e-mail name of the requester, which is signed by the private key matching the public key in the request. Windows 2000 Certificate Services uses this standard to receive certificate requests. Windows 2000 Certificate Services receives a request, processes it and will either issue the X.509 certificate to the request or deny the request. The information returned to the requester is either in the form of a single X.509 certificate or the certificate plus its chain up to the root certificate. This information is returned to the requester in the form of a degenerate PKCS #7 message.

Pre-Installation Considerations

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. It is recommended that the hierarchy consist of at least one root CA that only issues subordinate CA certificates. Place your 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. Several intermediate subordinate CAs can be used to issue certificates to the CAs providing end-entity 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. The answers to the following questions will determine the policy module selected during the Certificate Services installation process.

- ❑ 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 (discussed on page 6) 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 (discussed on page 5) on all subordinate CAs.
- ❑ How many subordinate CAs are required? At least a three-tier hierarchy is recommended. Also consider having more than one CA available for enrollment into a forest, ensuring at least one CA is always available to process requests.

Other pre-installation considerations:

- ❑ 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)

Root and Subordinate CA 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, the stand-alone policy must be installed first, and then replaced 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.

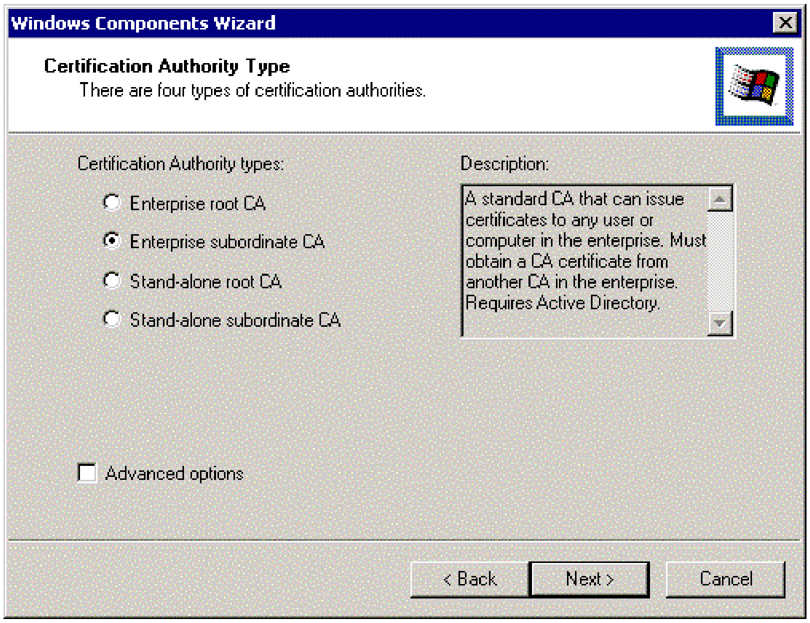
The CAs’ private keys provide the basis for trust in the certification process. For this reason, cryptographic hardware modules may be used to provide tamper-resistant key storage and to isolate the cryptographic operations from other software running on the server. Cryptographic hardware modules greatly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

Windows 2000 CA Policies

Enterprise Policy Module – A CA using the enterprise policy is referred to as an enterprise CA. Enterprise CAs are dependent on Active Directory and DNS. This is the recommended policy module for subordinate CAs within a Windows 2000 domain. Enterprise CAs make use of certificate templates to create certificates for a particular purpose and as a means of defining the enrollment policy for a forest. The use of these templates provides the CA with the following functionality:

- Credential checks are enforced on users during certificate enrollment. Security permission is set in Active Directory for each certificate template that determines the authorization for the type of certificate requested. If the user is not authorized to receive the requested certificate type, the request is denied. Setting security permissions on templates is discussed later in this document in the Enterprise CA Templates section.
- The certificate subject name is automatically generated.
- A predefined list of certificate extensions is added to the issued certificate from the template, reducing the amount of information a requester must provide regarding the certificate and its intended use. Two Microsoft-specific extensions are included with Windows 2000 enterprise CAs for management purposes: Certificate Template and CA Version. The Certificate Template extension is used to identify the template used to create the certificate. The CA Version extension is used to track how many times a CA has been renewed and the number of signing keys that are in the possession of the CA.

To install an enterprise CA, choose an enterprise CA Certification Authority type during the installation of Windows 2000 Certificate Services. See **Figure 1**:



Windows Components Wizard

Certification Authority Type

There are four types of certification authorities.

Certification Authority types:

○ Enterprise root CA
● Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description:

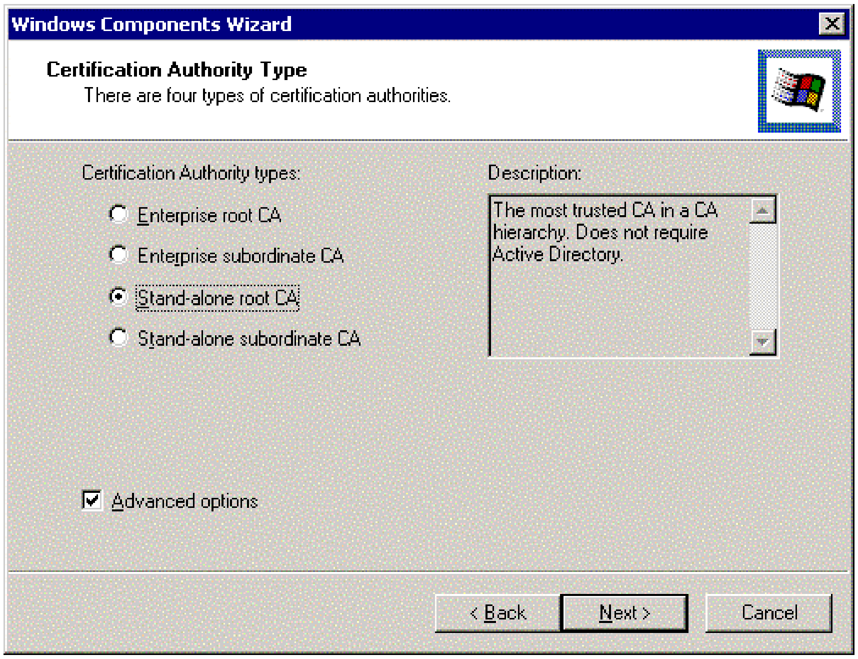
A standard CA that can issue certificates to any user or computer in the enterprise. Must obtain a CA certificate from another CA in the enterprise. Requires Active Directory.

□ Advanced options

Figure 1 Choosing Enterprise Subordinate CA for Certification Authority Type

A Windows 2000 enterprise CA has the simplest administration model with the lowest overhead per certificate. It works with Active Directory and the Windows 2000 security model to minimize the administrative burden of issuing certificates while providing an integrated single point of management. An enterprise CA uses Active Directory as a registration database. A user created in a windows 2000 domain is automatically registered to all enterprise CAs in the forest. This lets users who have appropriate permissions request a certificate from any enterprise CA. The Windows 2000 security model is used to identify the user requesting a certificate and verifies their eligibility based on the user's group membership. Enterprise CAs publish certificates and CRLs to Active Directory. Enterprise CAs can also issue certificates that can be used to logon to Windows 2000 domains using smart cards.

Stand-alone Policy Module – A CA using the stand-alone policy is referred to as a stand-alone CA. Stand-alone CAs do not typically make use of Active Directory. They can, however, take advantage of an Active Directory if it is available. A stand-alone CA is most often operated offline to provide a high degree of security. A Windows 2000 stand-alone CA can function independently of Active Directory and other components in the Windows 2000 forest. It can also be installed on a Windows 2000 server in a Windows NT 4.0 domain. To install a stand-alone CA, choose a stand-alone CA Certification Authority type during the installation of Windows 2000 Certificate Services. See **Figure 2**:


Windows Components Wizard

Certification Authority Type

There are four types of certification authorities.

Certification Authority types:

○ Enterprise root CA

○ Enterprise subordinate CA

● Stand-alone root CA

○ Stand-alone subordinate CA

Description:

The most trusted CA in a CA hierarchy. Does not require Active Directory.

☑ Advanced options

Figure 2 Choosing Stand-alone Root CA for Certification Authority Type

The stand-alone CA is a more secure implementation of the Certificate Services due to the fact that it generally is not connected to a network. This, however, requires more administrative overhead. Certificate requesters must explicitly supply all identifying information about themselves and the type of certificate desired (unlike the enterprise CA where information is taken from the Active Directory and the certificate type is described by a certificate template). By default, all requests sent to stand-alone CAs are set to pending and the administrator of the CA must verify the identity of the requester before the CA can satisfy the request. In addition, the administrator has to explicitly distribute the stand-alone CAs certificate to the domain user's local trust root store and manually update CRLs on a regular basis. Detailed steps for creating an offline root CA can be found in the Microsoft Help pages.

Security 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.

Installation of either policy by a Domain or Enterprise Admin, on a network accessible machine, creates CA and CRL objects in Active Directory. Therefore, much of the certificate chain building process and certificate revocation checking takes place using LDAP queries to Active Directory. Also, the root certificate is placed in Active Directory, allowing all Windows 2000 clients on the enterprise network to automatically receive copies of that CA's certificate.

Both types of CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME, and authentication to a secure web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Enterprise CAs have some added capabilities due to the added security they provide when authenticating certificate requesters. Enterprise CAs can issue certificates for logging onto a Windows 2000 domain using a smart card, and can issue certificates that can be used to authenticate the user from a Microsoft Internet Information Services server in the forest. Stand-alone CAs are not capable of providing this functionality.

There can be more than one enterprise root CA in a Windows 2000-based domain, thus more than one hierarchy. It is also possible to mix and match stand-alone and enterprise CAs in a hierarchy to best suit your needs. This is the recommended hierarchy. Create an offline stand-alone root CA that issues certificates to subordinate CAs only. These subordinate CAs can use the stand-alone policy as well, but would require a lot more administrator interaction, increasing the possibility of compromise. If the CAs will be supporting a Windows 2000 domain, enable the subordinate CAs to implement the enterprise policy and take advantage of the added security features it provides. An offline root CA provides assurance that it cannot be easily compromised, and any compromised subordinate CA on the network can be safely revoked.

Exit Policy Module

The exit module provided with Windows 2000 allows certificate publication to Active Directory or the file system, determined by what the certificate request specifies. It also publishes CRLs to specified URLs. The exit module determines where the CA publishes the CRL. The CA server must be a member of the Cert Publishers group in Active Directory to publish certificates in a domain. When certificates are published in Active Directory, they are associated with the object in Active Directory to which they were issued. A custom exit module can be created to replace an existing exit module, but this is not generally required. Guidelines for creating a custom exit module can be found in the *Microsoft Platform Software Development Kit*.

Installation Process

Enterprise CAs

Enterprise CAs are typically installed if certificates will be issued to users or computers within an organization using a Windows 2000 domain. All certificate requesters MUST have an entry in the Windows 2000 Server Active Directory. The enterprise root CA is the trust point in the enterprise. All other subordinate CAs are trusted only because the root is trusted. It is recommended that the enterprise root CA be configured to only issue certificates to subordinate CAs within the hierarchy. Subordinate CAs can then be setup to issue certificates to issuing CAs, which issue certificates to end-users.

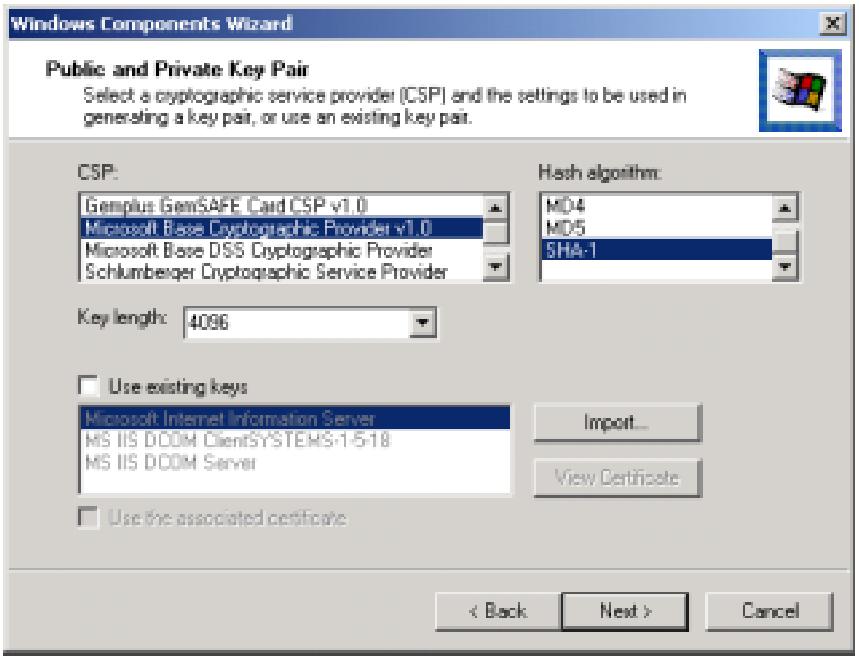
Enterprise Root CA

(Most of this information was taken from Microsoft's "Install an enterprise root certification authority" Help page)

- 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. If you intend to use the optional Web components, make sure IIS is also checked. IIS must be installed in order to use this feature. 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 **Enterprise root CA**. This option will be automatically selected. If another CA is already registered, the enterprise subordinate CA will be selected. If Active Directory is not available, the two enterprise options will be disabled.
- (Optional) Select the **Advanced options** check box to specify the following. See **Table 3**.

Advanced option	Comment
Cryptographic service provider (CSP)	The default is the Microsoft Base Cryptographic Provider. Certificate Servi 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 helpful if you are relocating or restoring a previously installed certification authority (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 longer the key length, the more secure the key is. For a root CA, you should use a key length of 4096 bits. This option is not available if you are using existing keys.

Table 3 Details of "Advanced Options" When Selecting Enterprise Root CA


Windows Components Wizard

Public and Private Key Pair

Select a cryptographic service provider (CSP) and the settings to be used in generating a key pair, or use an existing key pair.

CSP:
- Gemplus GemSAFE Card CSP v1.0
- Microsoft Base Cryptographic Provider v1.0
- Microsoft Base DSS Cryptographic Provider
- Schlumberger Cryptographic Service Provider

Hash algorithm:
- MD4
- MD5
- SHA-1

Key length: 4096

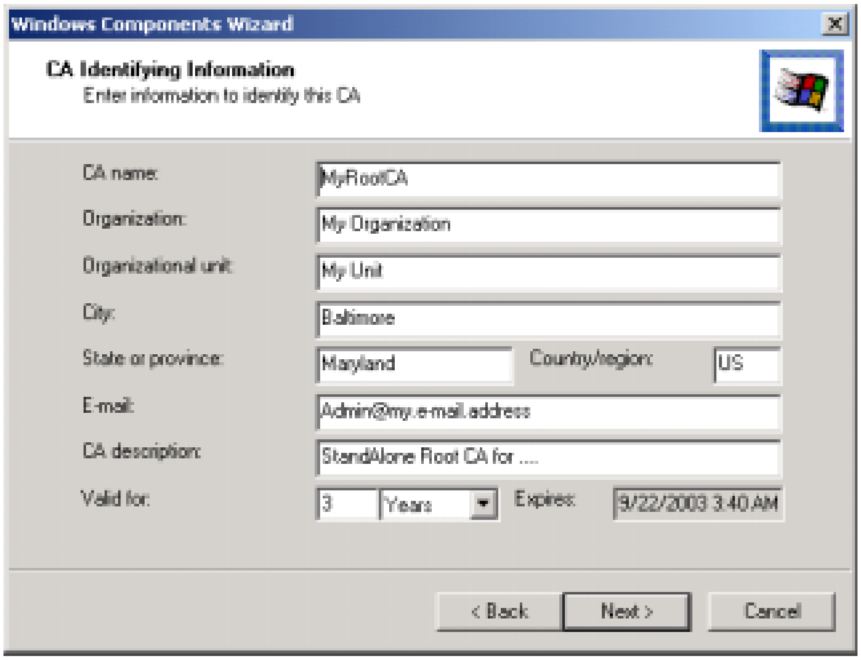
□ Use existing keys

- Microsoft Internet Information Server
- MS IIS DCOM ClientSYSTEMS-1-5-18
- MS IIS DCOM Server

□ Use the associated certificate

Figure 3 Enterprise Root CA - Sample Dialog Box for "Advanced Options"

- When configuration is completed, click **Next**.
- 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 4**.


Windows Components Wizard

CA Identifying Information

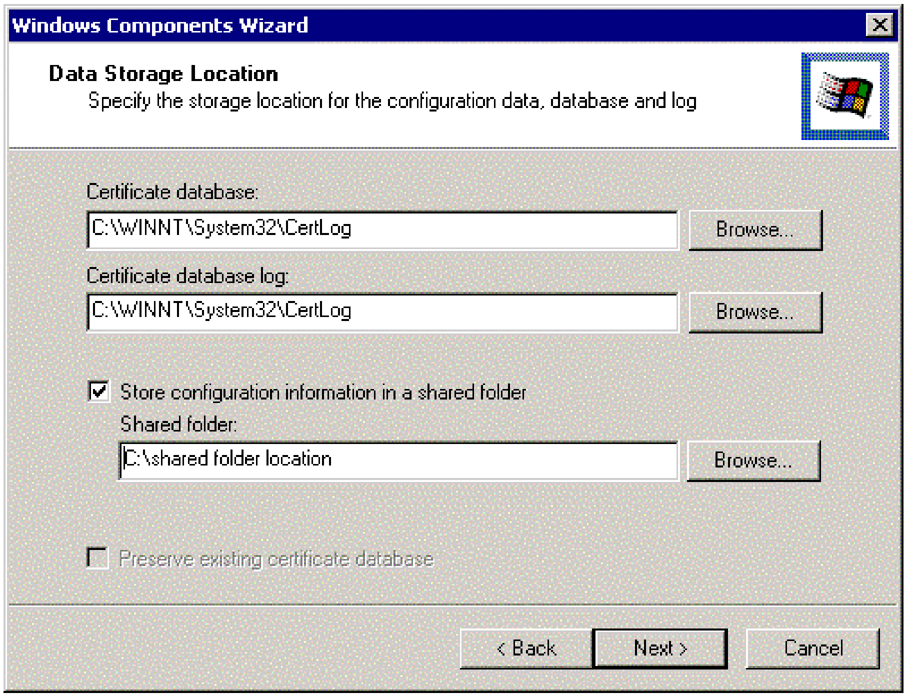
Enter information to identify this CA

CA name:	MyRootCA
Organization:	My Organization
Organizational unit:	My Unit
City:	Baltimore
State or province:	Maryland
Country/region:	US
E-mail:	Admin@my.e-mail.address
CA description:	StandAlone Root CA for ....
Valid for:	3 Years
Expires:	9/22/2003 3:40 AM

Figure 4 Enterprise Root CA - Identification Information

❑ In **Validity duration**, specify the validity duration for the root CA. Click **Next**. The validity duration choosen 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**. See **Figure 5**.



Windows Components Wizard

Data Storage Location

Specify the storage location for the configuration data, database and log

Certificate database:

C:\WINNT\System32\CertLog

Certificate database log:

C:\WINNT\System32\CertLog

☑ Store configuration information in a shared folder

Shared folder:

C:\shared folder location

□ Preserve existing certificate database

Figure 5 Enterprise Root CA - Data Storage Location

NOTE: It is a good idea to specify a shared folder location to store CA configuration information. Make it a Universal Name Convention (UNC) path and have all CAs point to the same folder. This way administration tools can be used to determine CA configuration in the event the Active Directory is unavailable.

❑ If the World Wide Web Publishing service is running, you will see a request to stop the service before proceeding with the installation. Click **OK**.

❑ If prompted, type the path to the Certificate Services installation files.

NOTE: The enterprise root CA selection requires that the host computer be a member of a domain and that it use Active Directory. For this reason, the administrator installing an enterprise CA must have Write permission to Active Directory.

If the administrator has Write permission to Active Directory, specifying the shared folder is optional; however, it is recommended.

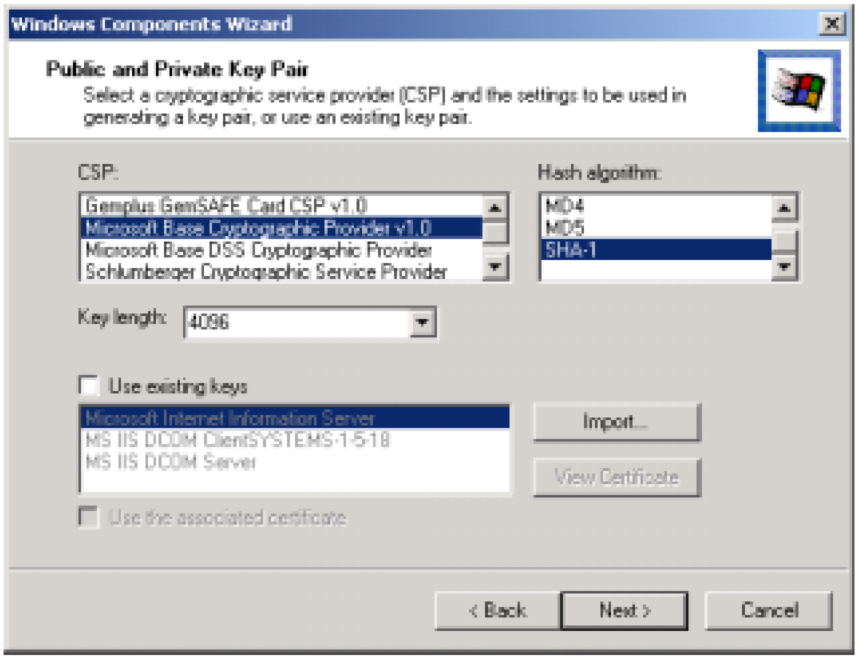
Stand-alone CAs

Stand-alone CAs are generally selected if it will be used to issue certificates to entities outside of your organization, the CA is supporting a non-Windows 2000 domain, or the use of Active Directory or other Windows 2000 PKI features is not desired. It is a good idea to configure a stand-alone CA as your root CA. Keep it offline once it is configured, physically secured, and enforce a two-person control on all actions taken on the CA through your security policy. This could be accomplished by granting one user "Log on locally" rights with no permissions to manage certificates, while a second user is granted permission to manage certificates, but does not have the right to "Log on locally". It would be a good idea to grant your Site Security Officer the "Log on locally" privilege. This would minimize the opportunity of a malicious administrator to manipulate critical certificate services' files.

Stand-alone Root CA

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

- ❑ 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**.
- ❑ (Optional) Select the **Advanced options** check box and apply the desired settings.



Windows Components Wizard

Public and Private Key Pair

Select a cryptographic service provider (CSP) and the settings to be used in generating a key pair, or use an existing key pair.

CSP:

- Gemplus GemSAFE Card CSP v1.0
- Microsoft Base Cryptographic Provider v1.0 (selected)
- Microsoft Base DSS Cryptographic Provider
- Schlumberger Cryptographic Service Provider

Hash algorithm:

- MD4
- MD5
- SHA-1 (selected)

Key length: 4096

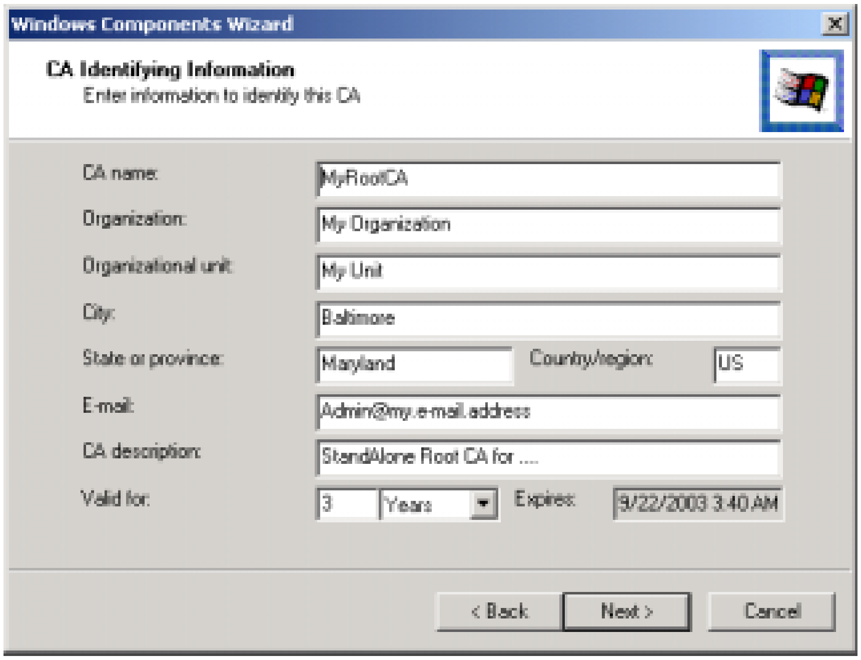
☐ Use existing keys

- Microsoft Internet Information Server
- MS IIS DCOM ClientSYSTEMS-1-5-18
- MS IIS DCOM Server

☐ Use the associated certificate

Figure 6 Stand-alone Root CA - Sample Dialog Box for "Advanced Options"

- ❑ When you are done, click **Next**.
- ❑ 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.

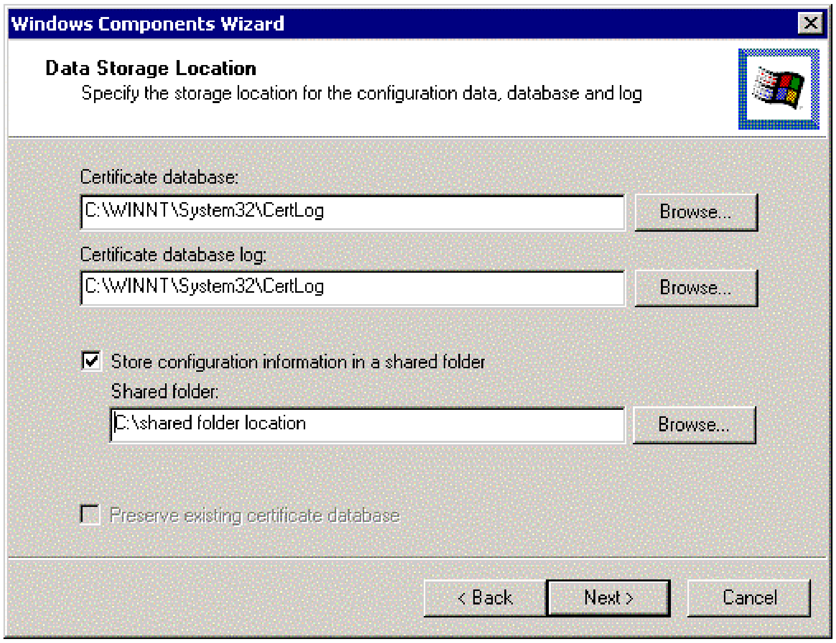


CA Identifying Information
Enter information to identify this CA

CA name:	MyRootCA
Organization:	My Organization
Organizational unit:	My Unit
City:	Baltimore
State or province:	Maryland
Country/region:	US
E-mail:	Admin@my.e-mail.address
CA description:	StandAlone Root CA for ....
Valid for:	3 Years
Expires:	9/22/2003 3:40 AM

Figure 7 Stand-alone Root CA - Identifying Information

- ❑ In **Validity duration**, specify the validity duration for the root CA. Click **Next**. The validity duration choosen 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.



Data Storage Location

Specify the storage location for the configuration data, database and log

Certificate database: C:\WINNT\System32\CertLog

Certificate database log: C:\WINNT\System32\CertLog

☑ Store configuration information in a shared folder

Shared folder: C:\shared folder location

☐ Preserve existing certificate database

Figure 8 Stand-alone Root CA - Data Storage Location

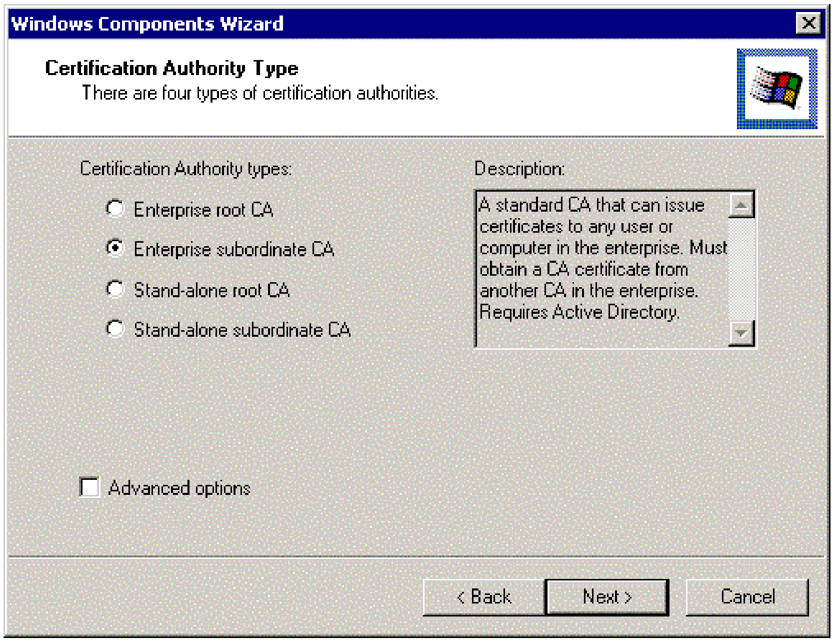
- If the World Wide Web Publishing Service is running, you will receive a request to stop the service before proceeding with the installation. Click **OK**.
- If prompted, type the path to the Certificate Services installation files.

Subordinate CA

Follow the same instructions for Enterprise and Stand-alone.

(Most of this information was taken from Microsoft's "Install an [enterprise/stand-alone] subordinate certification authority" Help page)

- 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**.

- 

Windows Components Wizard

Certification Authority Type

There are four types of certification authorities.

Certification Authority types:

○ Enterprise root CA

● Enterprise subordinate CA

○ Stand-alone root CA

○ Stand-alone subordinate CA

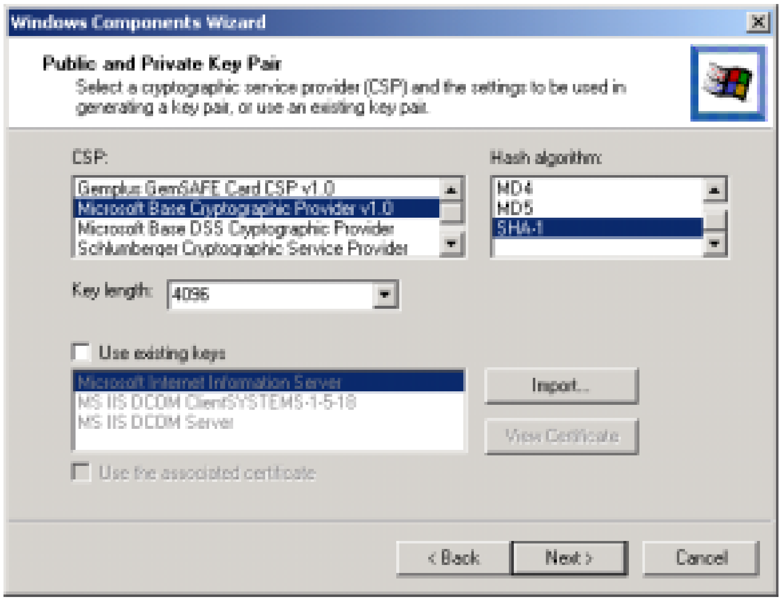
Description:

A standard CA that can issue certificates to any user or computer in the enterprise. Must obtain a CA certificate from another CA in the enterprise. Requires Active Directory.

□ Advanced options

Figure 9 Choosing Enterprise Subordinate CA

- (Optional) Select the **Advanced options** check box and apply desired settings.



Windows Components Wizard

Public and Private Key Pair

Select a cryptographic service provider (CSP) and the settings to be used in generating a key pair, or use an existing key pair.

CSP:

Gemplus GemSAFE Card CSP v1.0
Microsoft Base Cryptographic Provider v1.0
Microsoft Base DSS Cryptographic Provider
Schlumberger Cryptographic Service Provider

Hash algorithm:

MD4
MD5
SHA-1

Key length: 4096

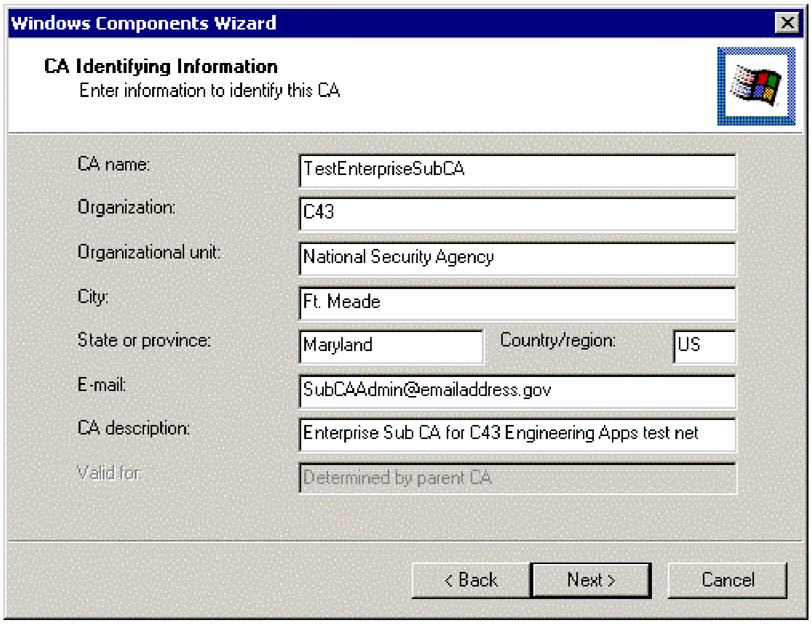
□ Use existing keys

Microsoft Internet Information Server
MS IIS DCOM ClientSYSTEMS-1-5-18
MS IIS DCOM Server

□ Use the associated certificate

Figure 10 Subordinate CA -- Sample Dialog Box for "Advanced Options"

- When you are done, click **Next**.
- Type in the name of the CA and other necessary identifying 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. Click **Next**.

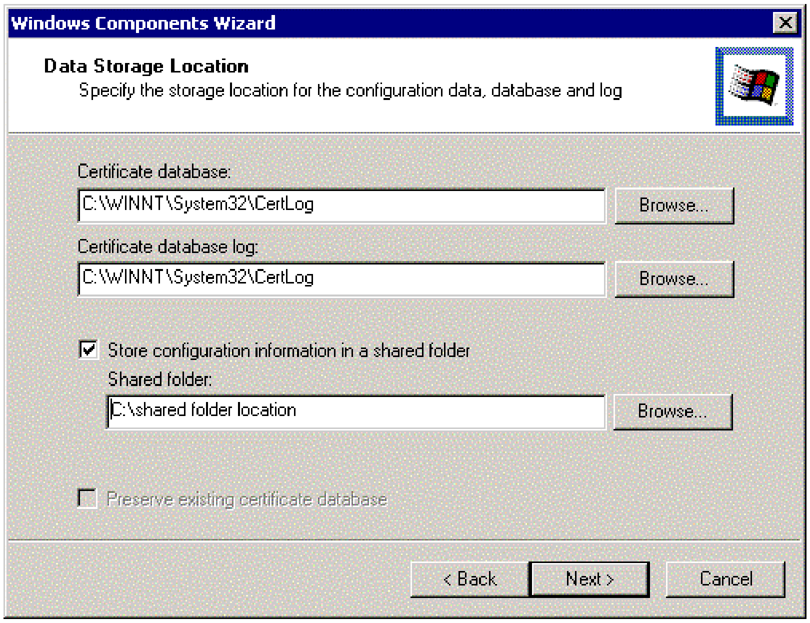


CA Identifying Information
Enter information to identify this CA

CA name:	TestEnterpriseSubCA
Organization:	C43
Organizational unit:	National Security Agency
City:	Ft. Meade
State or province:	Maryland
Country/region:	US
E-mail:	SubCAAdmin@emailaddress.gov
CA description:	Enterprise Sub CA for C43 Engineering Apps test net
Valid for:	Determined by parent CA

Figure 11 Subordinate CA - Identifying Information

- ❑ Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**.



Data Storage Location
Specify the storage location for the configuration data, database and log

Certificate database:
C:\WINNT\System32\CertLog

Certificate database log:
C:\WINNT\System32\CertLog

☑ Store configuration information in a shared folder
Shared folder:
C:\shared folder location

☐ Preserve existing certificate database

Figure 12 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 following “NOTE”.

- 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, you must submit a certificate request to a parent CA. The procedure for doing so differs depending on whether or not the parent CA is available online.

If a parent CA is available online:

- 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.

If a parent CA is not available online:

- 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 there is a subordinate CA certificate that does *not* include the full certification path, the new subordinate CA being installed must be able to build a valid CA chain when it starts. Thus, the parent CA's certificate must be placed 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. The certificate of the root CA also must be placed in the chain into the Trusted Root Certification Authorities store. These certificates should be installed in the appropriate certificate store before the CA certificate is installed 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 by clicking **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**
- 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**.

Renewing CA Certificates

A CA cannot issue certificates beyond the end of its validity period. When a CA reaches the end of its validity period, all certificates issued by that CA expire. This is done to ensure that a CA that has not been renewed deliberately cannot have the certificates issued by it used as valid security credentials. These certificates will no longer be valid, even if they have not reached the end of their own validity period.

As a CA nears the end of its validity period, it will issue certificates with shorter and shorter validity periods. To avoid the problem of issuing certificates with VERY short validity periods, have a plan in place to renew the CA well before the end of its validity period.

Since others rely on the root CA's certificate to form a certificate chain, and the life a root CA will most likely outlast its validity period, the root CA must be able to renew its certificate. If a root CA renews its certificate using the same key, others who rely on the root CA's certificate do not need to have the new root certificate prior to verifying certificates signed by it. Relying parties can obtain the new certificate any time after it has been created, especially after it has been used to issue new certificates. Attacks should be minimal against the root CA if the recommendations in this document are followed, i.e., offline, physically secured, two-person control, etc.

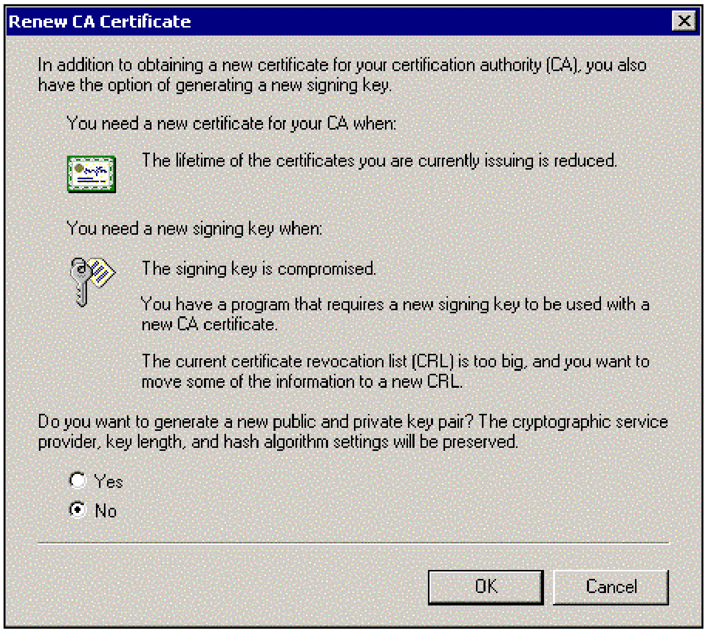
To ensure the security of any CA, select a long key length during installation, which is more secure against brute force attacks. This makes it possible to use the same private key for a longer period of time without fear of compromise. With today's technology, a key-length of 4096 is expected to be relatively safe against brute force attack for 15-20 years. Do not mistake this to mean that issuing certificates with long validity periods is recommended. The longer the certificate is valid, the greater the uncertainty of compromise posed by future developments in technology. A recommended strategy is to create CA certificates using a 4096-bit key. Set the validity period for the root CA certificate to 3-5 years. Renew the root certificate 1 year prior to the end of the validity expiration date. Each time the root certificate is renewed, evaluate whether or not, given the current technology in cryptographic analysis, the same key can be used for the next 3-5 years. Intermediate CAs (CAs which only issue certificates to other CAs) can have their certificates renewed 6-12 months prior to the end of their validity period (which can be no longer than 2 years) using existing keys. Since they serve a limited role in the PKI and their database logs can easily be monitored, using existing keys during the renew process poses minimal risk.

CAs that issue certificates to users and computers should be renewed 6-12 months prior to the end of their validity period using NEW keys. Issuing CAs are online and interact with users much more frequently than root or subordinate CAs, making them more susceptible to attack. Using this strategy makes an attack on any one key less valuable to a hacker because the compromised key would have a limited lifetime. In highly secure areas and in small intranet environments, renewing certificates using new keys is the most secure strategy for all CAs in the enterprise.

When a new key is used, a new CRL Distribution Point (CDP) is created, making CRL management easier. For CAs that issue large numbers of certificates and, possibly revoke large numbers of certificates, you can avoid the problem of having to distribute a very large CRL by renewing the CA with a new key well before the end of its validity period. This causes the CA to publish to the new CDP a separate CRL for the revoked certificates it has issued using the new key. It will also continue to publish a CRL to the old CPD for certificates signed with the old key for as long as those revoked certificates have not reached the end of their validity period. This strategy reduces the size of the CRL a certificate verifier has to download when presented with a certificate from an issuing CA.

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, **No** will be selected for root and subordinate CAs. See **Figure 13**
- ❑ Certificate Services will then restart and the validity date of the new certificate will be increased.


Renew CA Certificate

In addition to obtaining a new certificate for your certification authority (CA), you also have the option of generating a new signing key.

You need a new certificate for your CA when:

The lifetime of the certificates you are currently issuing is reduced.

You need a new signing key when:

The signing key is compromised.

You have a program that requires a new signing key to be used with a new CA certificate.

The current certificate revocation list (CRL) is too big, and you want to move some of the information to a new CRL.

Do you want to generate a new public and private key pair? The cryptographic service provider, key length, and hash algorithm settings will be preserved.

○ Yes
● No

Figure 13 Renewing CA Certificate

If the CA certificate being renewed belongs to a subordinate CA, the request must be submitted to a parent CA, then retrieve the new certificate and install it 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.

This Page Intentionally Left Blank

Chapter

2

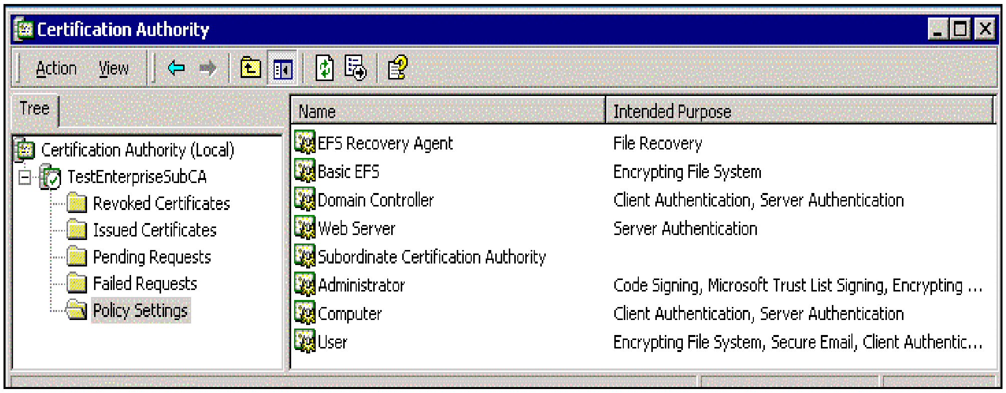
Managing Certificates with the MMC

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.

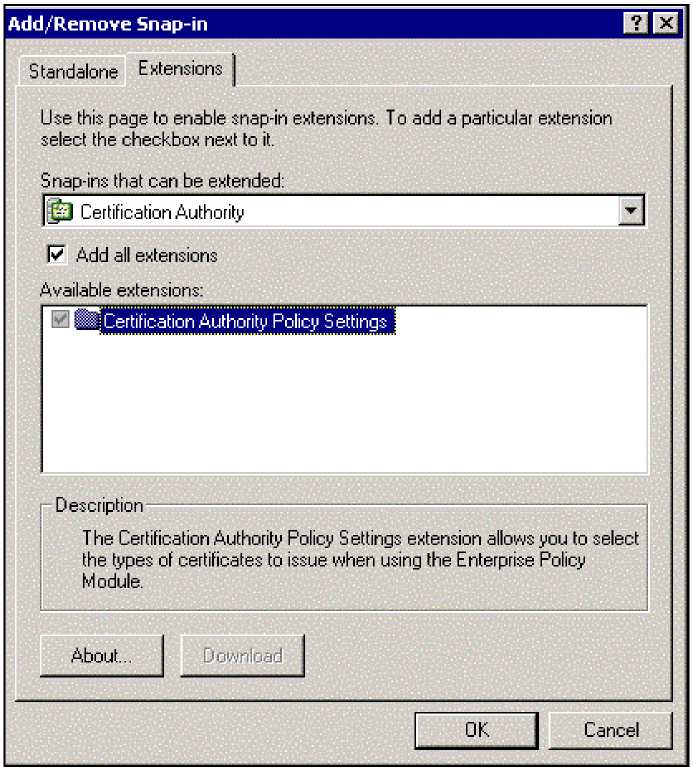


- Certification Authority (Local)
  - TestEnterpriseSubCA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Policy Settings

Name	Intended Purpose
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Subordinate Certification Authority	
Administrator	Code Signing, Microsoft Trust List Signing, Encrypting ...
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Client Authentic...

Figure 14 Certification Authority Snap-in

A snap-in extension is available for the Certification Authority snap-in. The Certification Authority Policy Setting extension allows the administrator to select the types of certificates the CA will be permitted to issue. Select the **Policy Settings** folder to view a list of templates the CA can be configured to issue (See **Figure 14**). Delete templates by right-clicking the template you wish to remove and select **Delete.** To add a certificate template, right-click the **Policy Settings** folder and select **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** (See **Figure 15**). The new template will then be displayed in the right pane of the Certification Authority window. This is where the administrator can control the types of certificates the CA will make available to requesting users (See **Figure 16**). More information regarding certificate templates can be found in the Enterprise CA Templates section of this document.



Use this page to enable snap-in extensions. To add a particular extension select the checkbox next to it.

Snap-ins that can be extended: Certification Authority

☑ Add all extensions

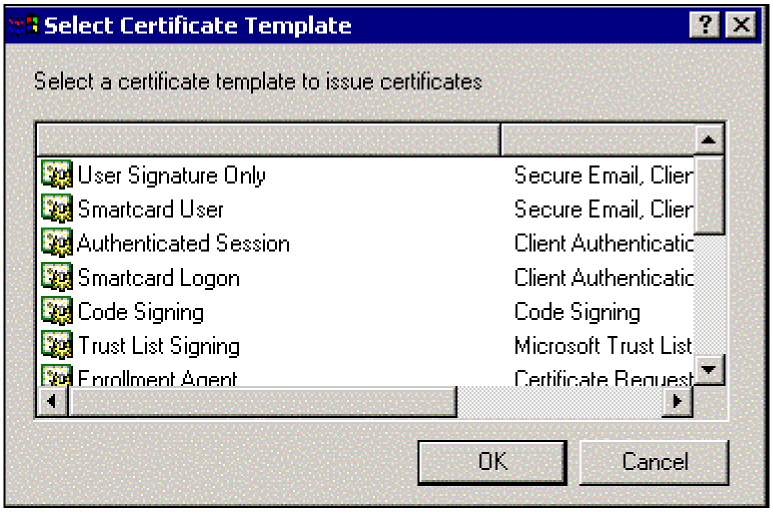
Available extensions:

☑ Certification Authority Policy Settings

Description

The Certification Authority Policy Settings extension allows you to select the types of certificates to issue when using the Enterprise Policy Module.

Figure 15 Add/Remove Certification Authority Policy Setting



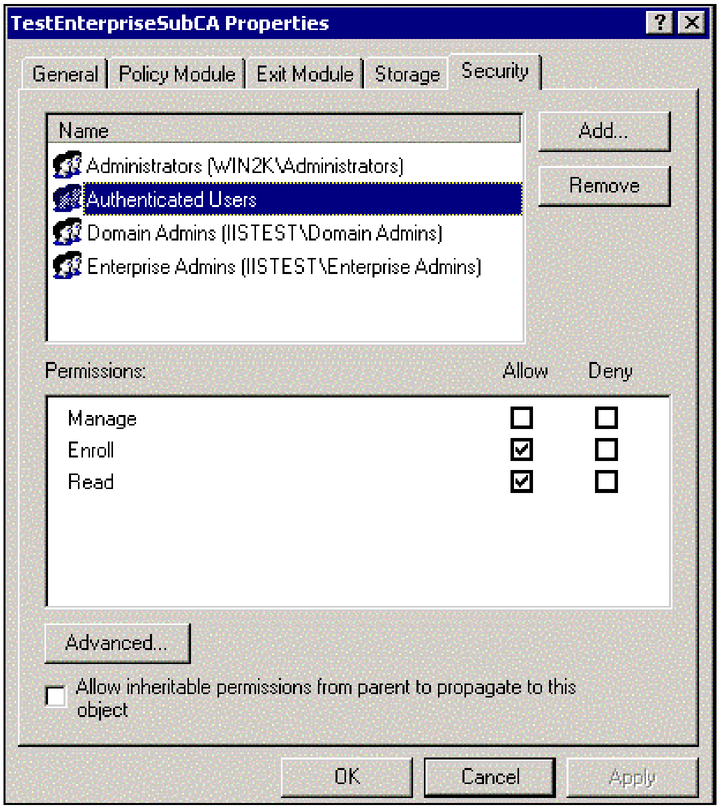
Select a certificate template to issue certificates

User Signature Only	Secure Email, Clier
Smartcard User	Secure Email, Clier
Authenticated Session	Client Authenticatic
Smartcard Logon	Client Authenticatic
Code Signing	Code Signing
Trust List Signing	Microsoft Trust List
Enrollment Agent	Certificate Request

Figure 16 Selecting Certificate Templates

It is a good idea to set security permissions and delegate control of CAs. 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 (See Figure 17). Unless your security policy requires a change to this setup, these permission settings are sufficient.

NOTE: 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.



Name
- Administrators (WIN2K\Administrators)
- Authenticated Users
- Domain Admins (IISTEST\Domain Admins)
- Enterprise Admins (IISTEST\Enterprise Admins)

Permissions:	Allow	Deny
Manage	□	□
Enroll	☑	□
Read	☑	□

□ Allow inheritable permissions from parent to propagate to this object

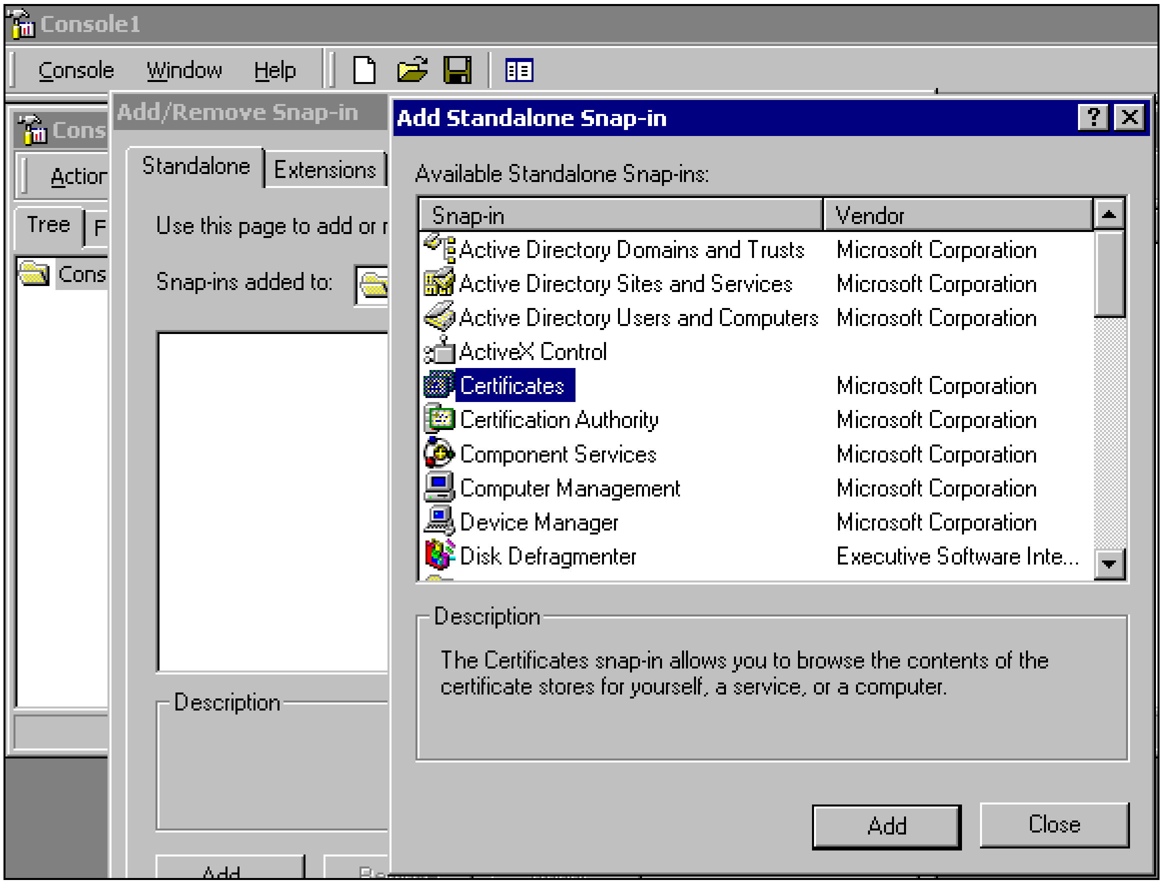
Figure 17 Setting Security Permissions for CA Control

Certificate Store and Active Directory

Certificates, CRLs, and certificate trust lists are stored in a permanent location for access by users. This permanent location is called a certificate store. Certificate stores manage certificates and their associated properties. An enterprise root certificate store is located on the local machine. There is also an enterprise root certificate store in Active Directory. When a domain administrator installs a Windows 2000 root CA, using the enterprise policy or stand-alone policy, the enterprise root certificate store is updated with the new certificate. A Windows 2000 Resource Kit tool, DSStore, is also available to administrators to add an offline stand-alone CA certificate to the store. The contents of the root certificate store in Active Directory are downloaded to each computer in the enterprise during bootup, when an auto-enrollment event is pulsed (about every eight hours), during group policy updates, or when manually pulsed using the DSStore. In this way, root certificates can be distributed to all computers in the forest. Active Directory is used as a certificate store by enterprise CAs to publish trusted root certificates, issued certificates, and CRLs. During the installation of an enterprise CA, and a stand-alone CA with access to Active Directory, information concerning the CA is written into a CA object in Active Directory. Domain clients use this information to find out about available CAs and the types of certificates they issue.

To view a computer's certificate store, the Certificates snap-in can be used. This is helpful when you want to verify that a certificate has been issued for the computers within the domain. Follow these steps to load the **Certificates** snap-in into a new MMC.

- ❑ Click **Start →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** (See **Figure 18**)



Available Standalone Snap-ins:

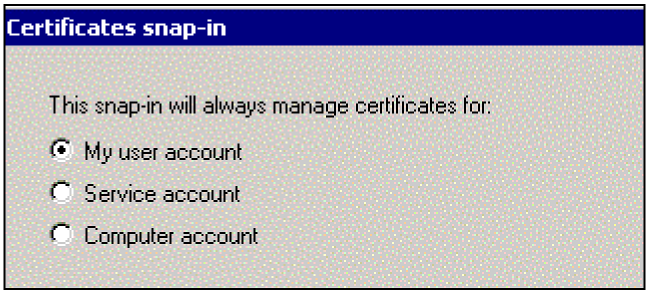
Snap-in	Vendor
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Executive Software Inte...

Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Figure 18 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 19**). 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 20**). 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.



Certificates snap-in

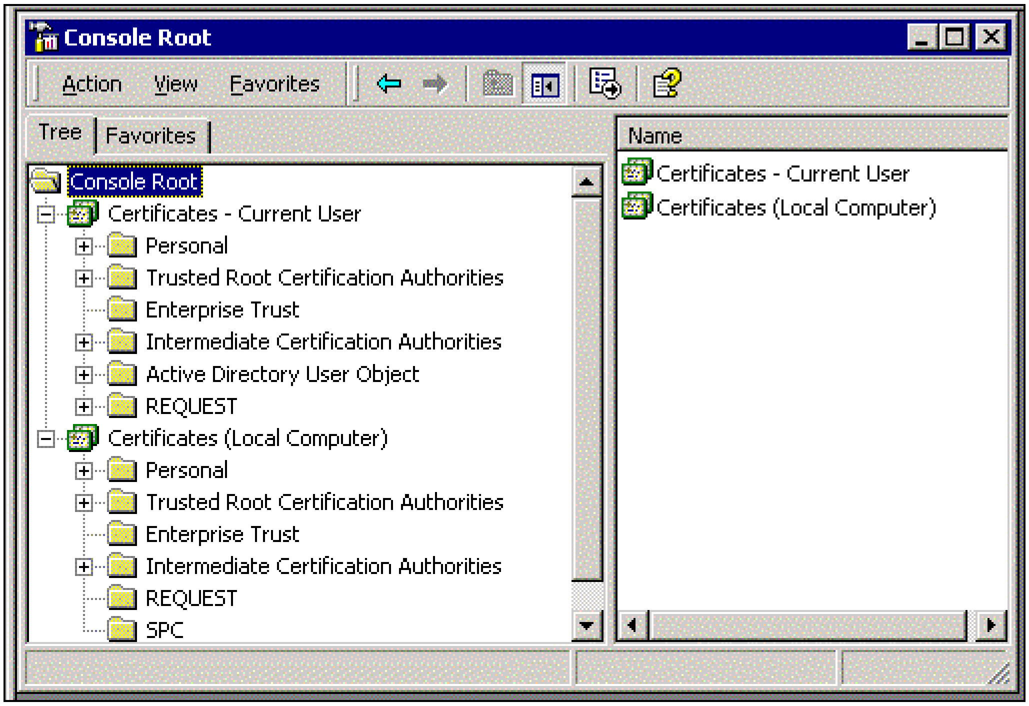
This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

Figure 19 Selecting Account for Certificate Management



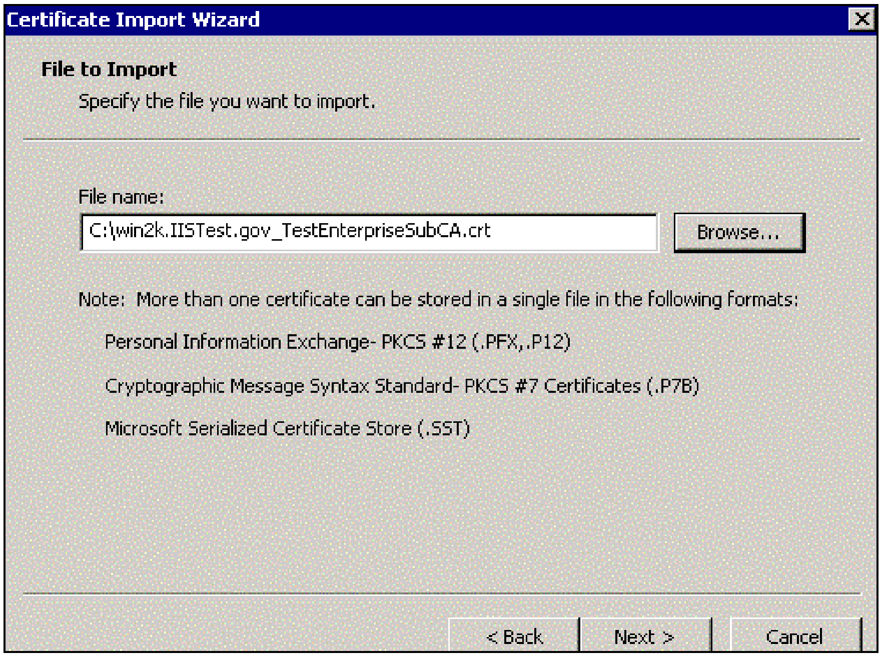
Console Root
- Certificates - Current User
  - Personal
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - Active Directory User Object
  - REQUEST
- Certificates (Local Computer)
  - Personal
  - Trusted Root Certification Authorities
  - Enterprise Trust
  - Intermediate Certification Authorities
  - REQUEST
  - SPC

Name
- Certificates - Current User
- Certificates (Local Computer)

Figure 20 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** ⇒ **Import** from the pull-down menu. This starts the Import Wizard.
- Fill in the appropriate information pertaining to the certificate to install (See **Figure 21**).



File to Import

Specify the file you want to import.

File name:

C:\win2k.IISTest.gov_TestEnterpriseSubCA.crt

Note: More than one certificate can be stored in a single file in the following formats:

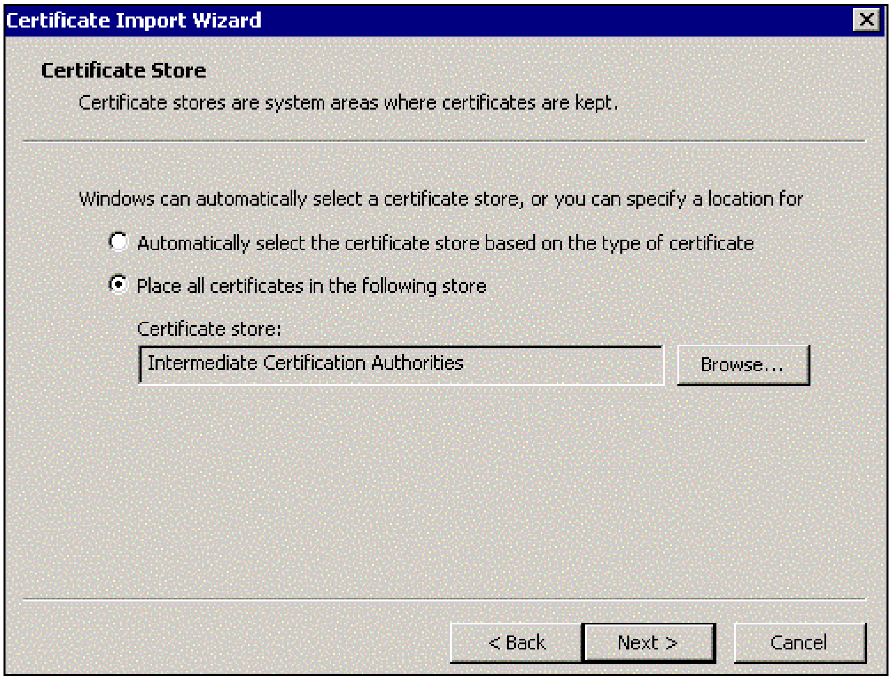
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Figure 21 Selecting File to Import in the Certificate Import Wizard

- ❑ Select the appropriate Certificate Store to install the certificate (See **Figure 22**).



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

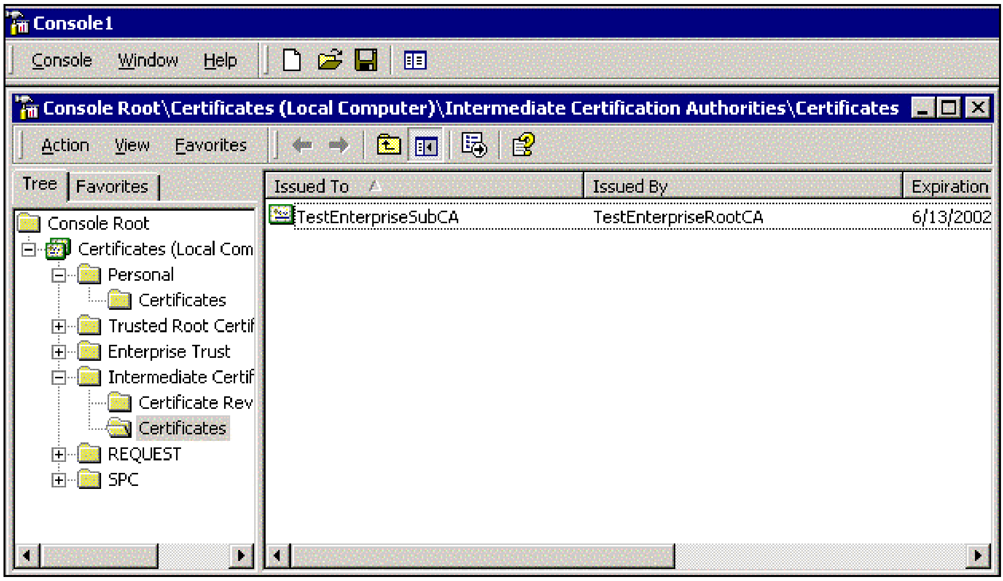
Certificate store:

Intermediate Certification Authorities

Figure 22 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.

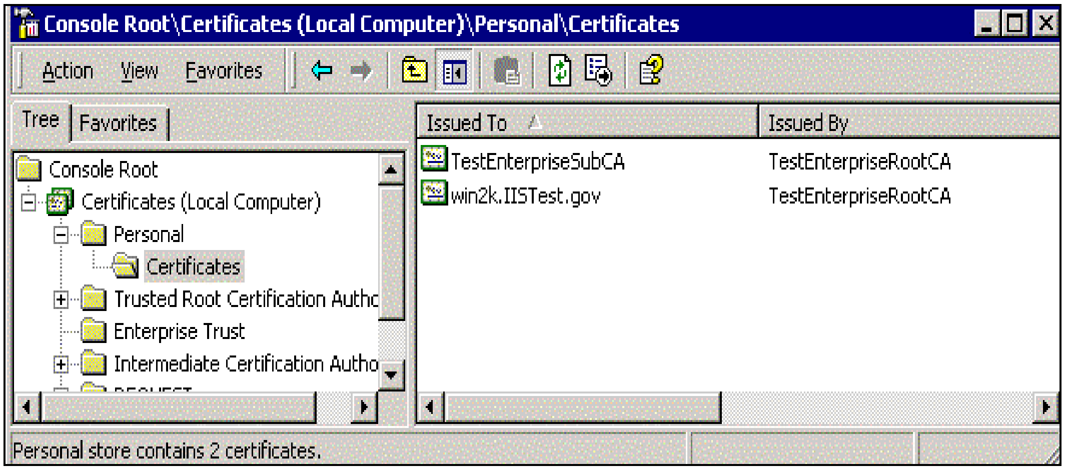
- In the Trusted Root Certification Authorities and Intermediate Certification Authorities stores, it is important to delete all untrusted CAs that are listed.



Issued To	Issued By	Expiration
TestEnterpriseSubCA	TestEnterpriseRootCA	6/13/2002

Figure 23 Deleting Untrusted CA

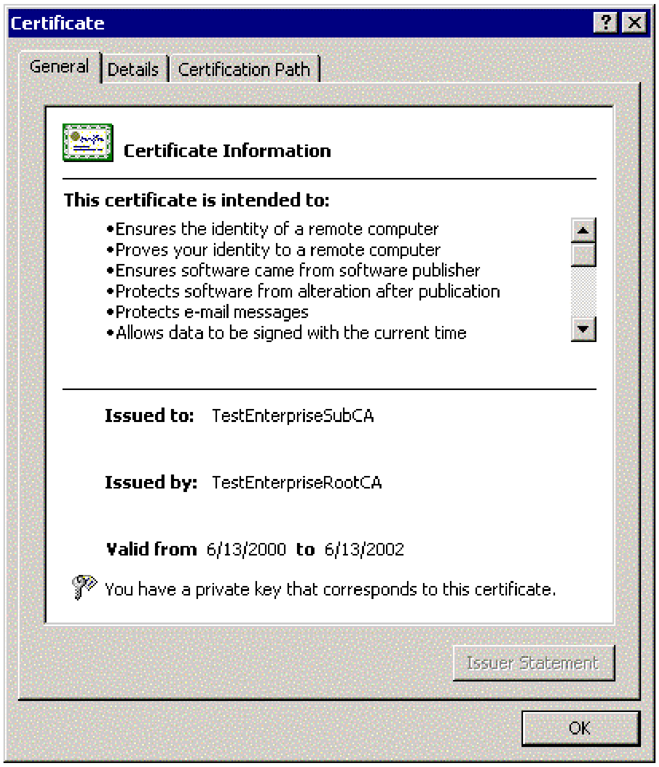
- Expand the **Personal** folder under the Local Computer Certificates and click the **Certificates** folder (store). See **Figure 24**. All certificates issued to the local machine are listed in the right pane. Double-click any certificate in the store to view its details. **Figure 25, Figure 26, and Figure 27** show the certificate General, Details, and Certification Path tabs respectively.


Console Root\Certificates (Local Computer)\Personal\Certificates
Action View Favorites
Tree Favorites
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authc
Enterprise Trust
Intermediate Certification Autho
REQUEST

Issued To	Issued By
TestEnterpriseSubCA	TestEnterpriseRootCA
win2k.IISTest.gov	TestEnterpriseRootCA

Personal store contains 2 certificates.

Figure 24 Personal Certificates



Certificate Information

This certificate is intended to:

- •Ensures the identity of a remote computer
- •Proves your identity to a remote computer
- •Ensures software came from software publisher
- •Protects software from alteration after publication
- •Protects e-mail messages
- •Allows data to be signed with the current time

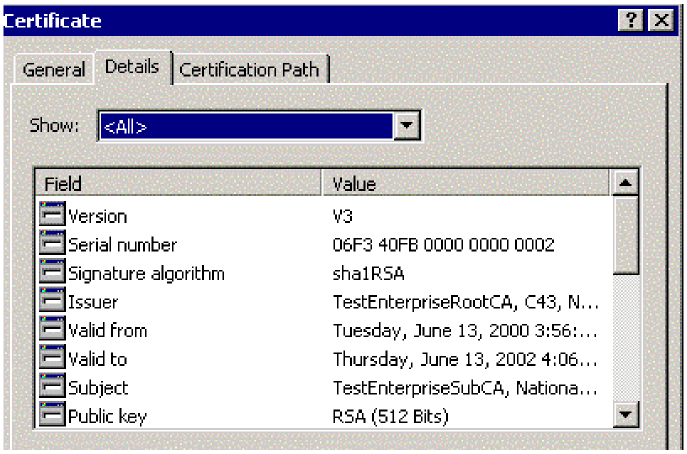
Issued to: TestEnterpriseSubCA

Issued by: TestEnterpriseRootCA

Valid from 6/13/2000 **to** 6/13/2002

You have a private key that corresponds to this certificate.

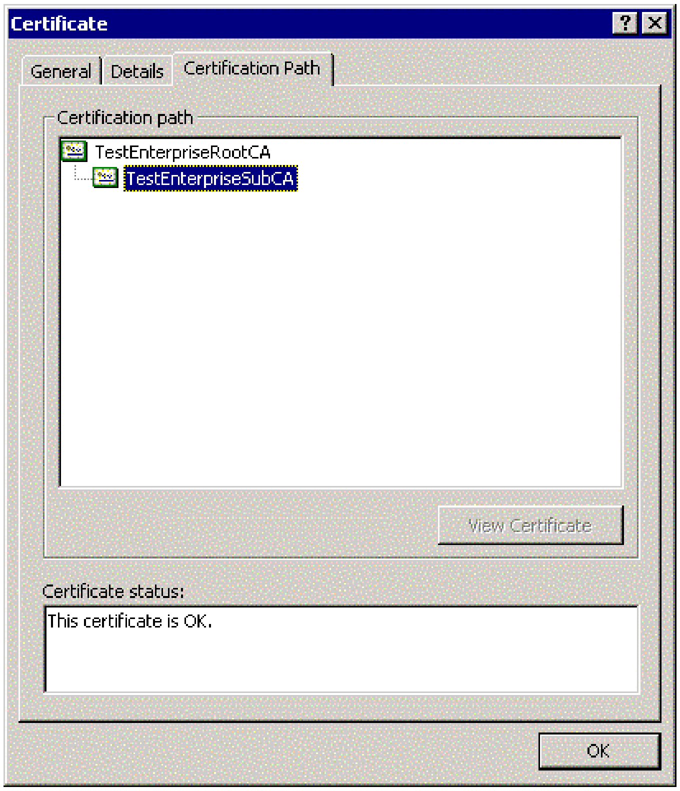
Figure 25 Certificate General Tab



Show: <All>

Field	Value
Version	V3
Serial number	06F3 40FB 0000 0000 0002
Signature algorithm	sha1RSA
Issuer	TestEnterpriseRootCA, C43, N...
Valid from	Tuesday, June 13, 2000 3:56:...
Valid to	Thursday, June 13, 2002 4:06...
Subject	TestEnterpriseSubCA, Nationa...
Public key	RSA (512 Bits)

Figure 26 Certificate Details Tab



Certificate status:

This certificate is OK.

Figure 27 Certificate Certification Path Tab

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. This prevents the user from having to provide detailed information about the type of certificate that is needed. Instead, they can select a template name that indicates the purpose of the certificate. 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: Based on the site's security policy, make available to certificate requesters ONLY the templates for the certificate types the CA is required to issue.

Templates define the information that goes into a certificate, certificate extensions, and the origin of the information. Various templates are published in Active Directory and are global across a Windows 2000 forest. Single-purpose and multi-purpose templates can be issued by an enterprise CA. Single-purpose templates generate certificates that can be used by a single application, such as Smart Card Logon, S/MIME, or Encrypting File System (EFS). Multi-purpose templates generate certificates that can be used for a number of applications, such as SSL, S/MIME and EFS. Templates exist for issuing certificates to both computers and users.

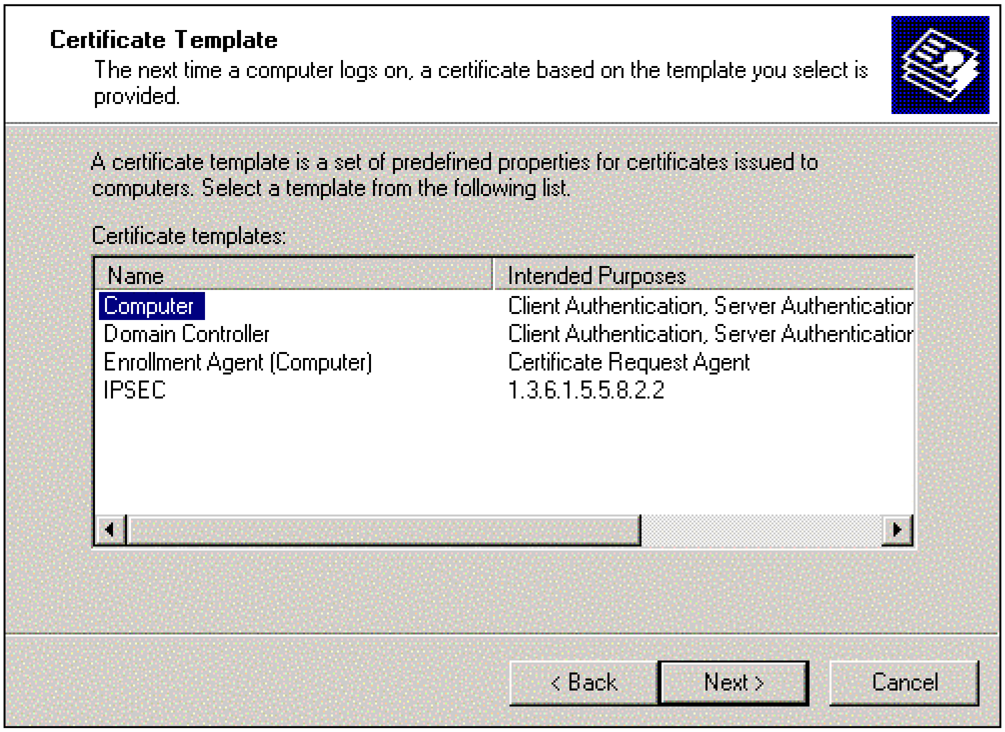
An enterprise CA uses domain authentication (access tokens) to identify users and computers. The CA impersonates the user to obtain the correct security context. This enables the policy module to establish the rights of the user to the requested template and the CA. Computers can be configured to automatically 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).

Setup automatic certificate requests for computers on a Domain Controller 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 28**:



Certificate Template

The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSEC	1.3.6.1.5.5.8.2.2

Figure 28 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

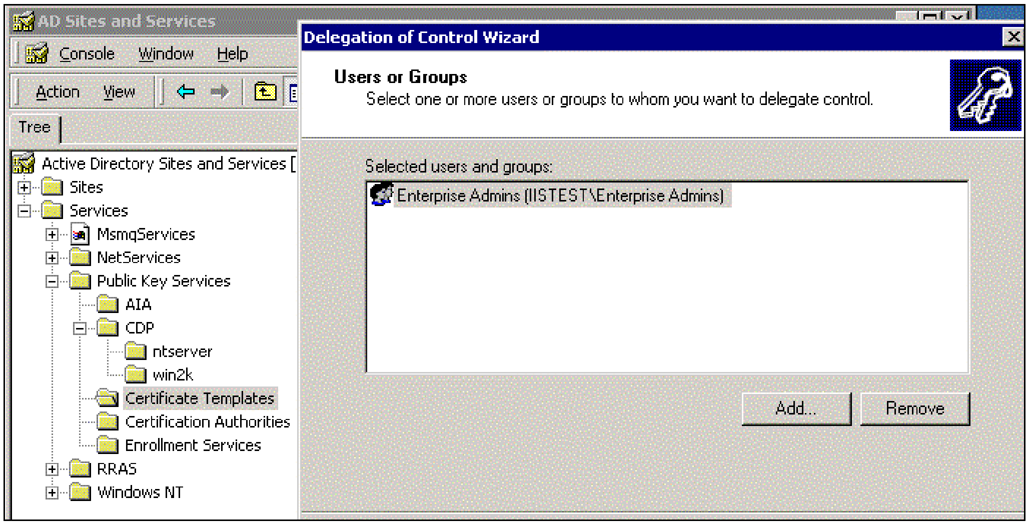
Certificate template security permissions determine who in the enterprise can enroll for the type of certificate specified by the template. Administrators should go through the list of templates and remove domain users and authenticated users from the security permissions list of those templates the 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 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 the user (the steps for doing this were discussed earlier in this section).

Default permissions on templates vary depending on the template. It is important to determine the purpose of the CA and select templates accordingly. Then, assign permissions to these templates. Permissions include: Full Control, Read, Write, and Enroll. End-users only require the permission to enroll for a certificate. Enterprise Admins do not require full control of templates. Their access varies based on the certificate type.

Default settings for Enterprise Admins are usually sufficient. 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. 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. It is a good idea to remove all certificates that the CA is not required to make available to users.

An administrator can also delegate control over the templates' container. Highlight the **Certificate Templates** container, right-click and select **Delegate Control**. The following window is displayed, allowing the administrator to delegate the management of the CA templates to the Enterprise Admins group, for example.



Delegation of Control Wizard

Users or Groups

Select one or more users or groups to whom you want to delegate control.

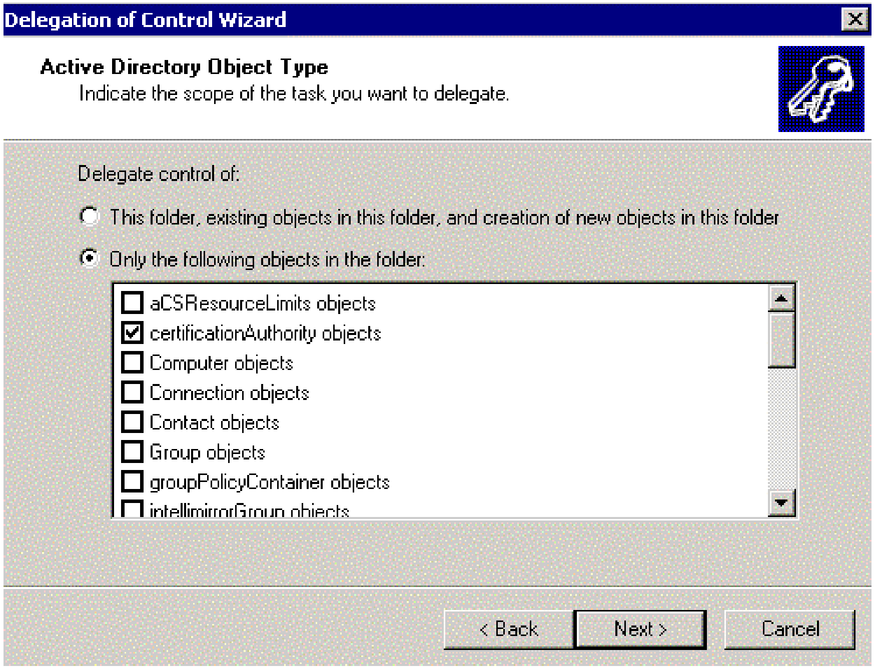
Selected users and groups:

Enterprise Admins (IISTEST\Enterprise Admins)

Figure 29 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 30**). 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.



Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

○ This folder, existing objects in this folder, and creation of new objects in this folder

● Only the following objects in the folder:

- □ aCSResourceLimits objects
- ☑ certificationAuthority objects
- □ Computer objects
- □ Connection objects
- □ Contact objects
- □ Group objects
- □ groupPolicyContainer objects
- □ intellimirrorGroup objects

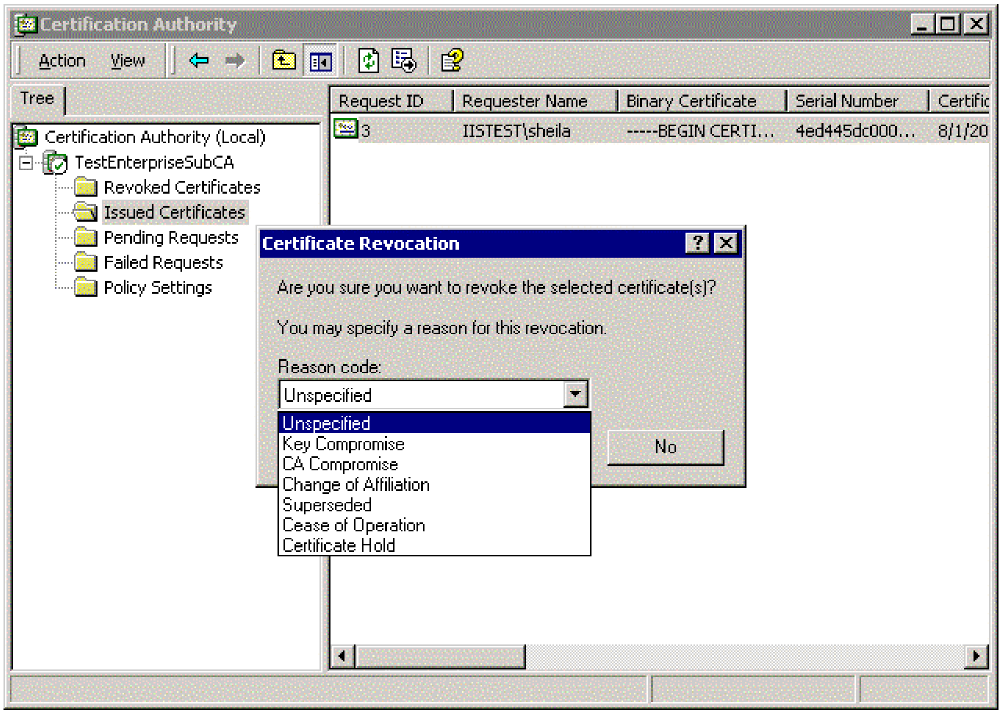
Figure 30 Delegating Control of the Following Objects

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:

- ❑ Using the Certification Authority, 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**. (See **Figure 31**).



Request ID	Requester Name	Binary Certificate	Serial Number	Certific
3	IISTEST\sheila	-----BEGIN CERTI...	4ed445dc000...	8/1/20

Are you sure you want to revoke the selected certificate(s)?

You may specify a reason for this revocation.

Reason code: Unspecified

- Unspecified
- Key Compromise
- CA Compromise
- Change of Affiliation
- Superseded
- Cease of Operation
- Certificate Hold

Figure 31 Selecting Reason for Certificate Revocation

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.

- The certificate is marked as revoked and is moved to the **Revoked Certificates** folder. The revoked certificate will appear on the CRL the next time it is published.
- 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.

Every CA publishes an updated CRL at regular intervals, determined by the administrator. The default publish period is set to one week. This is based on the machine's local time and the date the CA was installed. There is a difference in the publish period and the validity period of a CRL. The validity period is extended by 10% (up to 12 hours) of the publish period to allow for Active Directory replication. For example, if the CA sets the publish period to 24 hours, the CRL will be valid for 26.4 hours. Also, 10 minutes is added to either side of the validity period to allow for variances in computer clock settings.

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. By default, a CRL file is published on the CA in `*Systemroot*\System32\Certsrv\Certenroll`. 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.

Chapter

3

Additional Security Issues

Antiviral Program

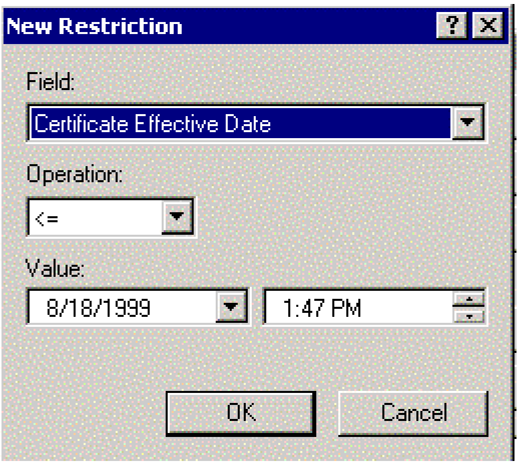
There are numerous public sector sources for information on antiviral products. A suggested starting point is the International Computer Security Association at http://www.ncsa.com. This Web page contains a lot of generic information about viral solutions and hot links to the major vendors.

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

Audits

The Certificate Services Log and Database is useful when auditing a CA. It can be used to review queued requests and issued certificates. An administrator can use the Certificate Services Log and Database when determining which certificates need to be placed on the CRL. For instance, an administrator may discover an intrusion occurred on the CA on a specific date and determine all certificates issued after that date cannot be trusted. A filter can be used to display information about certificates issued during a specified period of time. Those certificates can be placed on a CRL and new certificates can be issued. To display the Certificate Services Log and Database, perform the following steps:

- ❑ 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.
- ❑ By right-clicking **Issued Certificates** and selecting **View – Choose Columns**, the order of the displayed columns and add or remove displayed columns can be changed.
- ❑ By right-clicking **Issued Certificates** and selecting **View – filter**, the certificates to display based on the filter criteria can be selected. **Figure 32** is an example of the data that can be set in the filter window.



New Restriction

Field: Certificate Effective Date

Operation: <=

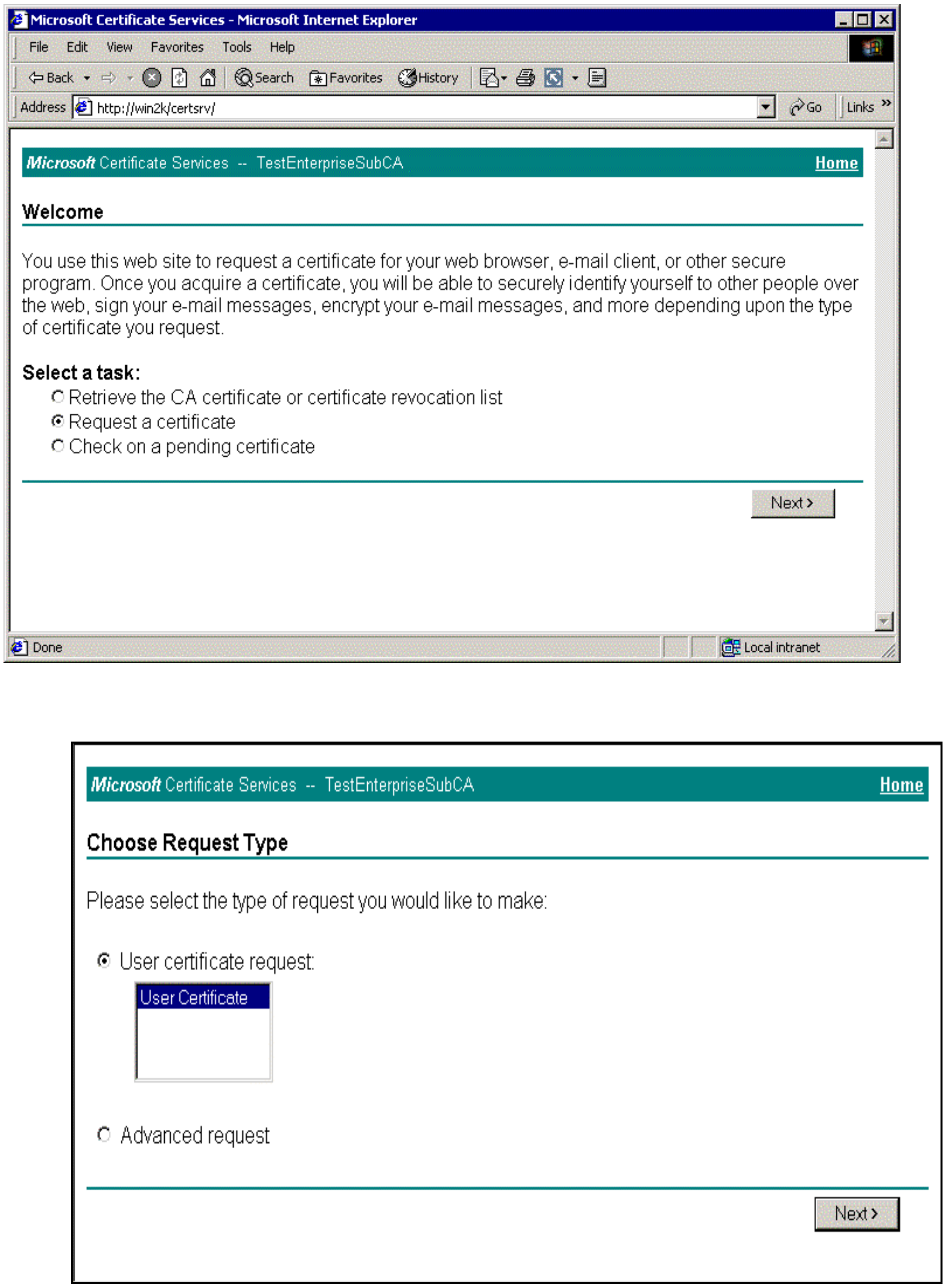
Value: 8/18/1999 1:47 PM

Figure 32 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. No more input is required from the user to issue a certificate.

During certificate enrollment, credential checks are performed on users. 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, but issues a certificate based on the information submitted by the requester. By default, the CA 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 33**).


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://win2k/certsrv/
Go Links
Done
Local intranet

Microsoft Certificate Services -- TestEnterpriseSubCA **Home**

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

○ Retrieve the CA certificate or certificate revocation list
● Request a certificate
○ Check on a pending certificate

Next >

Microsoft Certificate Services -- TestEnterpriseSubCA **Home**

Choose Request Type

Please select the type of request you would like to make:

● User certificate request:

User Certificate

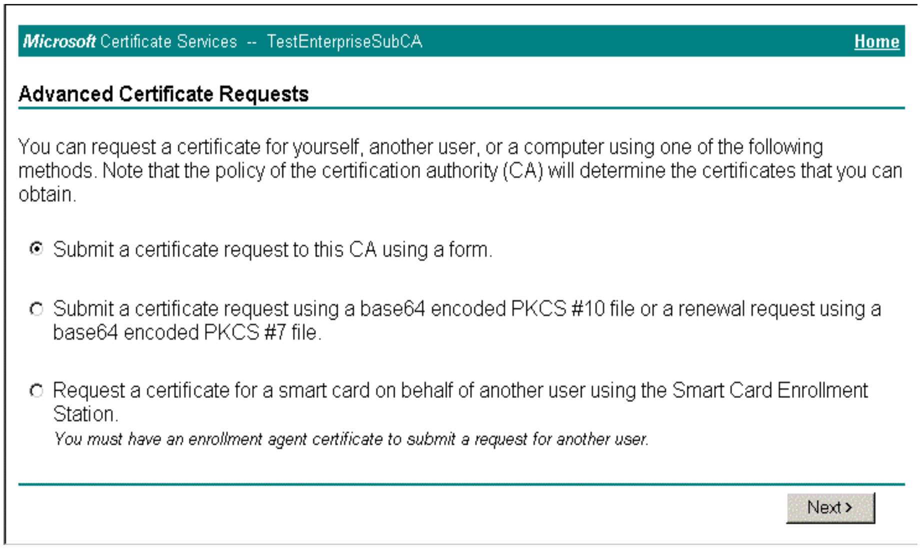
○ Advanced request

Next >

Figure 33 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 options seen in **Figure 34** are available when **Advanced request** is selected.



Microsoft Certificate Services -- TestEnterpriseSubCA — Home

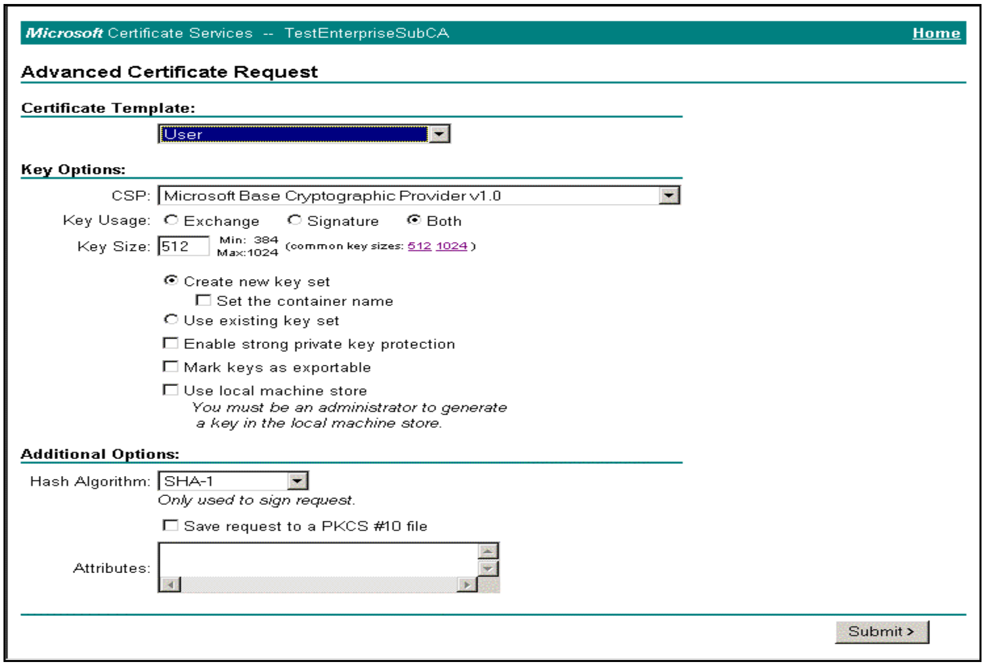
Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

● Submit a certificate request to this CA using a form.

○ Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.

○ Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.



Microsoft Certificate Services -- TestEnterpriseSubCA — Home

Advanced Certificate Request

Certificate Template:
User

Key Options:
CSP: Microsoft Base Cryptographic Provider v1.0
Key Usage: ○ Exchange ○ Signature ● Both
Key Size: 512 Min: 384 Max:1024 (common key sizes: 512 1024)

● Create new key set
□ Set the container name
○ Use existing key set
□ Enable strong private key protection
□ Mark keys as exportable
□ Use local machine store
You must be an administrator to generate a key in the local machine store.

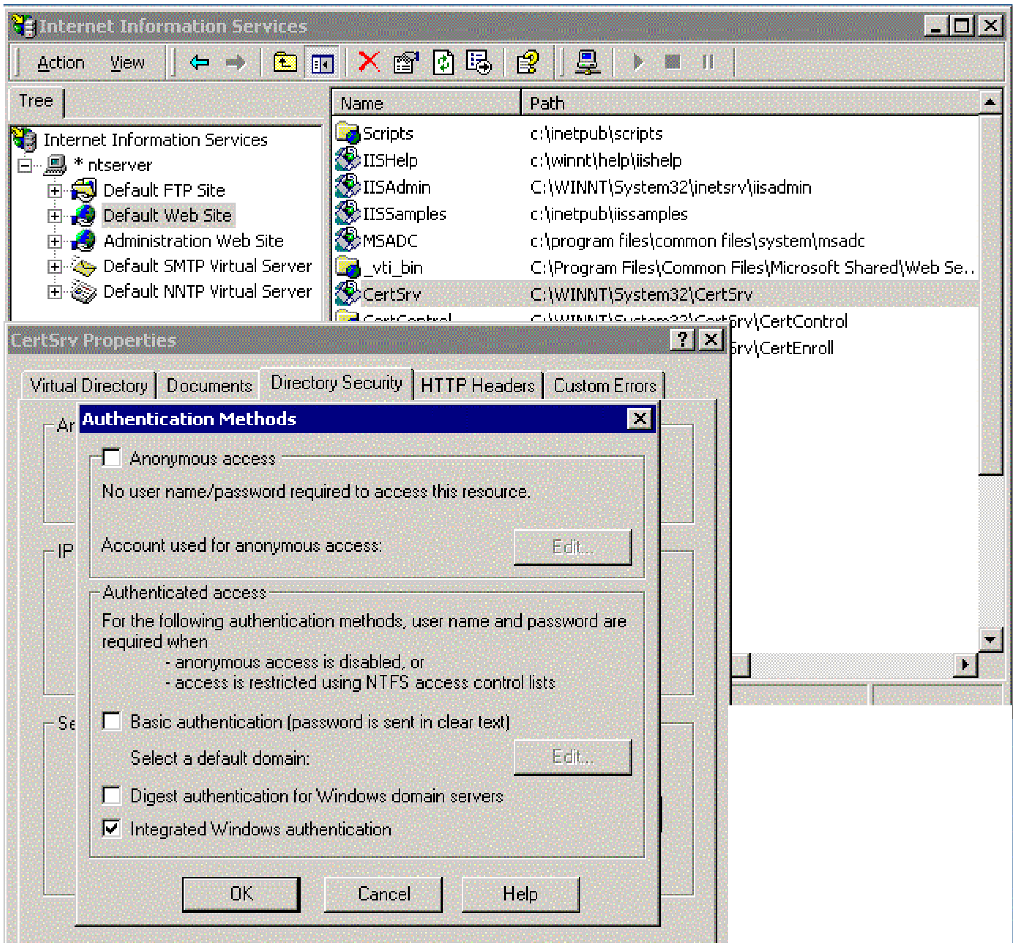
Additional Options:
Hash Algorithm: SHA-1
Only used to sign request.
□ Save request to a PKCS #10 file
Attributes:

Figure 34 Example for 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 **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.



Name	Path
Scripts	c:\inetpub\scripts
IISHelp	c:\winnt\help\iishelp
IISAdmin	C:\WINNT\System32\inetsrv\iisadmin
IISSamples	c:\inetpub\iissamples
MSADC	c:\program files\common files\system\msadc
_vti_bin	C:\Program Files\Common Files\Microsoft Shared\Web Se..
CertSrv	C:\WINNT\System32\CertSrv
CertControl	C:\WINNT\System32\CertSrv\CertControl
	...rv\CertEnroll

Authentication Methods

☐ Anonymous access

No user name/password required to access this resource.

Account used for anonymous access:

Authenticated access

For the following authentication methods, user name and password are required when
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☐ Basic authentication (password is sent in clear text)

Select a default domain:

☐ Digest authentication for Windows domain servers

☑ Integrated Windows authentication

Figure 35 Securing Certificate Service Web Pages

This Page Intentionally Left Blank

Chapter

4

Backups

Backup Procedures

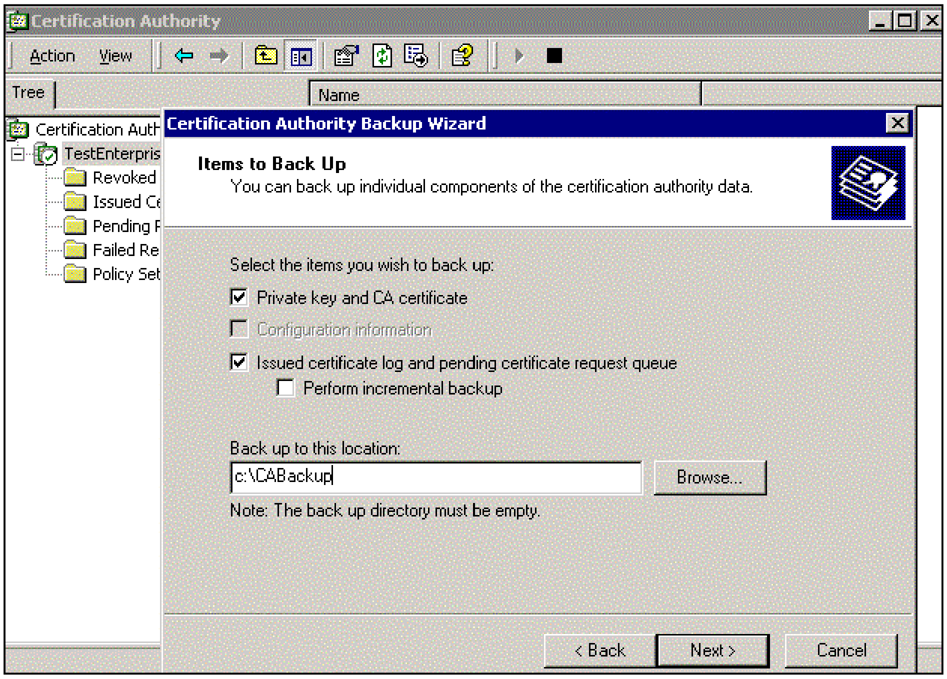
It is very important to include a disaster recovery policy in your site's security plan. There are several ways to backup the data on your server. Automatic backups, such as disk mirroring or disk duplexing, where there is a complete copy of the server's hard drive that can go online in the event the 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 36**)
- ❑ 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 37).
- ❑ The next window lists the options you chose to backup. Click **Finish** and the backup will take place. (See **Figure 38**).



Certification Authority Backup Wizard

Items to Back Up

You can back up individual components of the certification authority data.

Select the items you wish to back up:

☑ Private key and CA certificate

☐ Configuration information

☑ Issued certificate log and pending certificate request queue

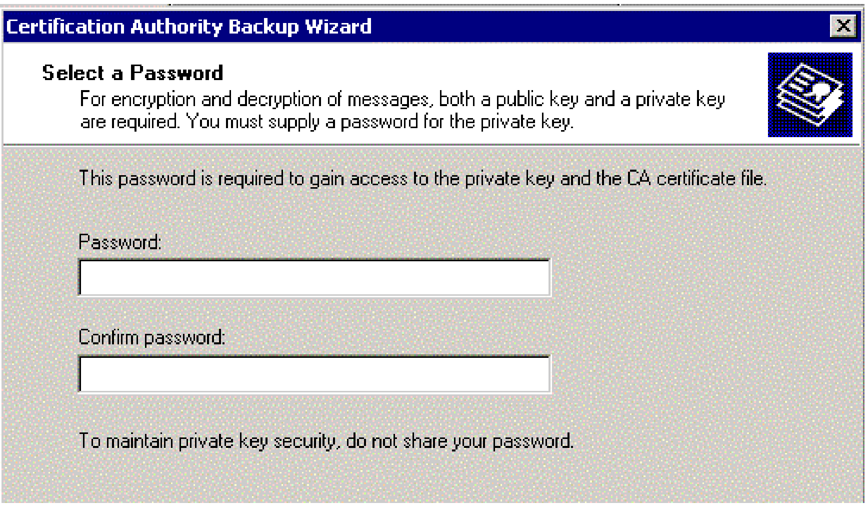
☐ Perform incremental backup

Back up to this location:

c:\CABackup

Note: The back up directory must be empty.

Figure 36 Selecting Items to Back-up



Select a Password

For encryption and decryption of messages, both a public key and a private key are required. You must supply a password for the private key.

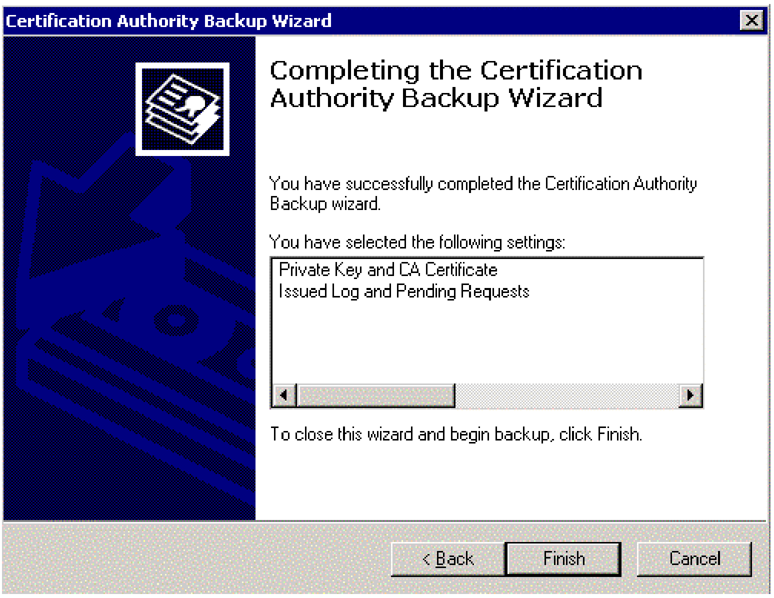
This password is required to gain access to the private key and the CA certificate file.

Password:

Confirm password:

To maintain private key security, do not share your password.

Figure 37 Selecting a Password for CA Backup



Completing the Certification Authority Backup Wizard

You have successfully completed the Certification Authority Backup wizard.

You have selected the following settings:

Private Key and CA Certificate
Issued Log and Pending Requests

To close this wizard and begin backup, click Finish.

Figure 38 Completion of CA Backup Wizard

Restoring Certificate Services

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

□ If Certificate Services is running, you are prompted to stop it. Click **OK**

□ The Certification Authority Restore Wizard opens. Click **Next**

□ 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**

□ 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**

□ 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

References

McLean, Ian, *Windows 2000 Security Little Black Book*, 2000.

Microsoft's web site, http://www.microsoft.com/