Report Number: C4-058R-00

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

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

Author:
Sheila Christman


Updated: 10 October 2001
Version 2.1.1

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

W2KGuides@nsa.gov

This Page Intentionally Left Blank

## Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- This document may contain recommended settings for the system Registry. Windows 2000 Certificate Services can be severely impaired or disabled with incorrect changes or accidental deletions when using a Registry editor (Regedt32.exe or Regedit.exe) to change the system configuration.
- Currently, there is no **undo** command for deletions within the Registry. Registry editor prompts the user to confirm the deletions if **Confirm on Delete** is selected from the options menu. When a key is deleted, the message does not include the name of the key being deleting. Therefore, check selection carefully before proceeding.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of July 26, 2001. See Microsoft's web page 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.

This Page Intentionally Left Blank

## Trademark Information

This Page Intentionally Left Blank

# 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 services. Although Microsoft's Internet Information Service (IIS) is required to enable users to request certificates through web pages, this document does not provide instructions for securely installing and managing IIS. That information, along with detailed information on using certificates with Internet Information Service, can be found in the document entitled *Secure Installation and Configuration of Microsoft's Internet Information Service 5.0*.

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

Some Certificate Services' security issues and corresponding configuration and administrative actions are very specific to the way the service is being implemented. 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 their site's local security policies.

| **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 Services 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 "*x*test.gov" will be used in the examples, screenshots, and listings.

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

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

This document consists of the following chapters:

**Chapter 1, "Windows 2000 Certificate Services,"**

**Chapter 2, "Managing Certificates with the MMC,"**

**Chapter 3, "Additional Security Issues,"**

**Chapter 4, "Backups,"**

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

## An Important Note About Operating System Security

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

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

**Table 2 Permissions on Certificate Directories**

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

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

This Page Intentionally Left Blank

Chapter 1

# Windows 2000 Certificate Services



Microsoft Windows 2000 Certificate Services offers an integrated public key infrastructure (PKI) that enables the secure exchange of information across the Internet, extranets, and intranets. PKI refers to a system of digital certificates and certificate authorities (CAs) that verify and authenticate the validity of each party involved in an electronic transaction. 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 recommended settings for securing a Windows 2000 environment (found in the set of accompanying NSA Windows 2000 security guides) that are appropriate for your site based on the local security policy. File permissions, registry settings, password usage, user rights, and other issues associated with Windows 2000 security have a direct impact on Certificate Services security. Install the High Encryption pack that comes as an optional install with the Windows 2000 software. This package provides the capability to use strong cryptography by allowing certificates to be created using large cryptographic key lengths.

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).

In a nutshell, public key (or asymmetric) cryptography is based on a "key pair". One key in the pair is called the "public" key, which can be published in a public directory where any user can access it. The other is the "private" key, known only to and kept secure by the user for whom it was created. Although the two keys are mathematically related, the private key cannot be determined from the public key. Encryption and signing are two operations associated with public key cryptography. Traffic encrypted using a public key can only be decrypted using the associated private key and vice versa. Signing can be used as a way to verify the source of a piece of data. Signing does not protect the data from being viewed by anyone who has access to the sender's public key. More on the signing process follows. In public key cryptography, security is provided through the protection of the private keys.

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

**Authentication**: a security mechanism that provides assurance that a message was actually sent by the person indicated.

**Non-repudiation**: a security mechanism that provides assurance that a sender of a message cannot later deny having sent it.

**Data Integrity**: a security mechanism that provides assurance that a message has not been modified prior to reaching its destination.

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 and 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, the slightest change to the original 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”. An example of RSA’s implementation follows:

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 a 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 was not changed during transit (providing data integrity).In the previous 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. This validation occurs for each intermediate CA’s certificate until a trusted issuing root CA’s certificate is reached.

## PKI and Certificate Chaining

A Public Key Infrastructure (PKI) uses public key cryptography to create an environment where individuals can communicate and share information in a secure manner by establishing a trust between themselves and those with whom they wish to communicate. In order for this trust to be established, certificates must chain to a root CA that is trusted by the inquiring entity. 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 typical PKI, several layers of CAs will exist. A CA has two primary functions: issue certificates to subordinate CAs or end-entities (such as users and computers) and the revocation of those issued certificates when they become invalid. The CA accomplishes this by placing the invalid certificate(s) on a certificate revocation list (CRL) and makes the list available to all entities that are configured to trust the validity of the revoked certificate.

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 certificate. Authority Information Access (AIA) locations, published in certificates by the 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. By verifying the validity of all intermediate CAs and the root CA in a certificate chain, trust in the certificate can be established.

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. In small intranets, the middle layer of subordinate CAs can be eliminated within the hierarchy as long as the root CA is protected as described in this document. 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. If it is feasible to do so within your environment, maintaining your own stand-alone root CA allows for more control over its security and the chain of trust established to it from an end-entity certificate.
- Are the services required for a Windows 2000 domain (intranet) only? If so, implement the enterprise policy module (discussed on page 10) on all subordinate CAs.
- Are the services required to support users and computers outside of a Windows 2000 domain? A stand-alone policy module (discussed on page 11) is required for a CA that supports an environment that is not entirely Windows 2000.
- How many subordinate CAs are required? At least a three-tier hierarchy is recommended; however, in small intranets, a two-tier hierarchy may be implemented as long as the CAs are protected in the same way as the Domain Controllers. If you are implementing a hierarchy to service a large number of users, ensure requests will be processed in a timely fashion by having more than one CA capable of handling requests within your environment.

**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 that hardware modules be used 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.
- 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**)

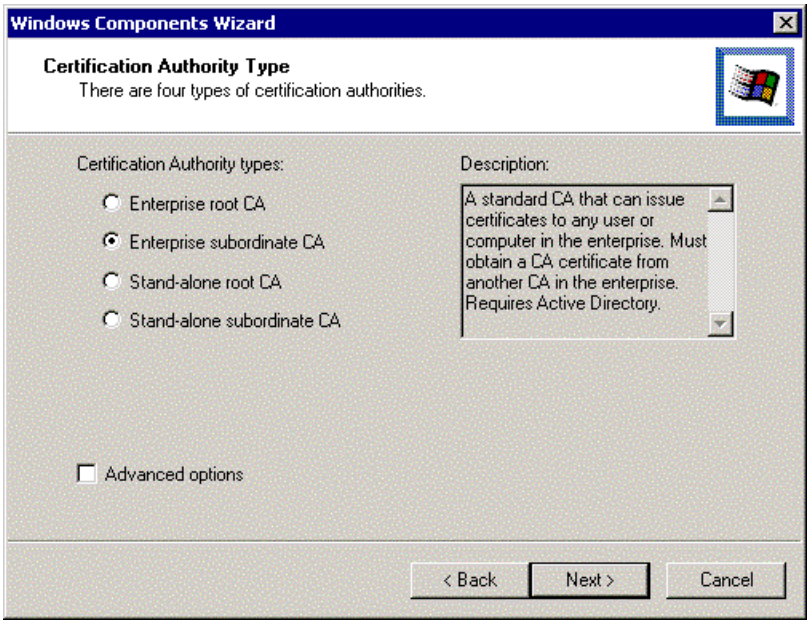


**Figure 1 Choosing Enterprise Subordinate CA for Certification Authority Type**

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**)

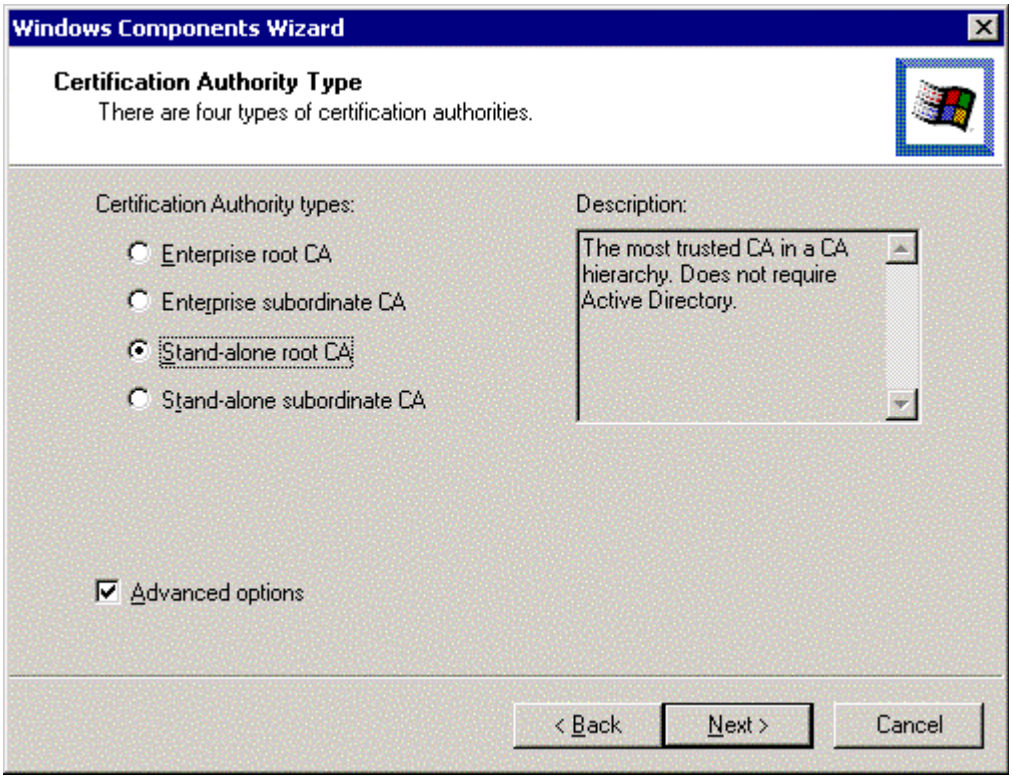


**Figure 2 Choosing Stand-alone Root CA for Certification Authority Type**

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 (this option cannot be configured for an enterprise CA). 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. Make sure the CRL Distribution Points (CDPs) are correct following a CA install. 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. It is extremely difficult for a stand-alone CA to provide 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. The recommended hierarchy is this mixed implementation. 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 allows it to safely revoke any compromised subordinate CA on the network.

### 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. Although this is not the recommended configuration for a root CA, security-relevant information pertaining to an enterprise root CA installation will be discussed since it is a Certificate Services option. Configure an enterprise root CA 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

As stated previously, this is not the recommended policy option for a root CA. If possible, configure your PKI with a stand-alone root CA and a mix of enterprise and stand-alone subordinate CAs to suit your security policy needs.

*(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.
- Select the **Advanced options** check box to specify the options listed in **Table 3**.

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

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

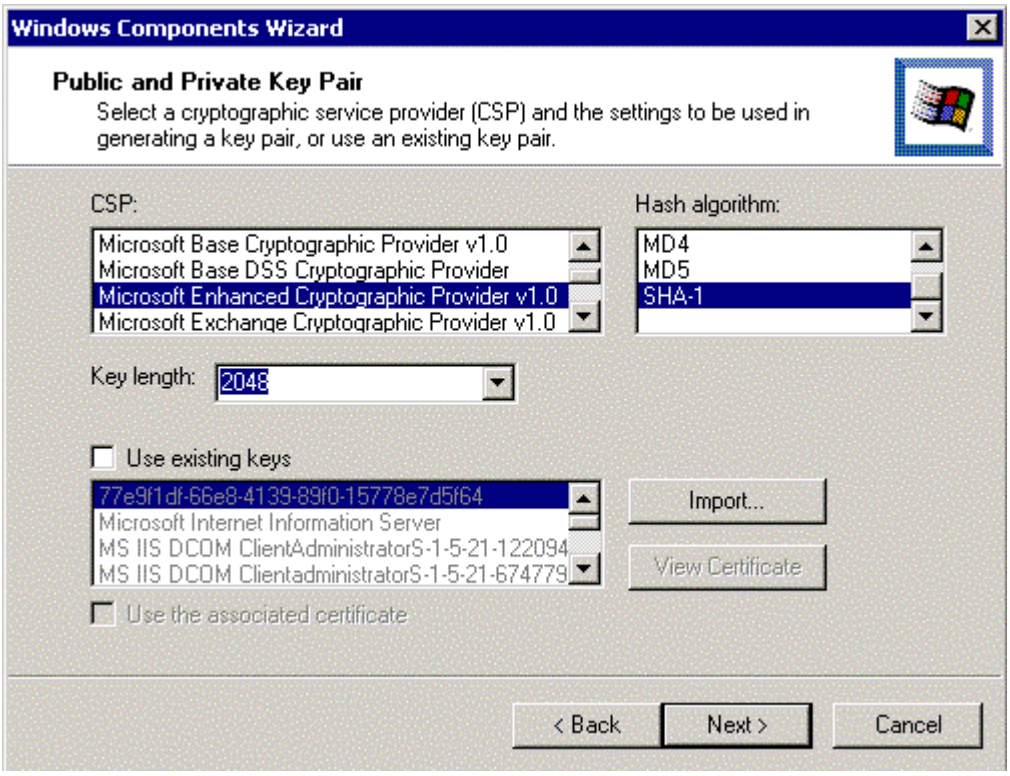


**Figure 3 Enterprise Root CA - Advanced Options**

- 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**)

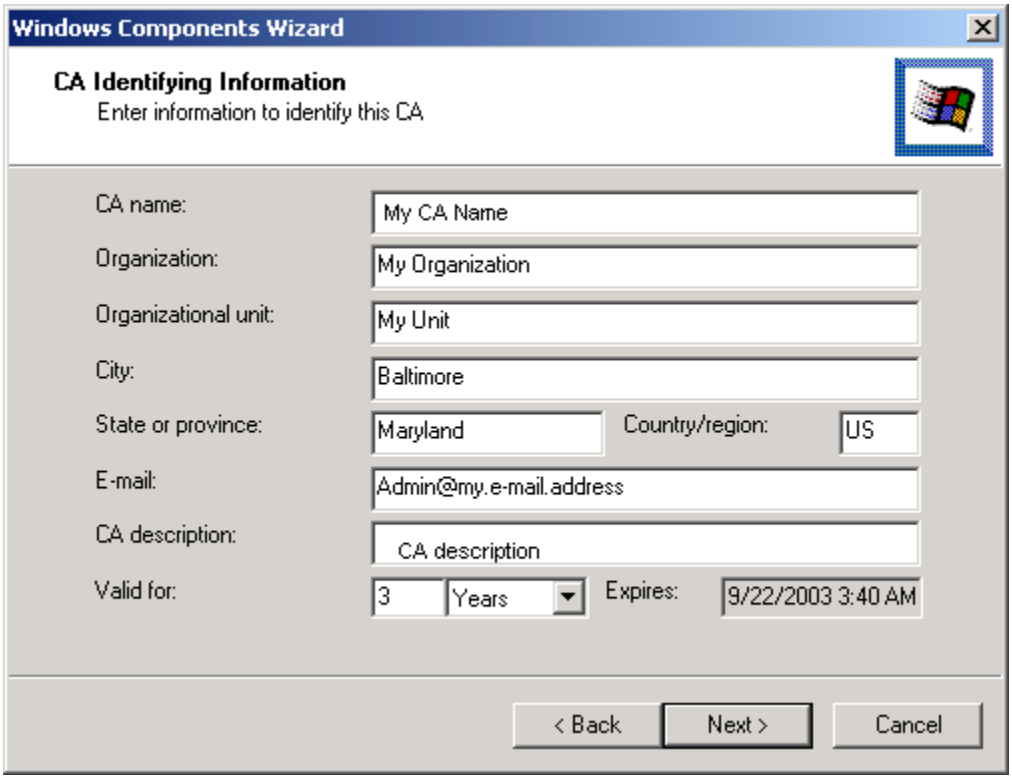


**Figure 4 Enterprise Root CA - Identification Information**

- In **Validity duration**, specify the validity duration for the root CA. Click **Next**. The validity duration chosen for the CA will determine when the CA "expires." Recommended settings are 3 to 5 years.
- Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**. (See **Figure 5**)

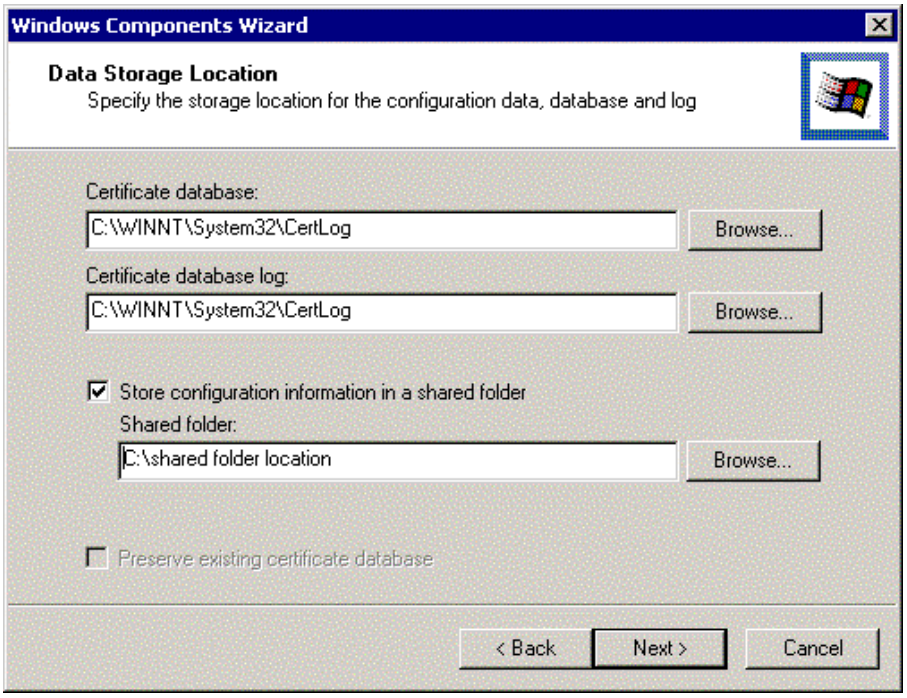


**Figure 5 Enterprise Root CA - Data Storage Location**

**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

A Stand-alone policy module is generally selected if a CA will be used to issue certificates to entities outside of an 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 placing the root CA behind a door with dual combo locks. This would then require two individuals in order to gain physical access to the root CA. These extra security measures 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 installing the root CA with access to Active Directory, log on to the system as a Domain Administrator. It is recommended the stand-alone root CA be offline, however, it can be removed from the network following the installation. This way the root CA's information can be loaded into Active Directory without manually inserting it or using the DSStore tool
- 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**.
- Select the **Advanced options** check box and apply the desired settings (refer to **Table 3** to determine the appropriate settings for these fields).

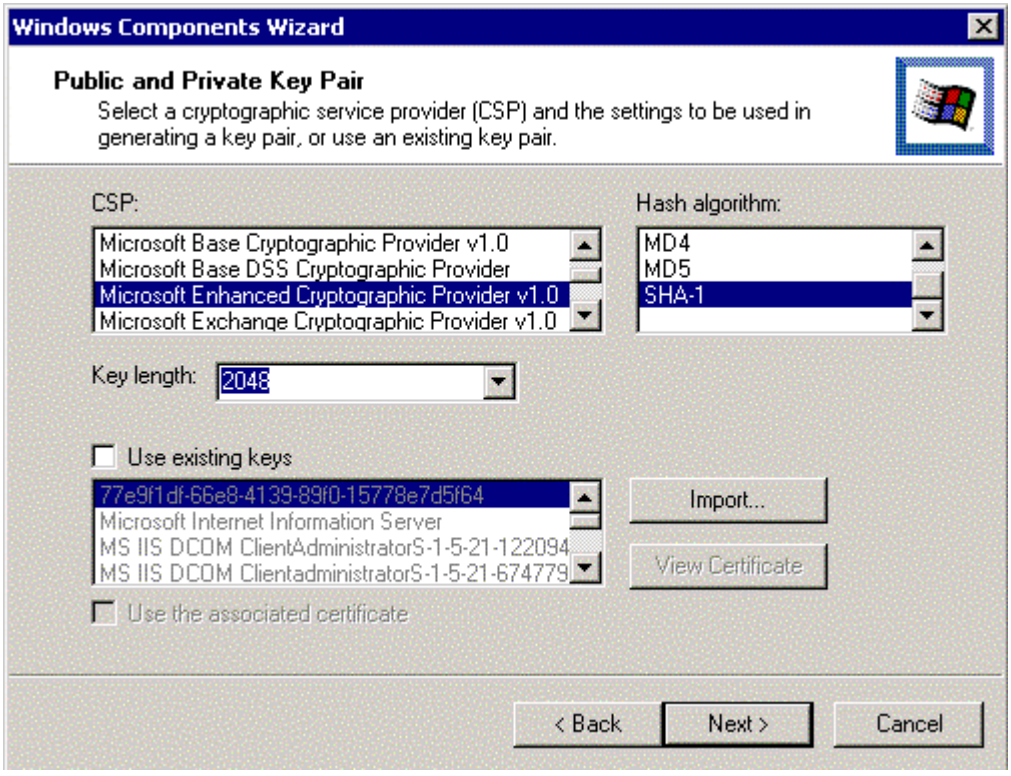


**Figure 6 Stand-alone Root CA – Advanced Options**

- 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.

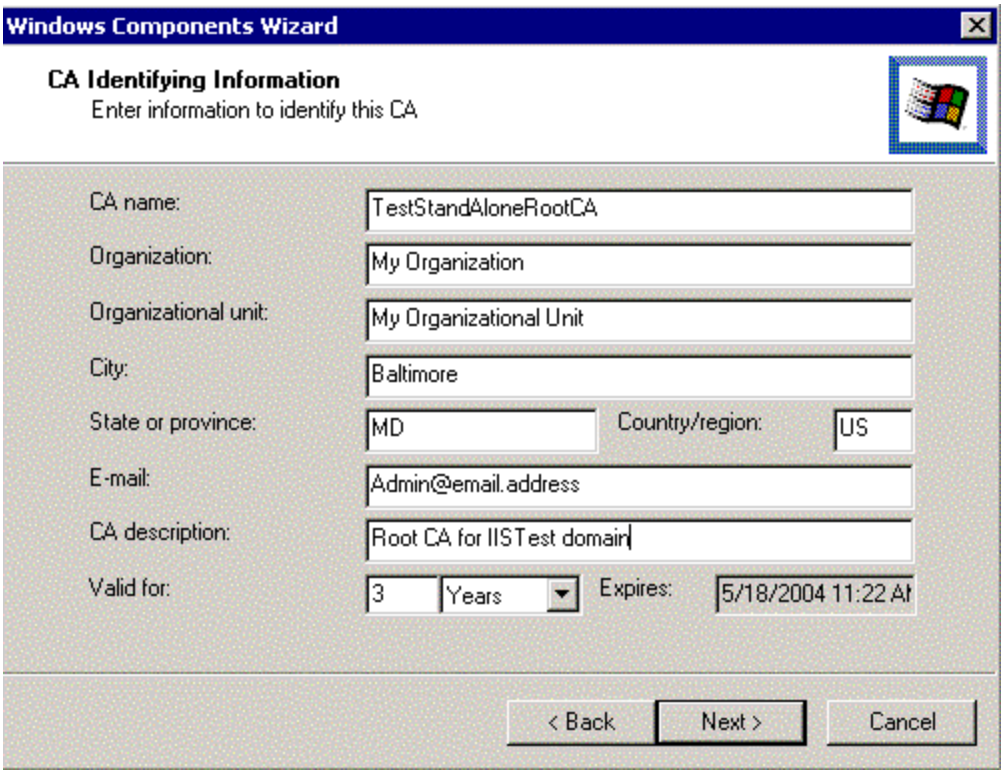


**Figure 7 Stand-alone Root CA - Identifying Information**

- In **Validity duration**, specify the validity duration for the root CA. Click **Next**. The validity duration chosen for the CA will determine when the CA "expires." Recommended setting is 3 to 5 years.

- Specify the storage locations of the certificate database, the certificate database log, and the shared folder. Click **Next**. If Active Directory is available for an online stand-alone root CA install and you have Write permission to Active Directory, then specifying the shared folder is optional; however, it is recommended.

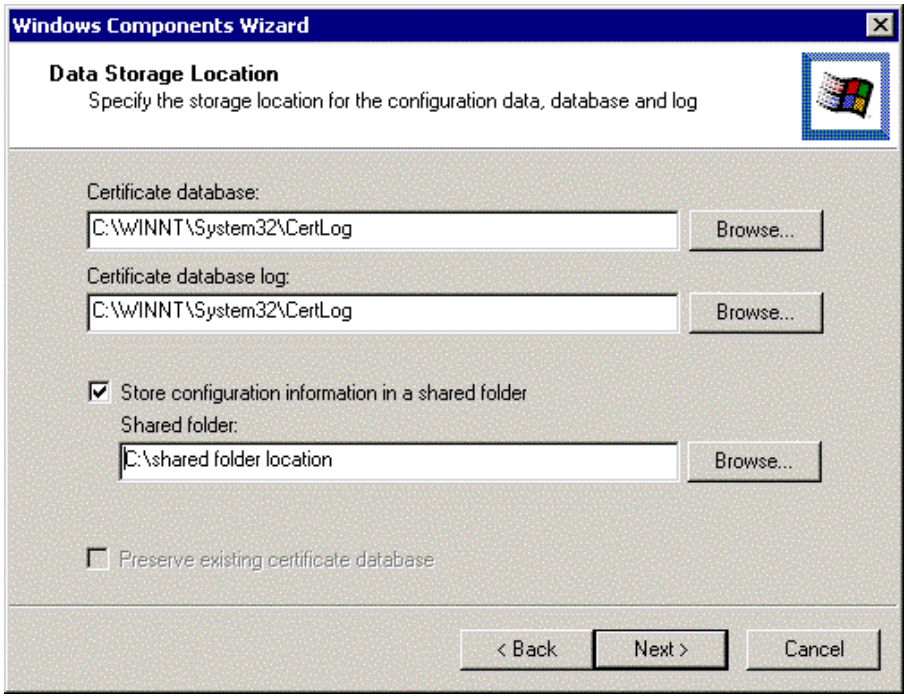


**Figure 8 Stand-alone Root CA – Data Storage Location**

- 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**.

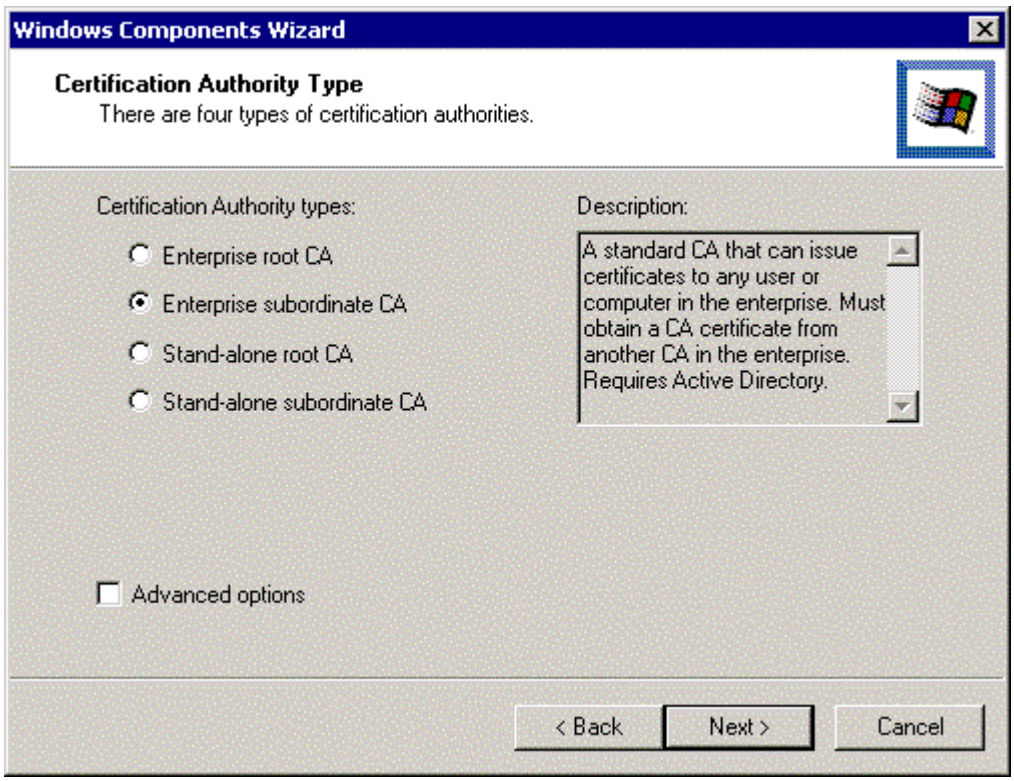


**Figure 9 Choosing Enterprise Subordinate CA**

- Select the **Advanced options** check box and apply the desired settings (refer to **Table 3** to determine the appropriate settings for the fields shown in **Figure 10**).

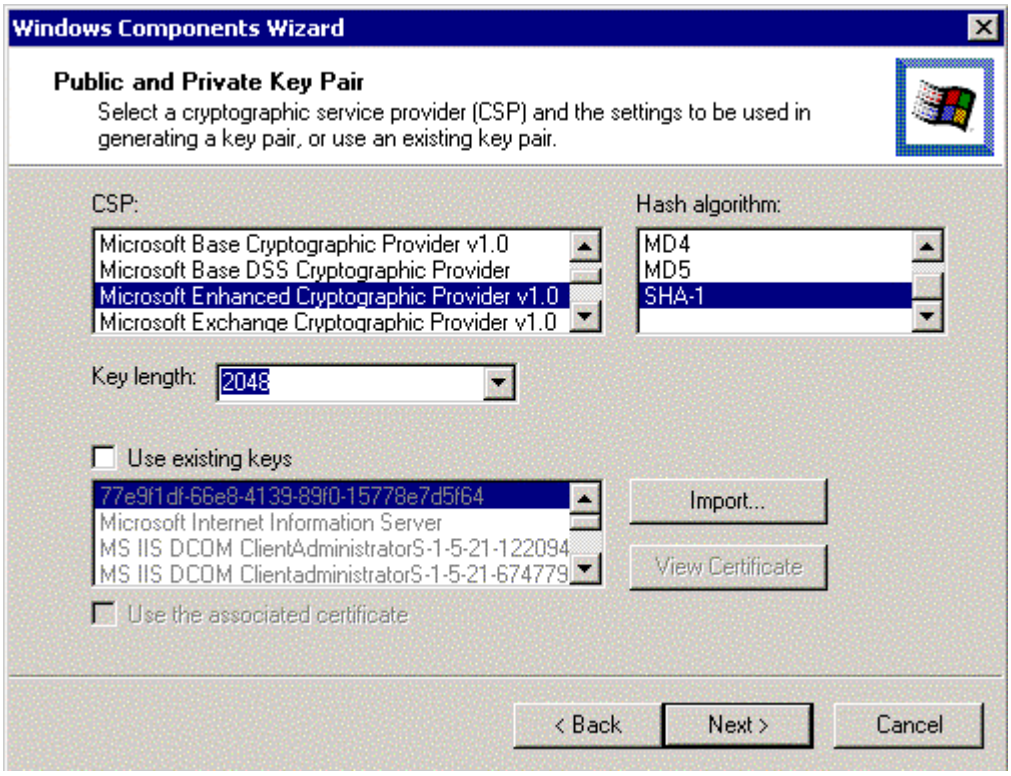


**Figure 10 Subordinate CA – Sample Dialog Box for "Advanced Options"**

- When you are finished, 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**.

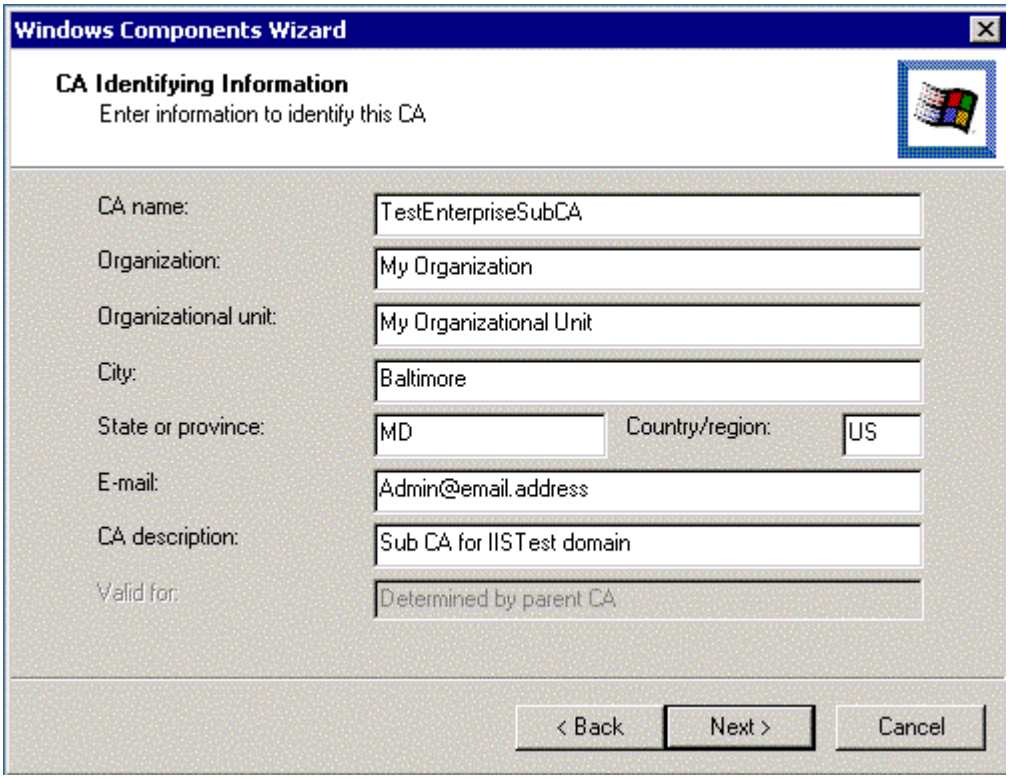


**Figure 11 Subordinate CA – Identifying Information**

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

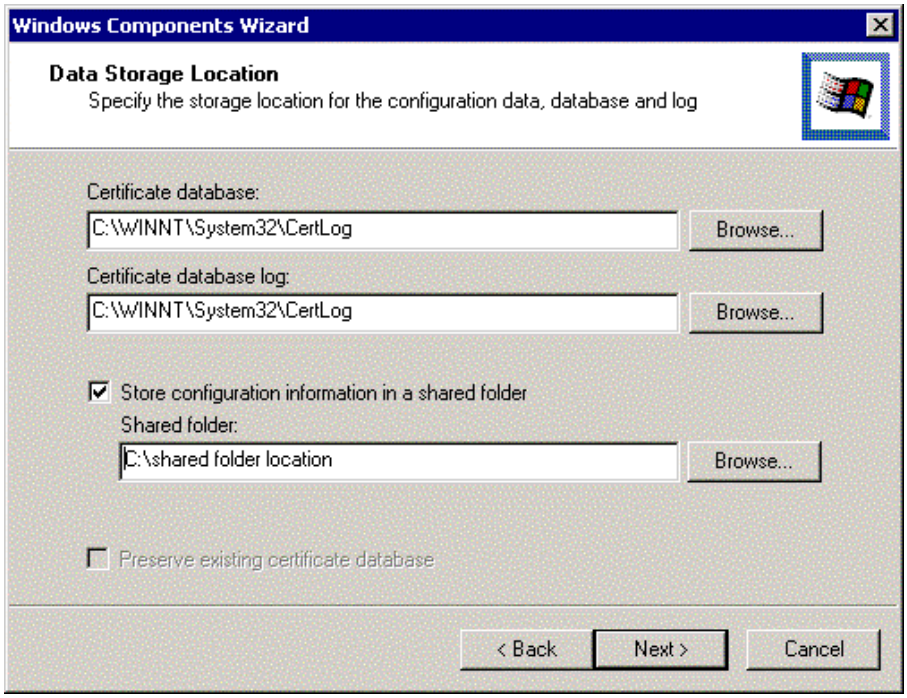


**Figure 12 Subordinate CA – Data Storage Location**

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 the 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 Microsoft Certificate Services 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 Microsoft Certificate Service 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 deliberately not been renewed 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.

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.

Since others rely on the root CA's certificate to form a certificate chain, and the life of a root CA will most likely outlast its validity period, the root CA must be able to renew its certificate. Two options are available when renewing certificates: renew using existing signing keys and renew using new signing keys. The most secure approach is to renew certificates using NEW keys. There are circumstances where it is appropriate to use existing keys. For example, if a CA must be restored following a hardware failure or if the CA must be restored following a relocation. If the CA certificate has to be renewed using existing keys, ensure the CAs are offline, physically secured and a two-person control policy is implemented for accessing the CA.

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.

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. However, 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 the longest key length available that is compatible with the site's configuration. 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 with a new key pair and extended validity period of 3-5 years.

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 CDP 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.

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. Almost always **Yes** will be the selected option. (See **Figure 13**)
- Certificate Services will then restart with a new validity period for the renewed CA certificate.

If the CA certificate being renewed belongs to a subordinate CA, the request must be submitted to a parent CA. 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.**

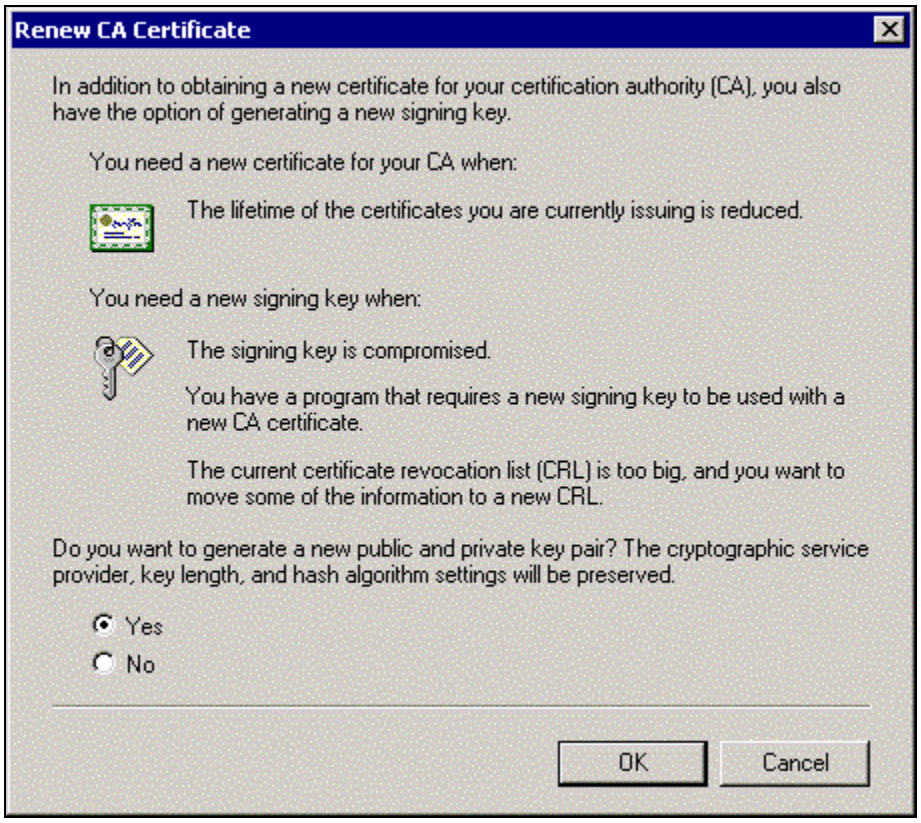


**Figure 13 Renewing a CA Certificate**

Chapter 2

# Managing Certificates Using the MMC



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

## Certificate Services Snap-Ins

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

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

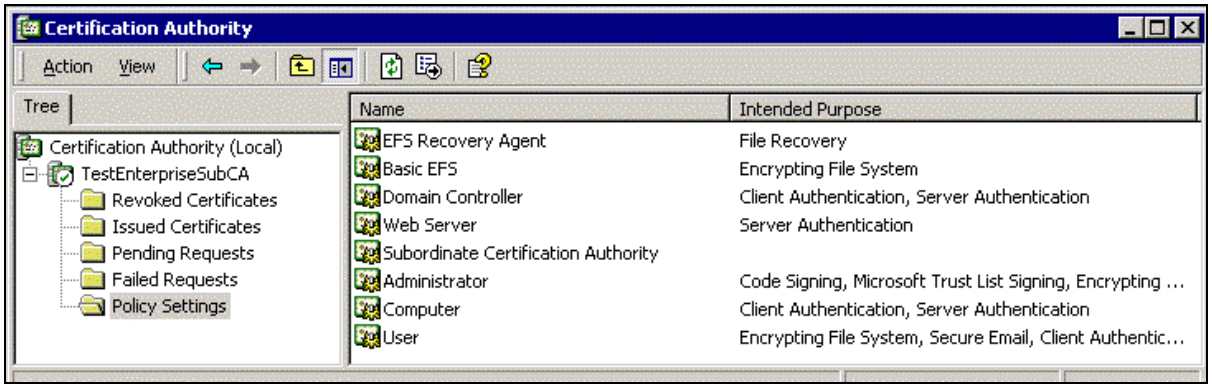


**Figure 14 Certification Authority Snap-In**

A snap-in extension is available for the Certification Authority snap-in (See **Figure 15**). The Certification Authority Policy Setting extension allows the administrator to select the types of certificates the CA will be permitted to issue.

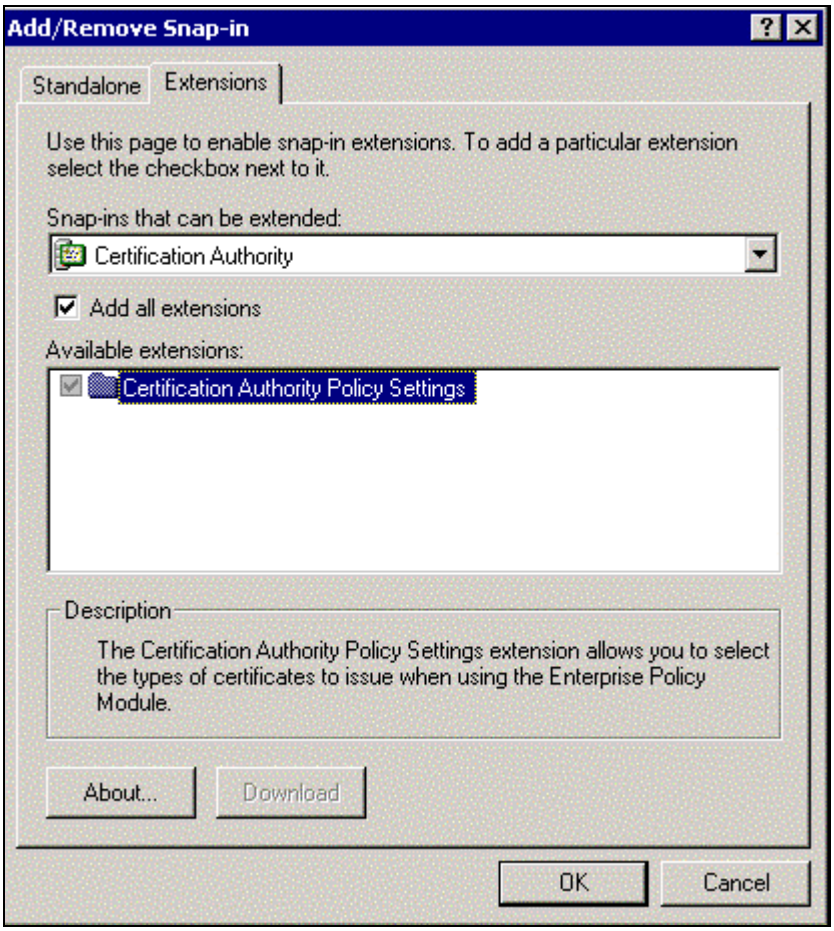


**Figure 15 Add/Remove Snap-in Extensions**

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 (See **Figure 16**). Select ONLY the certificate templates your CA is required to issue and click **OK.** The new template will then be displayed in the right pane of the Certification Authority window. This is where the administrator can control the types of certificates the CA will make available to requesting users. More information regarding certificate templates can be found in the Enterprise CA Templates section of this document.

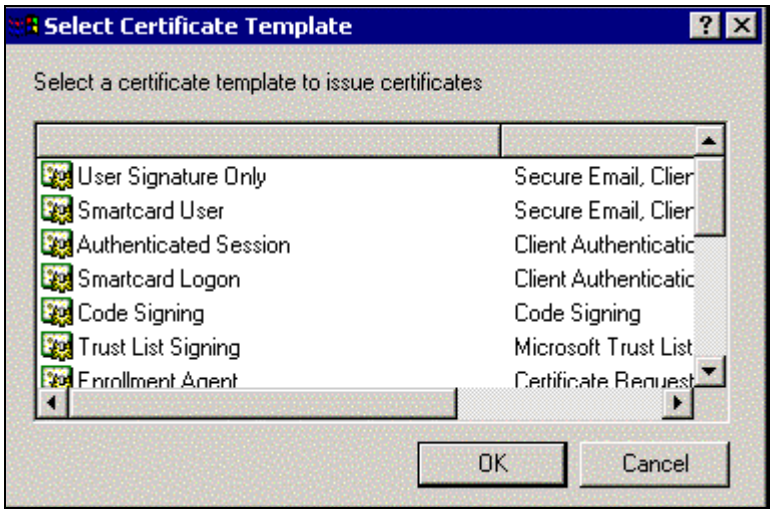


**Figure 16 Selecting Certificate Template**

It is very important 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. If a user other than an administrator is required to manage the CA, an administrator could grant this user the permission to manage, thereby allowing control of the CA to the user without granting administrative privileges over the entire server.

**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.**

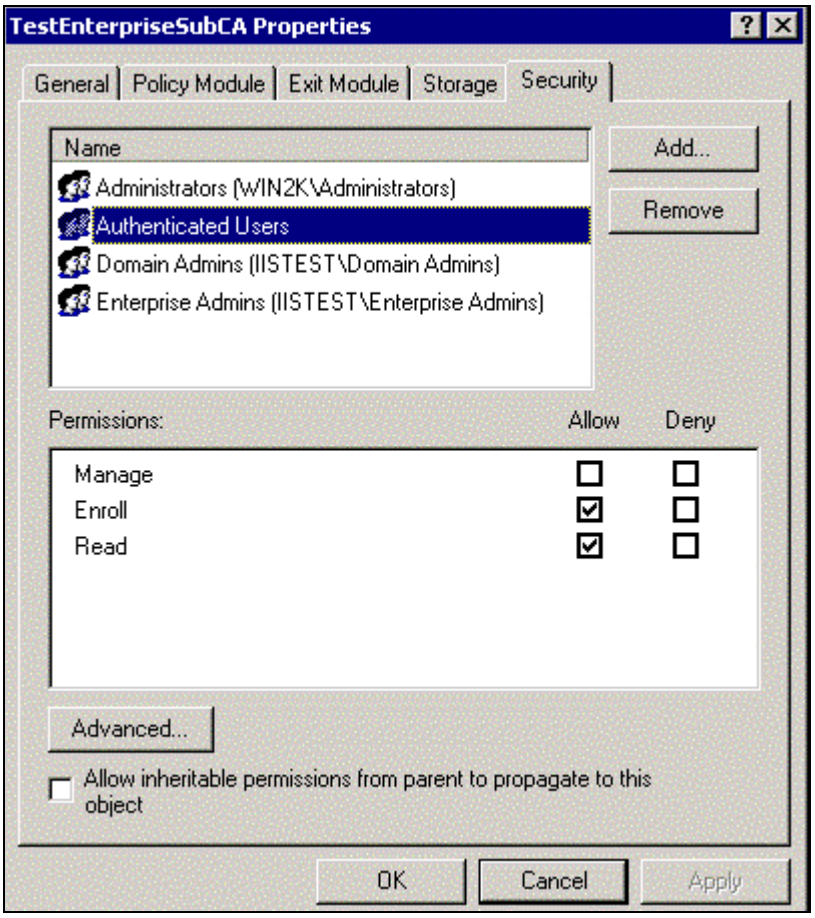


**Figure 17 Setting Security Permissions for CA Control**

## Certificate Store and Active Directory

Certificates, CRLs, and certificate trust lists (CTLs) 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 (or third party 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 tool. In this way, root certificates can be distributed to all computers in the forest. Active Directory is used as a certificate store by 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.

The DSStore tool is an excellent tool for managing certificates in Active Directory. It can be used to perform the following: (More information on the use of this tool can be found in the white paper “Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon”).

1. Manage enterprise roots in Active Directory
2. Check validity of Domain Controller and smart card certificates
3. List information about CAs, a machine’s certificates, and machine objects
4. Add non-windows 2000 CAs or offline CAs to Windows 2000 PKI
5. Troubleshoot certificate chains

The DSStore tool and a certificate trust list (CTL) created through group policy should be used to manage certificates within a PKI environment. However, administrators can also manage certificates on individual machines by performing the following steps.

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**).

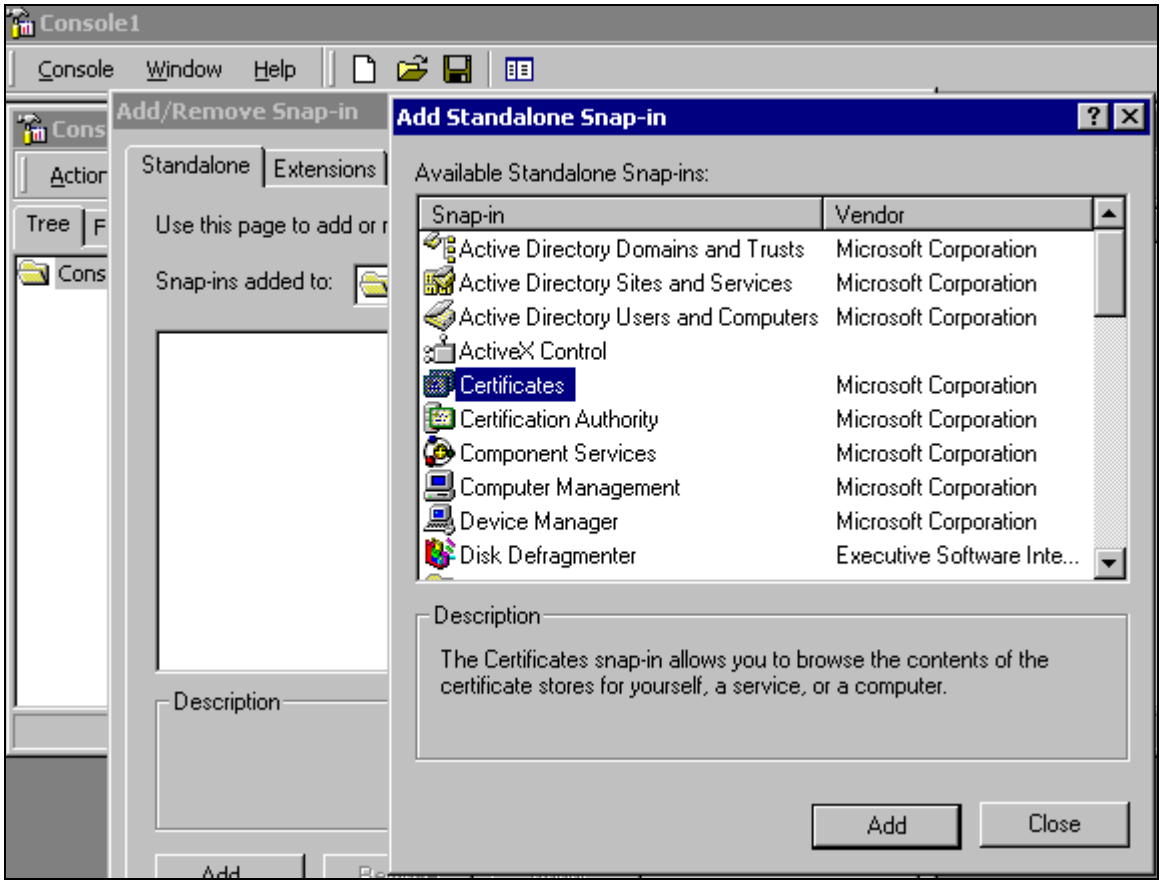


**Figure 18 Adding Certificates Snap-in**

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.

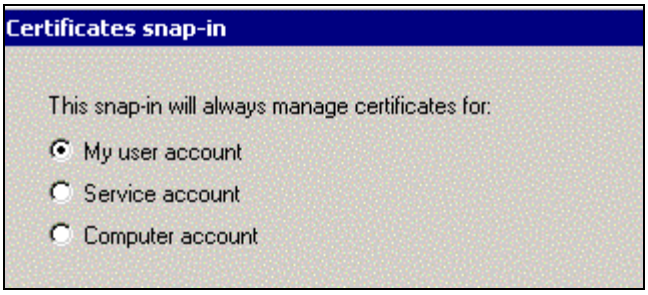


**Figure 19 Selecting Account for Certificate Management**

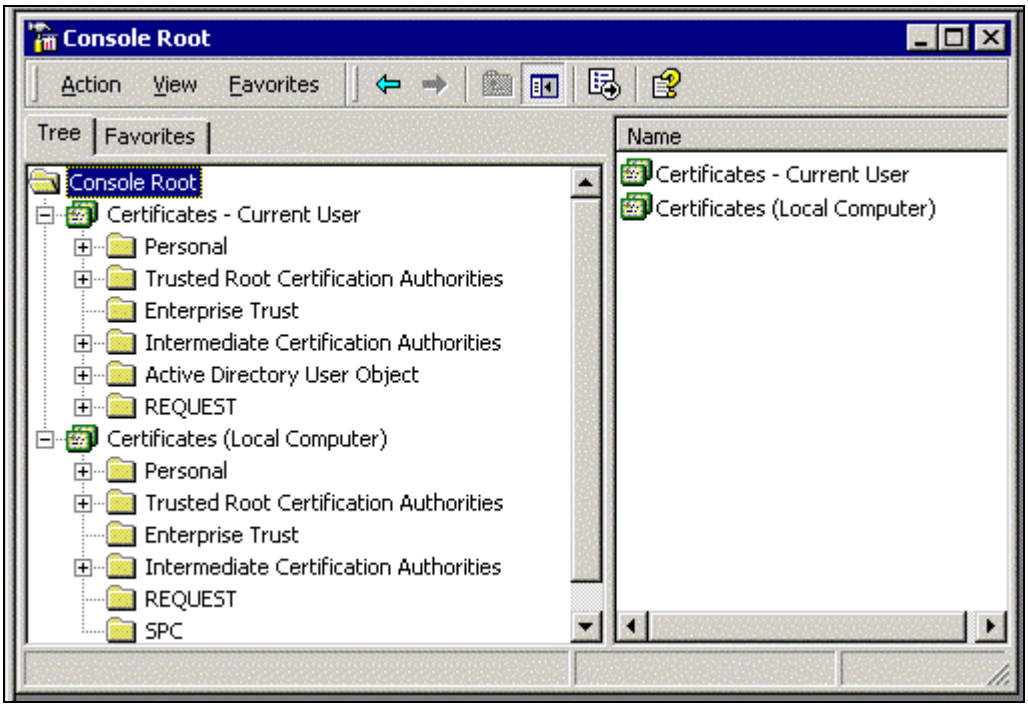


**Figure 20 Creating MMC Snap-ins**

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**).

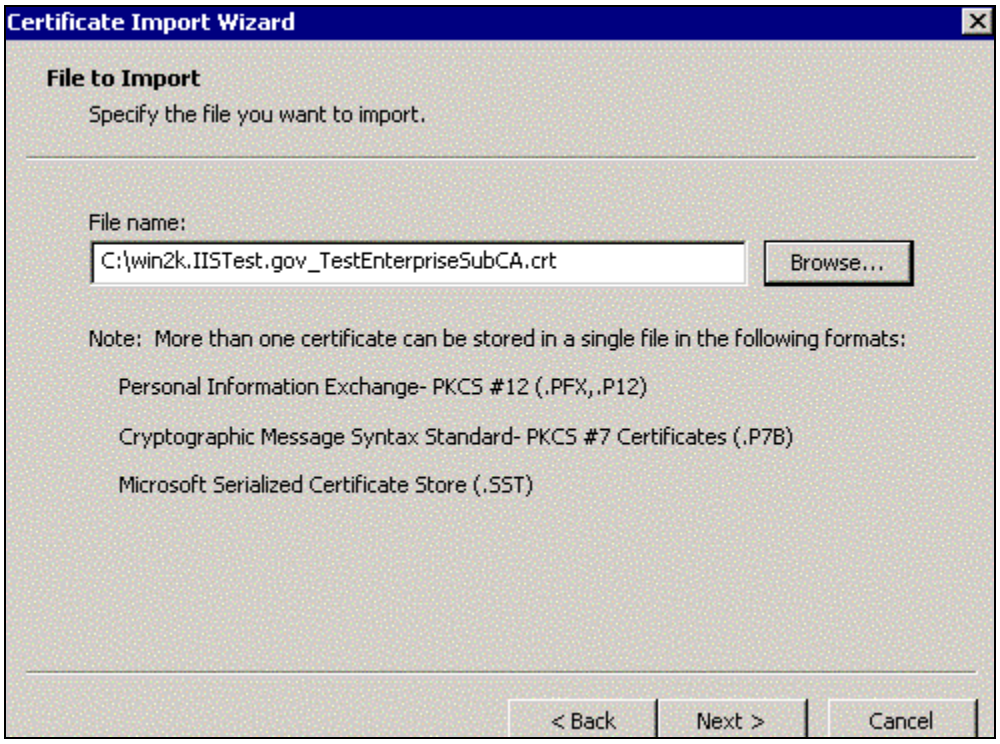


**Figure 21 Certificate Import Wizard - Selecting File to Import**

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

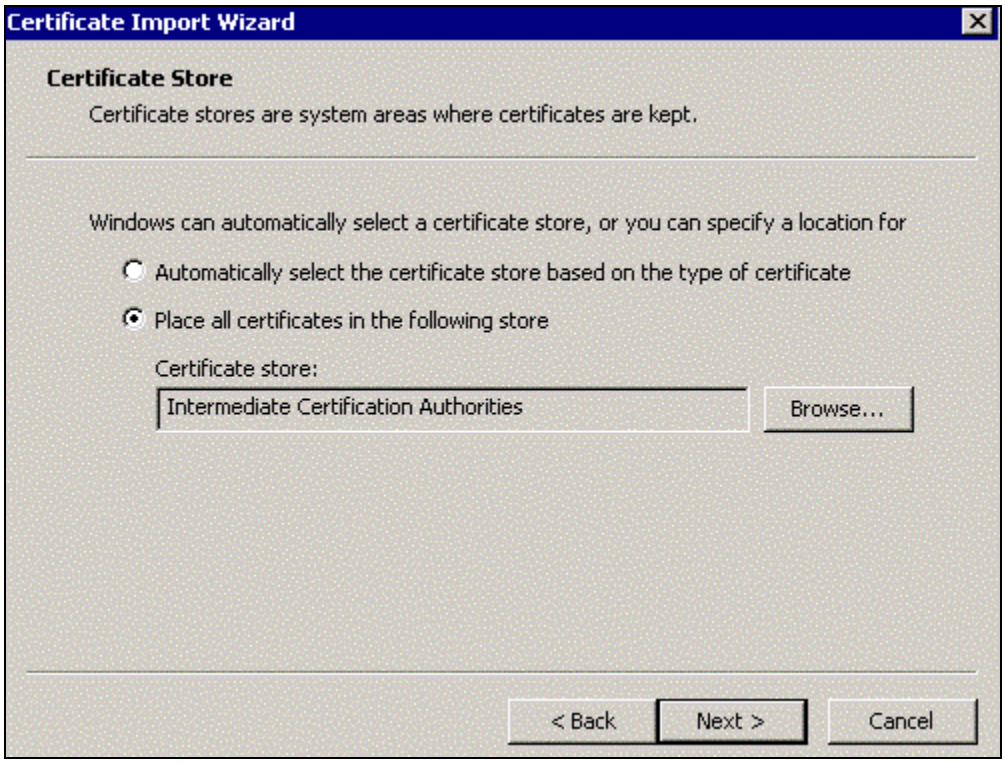


**Figure 22 Certificate Import Wizard – Selecting Certificate Store**

- In the Trusted Root Certification Authorities and Intermediate Certification Authorities stores, many CA certificates are installed by default. It is important to delete all untrusted CAs, making sure only trusted CAs are listed in these certificate stores. (See **Figure 23**) The IEAK can be used to perform this task on clients within your domain. See Microsoft's website at www.microsoft.com/windows/ieak for more information on the Internet Explorer Administration Kit (IEAK).
- 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 examples of the certificate window's General, Details, and Certification Path tabs, respectively.

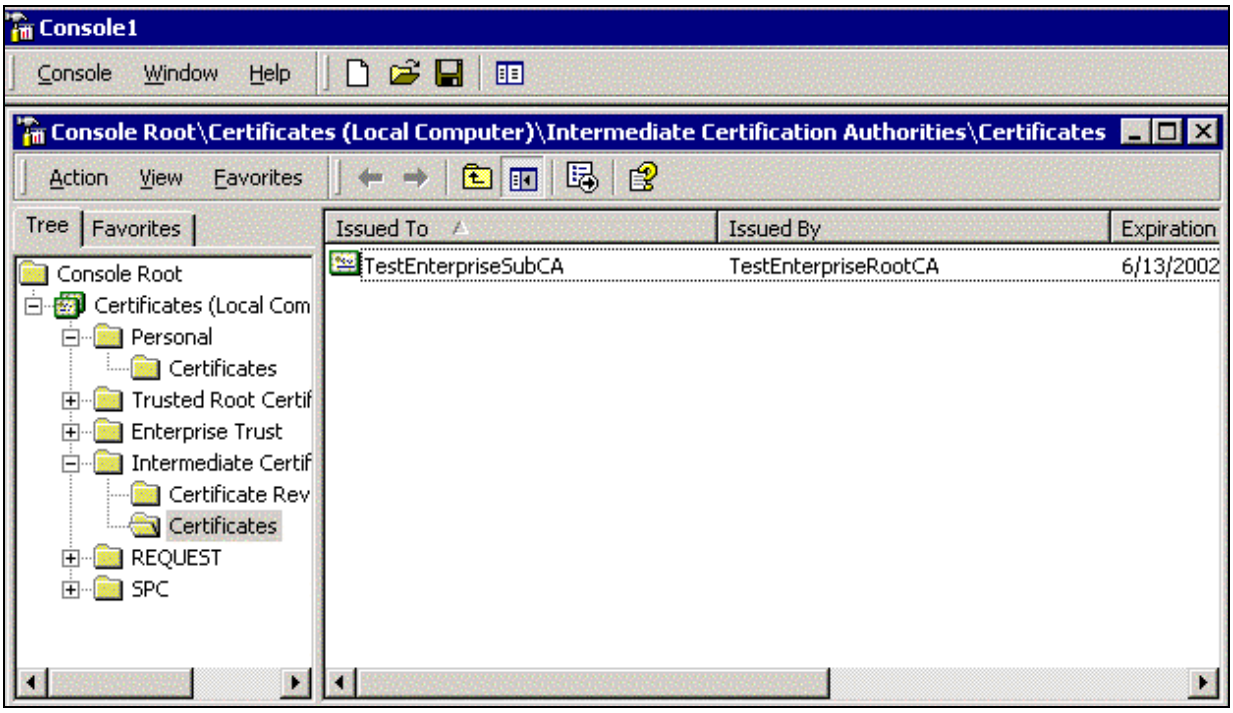


**Figure 23 Deleting Untrusted CA**

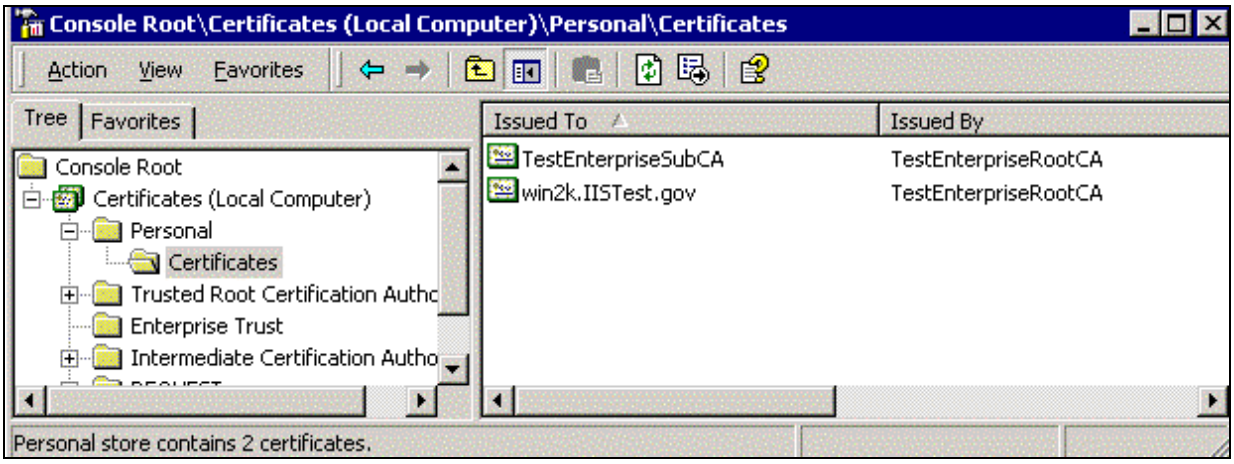


**Figure 24 Personal Certificates**

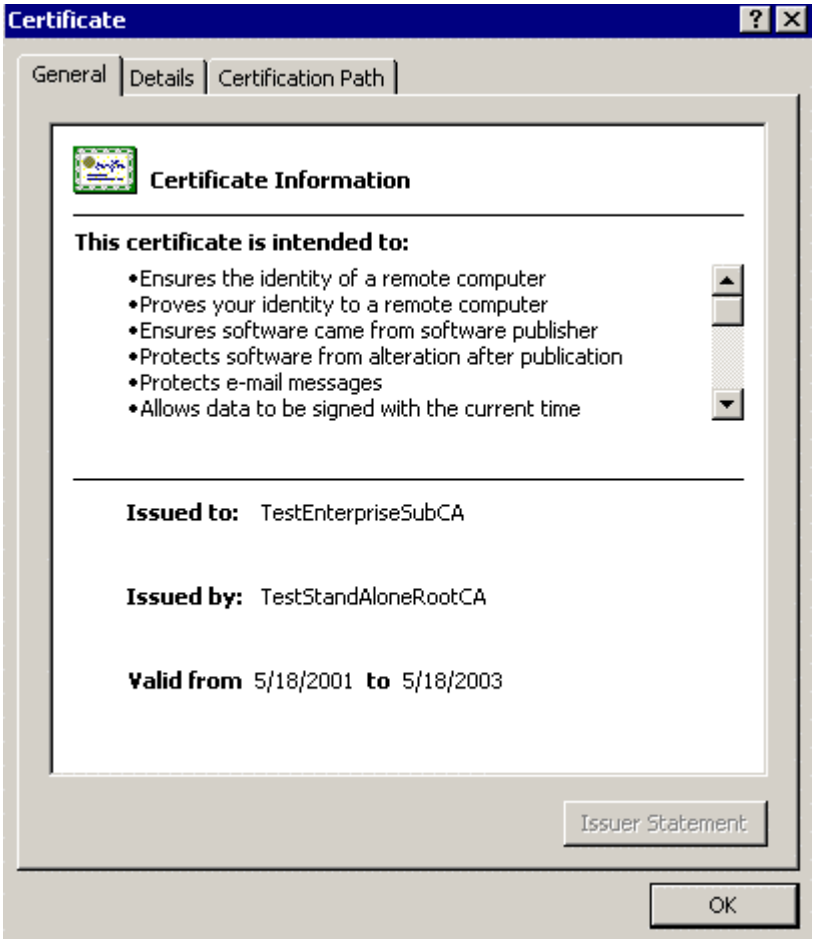


**Figure 25 Certificate – General Tab**

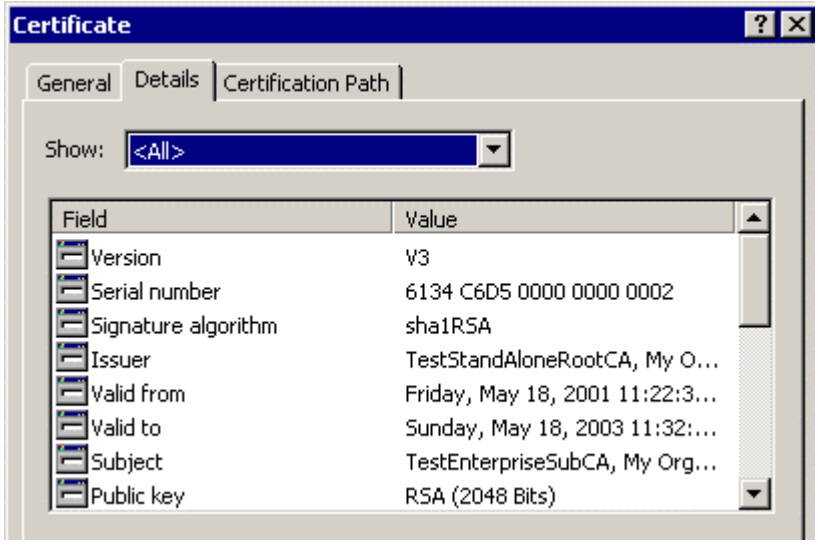


**Figure 26 Certificate – Details Tab**

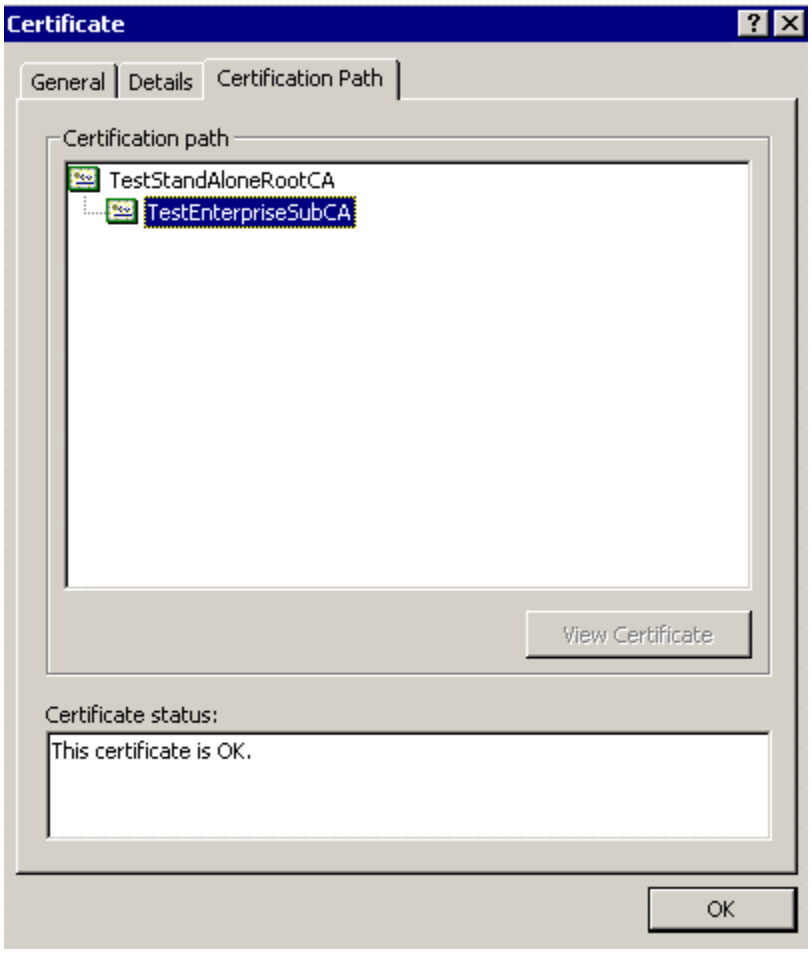


**Figure 27 Certificate – Certification Path Tab**

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

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 template, 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.**

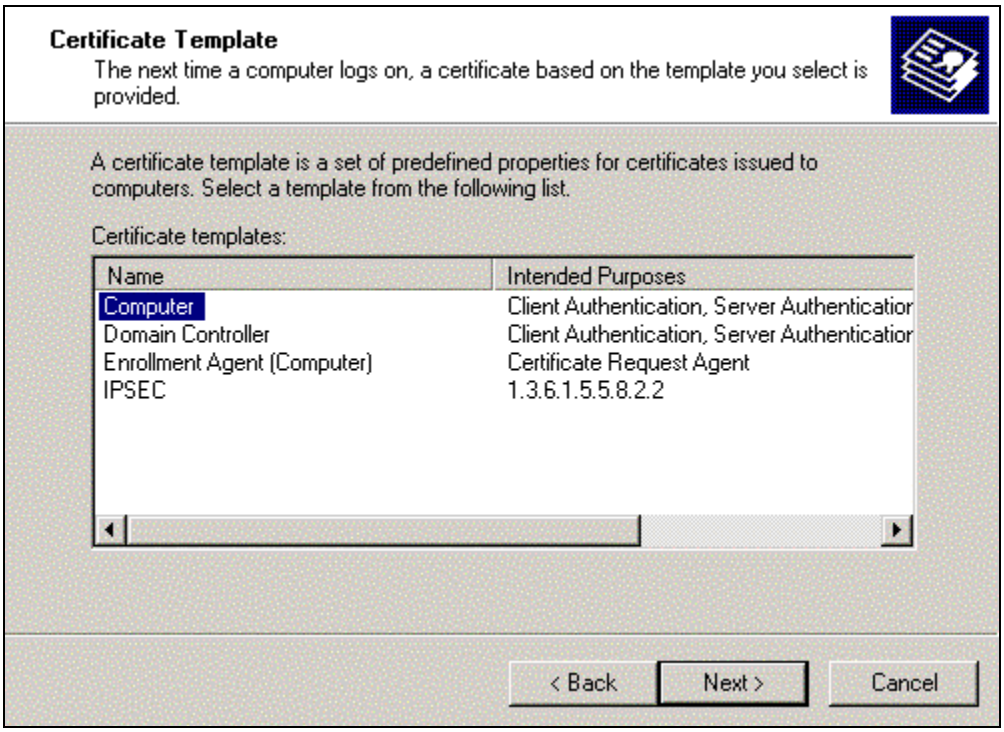


**Figure 28 Selecting a Certificate Template**

- 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**)
- 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 (**Figure 29)**, allowing the administrator to delegate the management of the CA templates to a specified group, i.e., Enterprise Admins, for example.

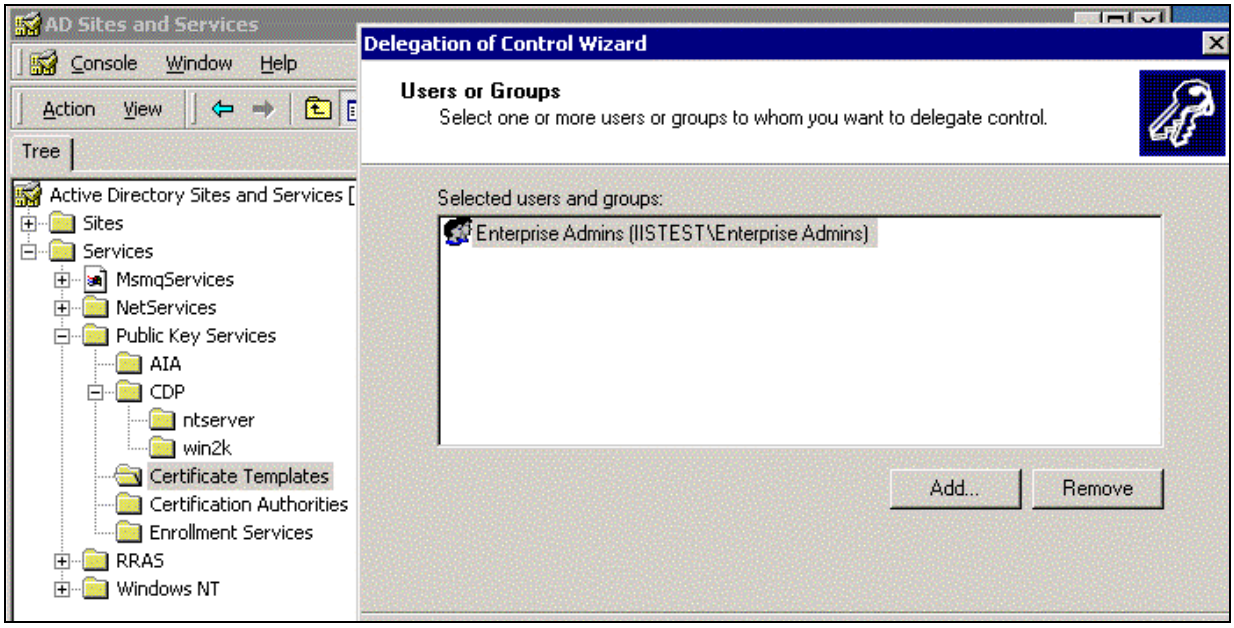


**Figure 29 Delegating Control of Templates**

**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 to accomplish the assigned task(s).

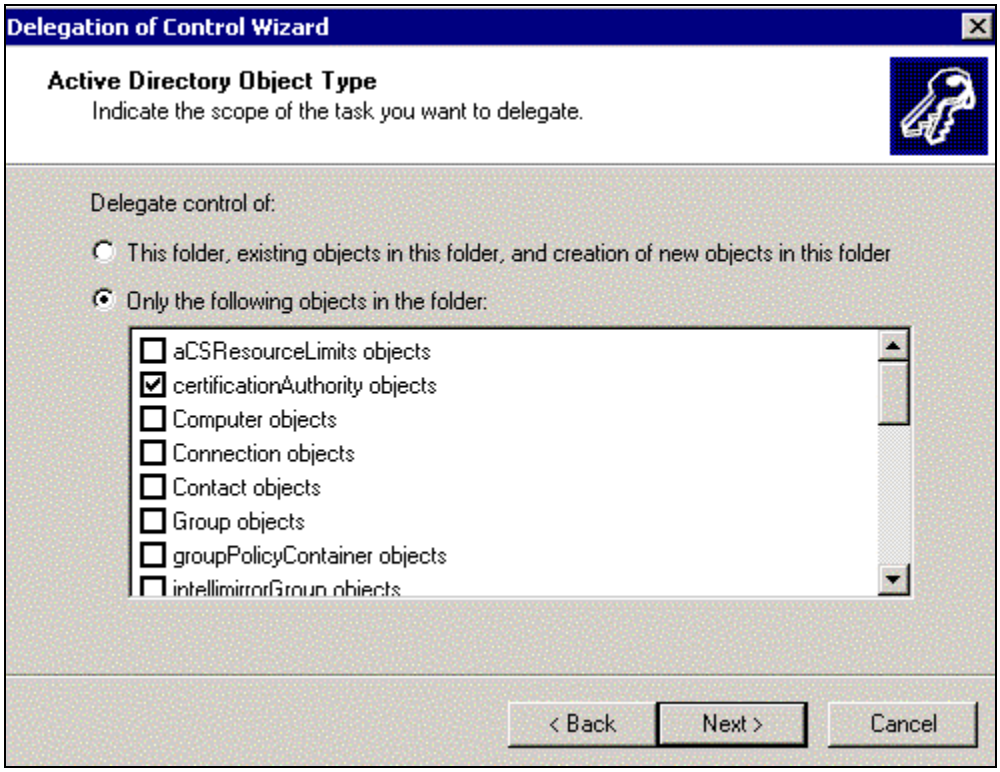


**Figure 30 Delegating Control of Objects**

## 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**)

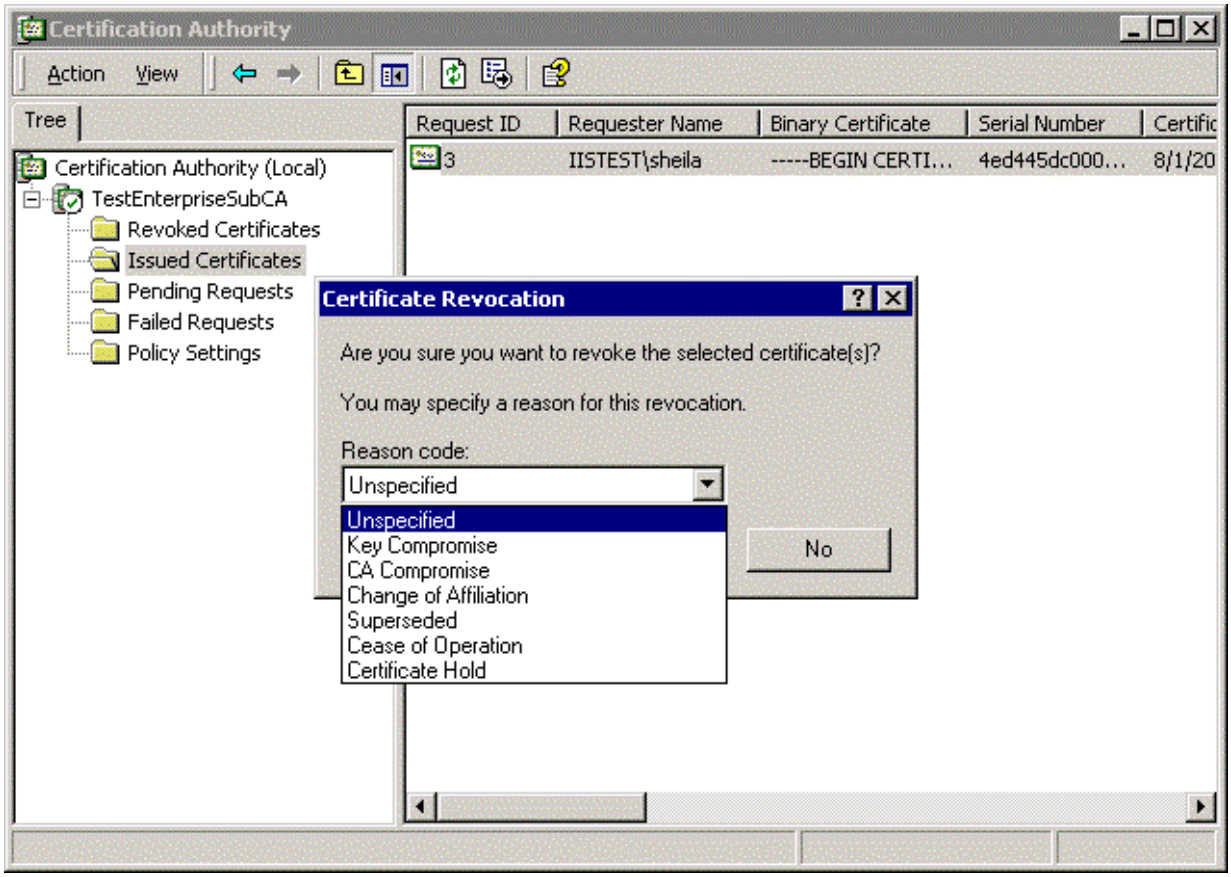


**Figure 31 Selecting A Reason for Certificate Revocation**

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. Certutil is a very useful utility. 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 CRL's publication period expiration so they may retrieve the new copy. In addition, 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**. The CRL Publishing Parameters window is displayed. 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 interval can be configured on the CRL Publishing Parameters window. 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. A CRL file is published in *Systemroot*\System32\Certsrv\Certenroll on the CA by default. Windows 2000 supports CRL publication to Active Directory. Clients can then obtain this information from Active Directory and cache it locally to use when verifying certificates. CRL distribution points can be configured by right clicking the CA in the MMC and selecting **properties**. Select **Configure** on the **Policy Module** tab and select the appropriate CRL Distribution Points (or add a new one) under the **X509 Extensions tab**.

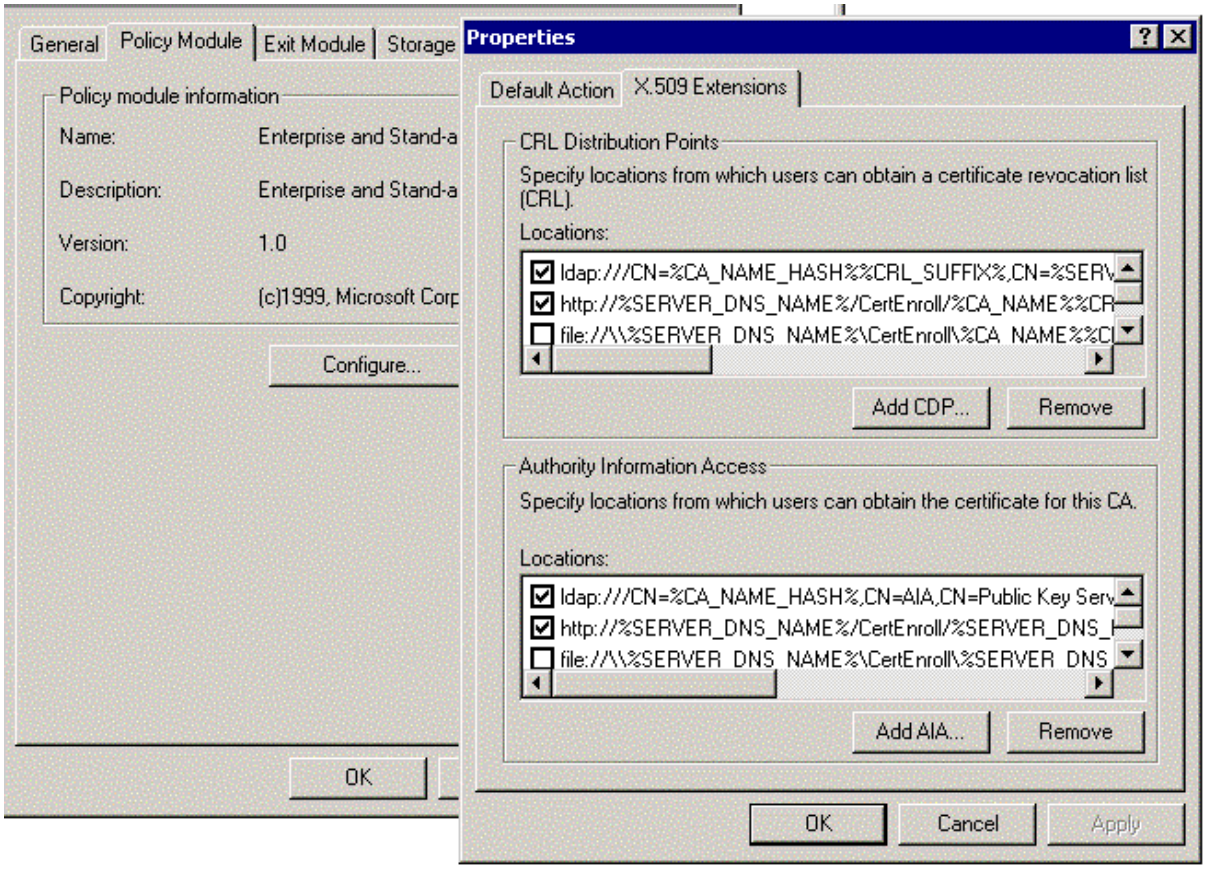


**Figure 32 Configuring CRL Distribution Points**

Chapter

3

# Additional Security Issues

## Antivirus 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 antivirus 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.
- Right-click **Issued Certificates** and select **View – Choose Columns** to change the order of the displayed columns and add/remove columns.
- Right-click **Issued Certificates** and select **View – filter**, to display certificates based on the selected filter criteria. **Figure 33** is an example of the data that can be set in the filter window.

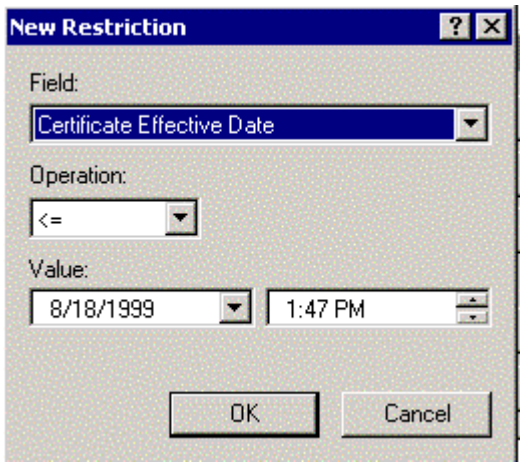


**Figure 33 Sample Data for Filtering Information**

## 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 combined with information in the Active Directory. This is all that is required from the user for a certificate to be issued.

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 selected certificate type, the user can 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 stand-alone 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.

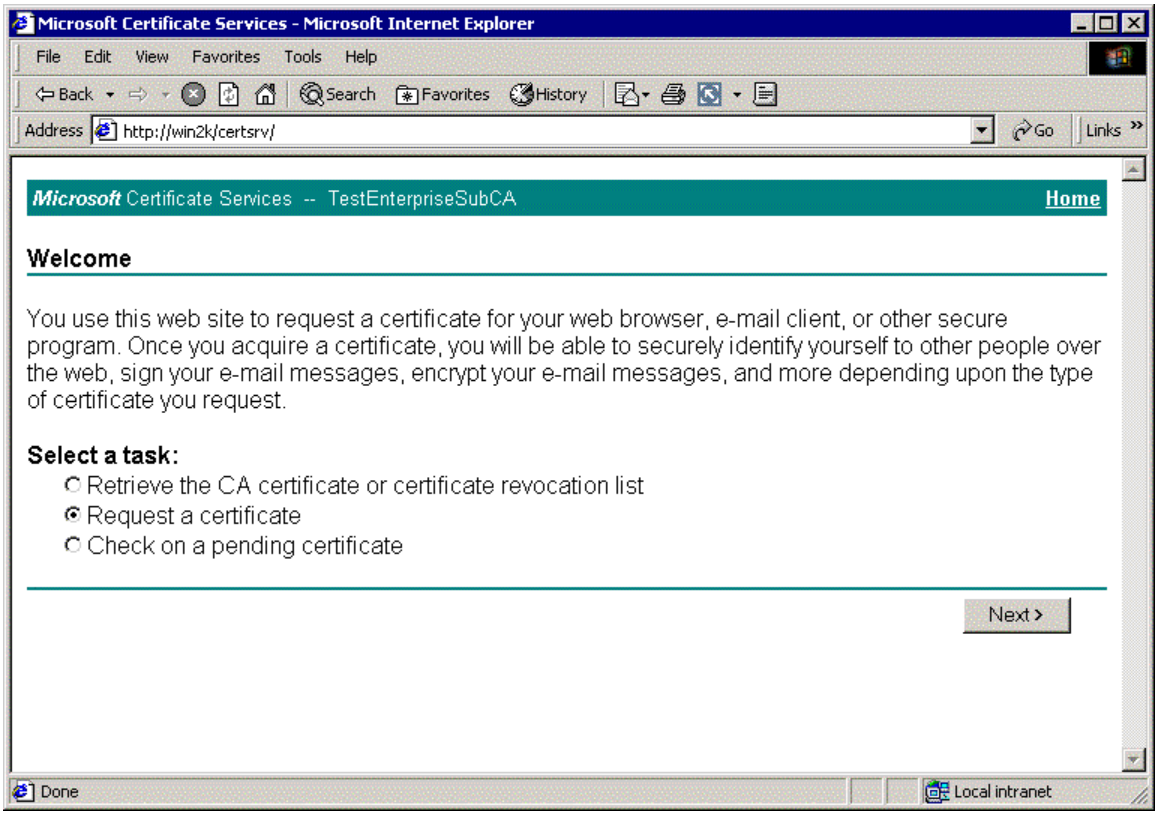


**Figure 34 Certificate Services Web Page**

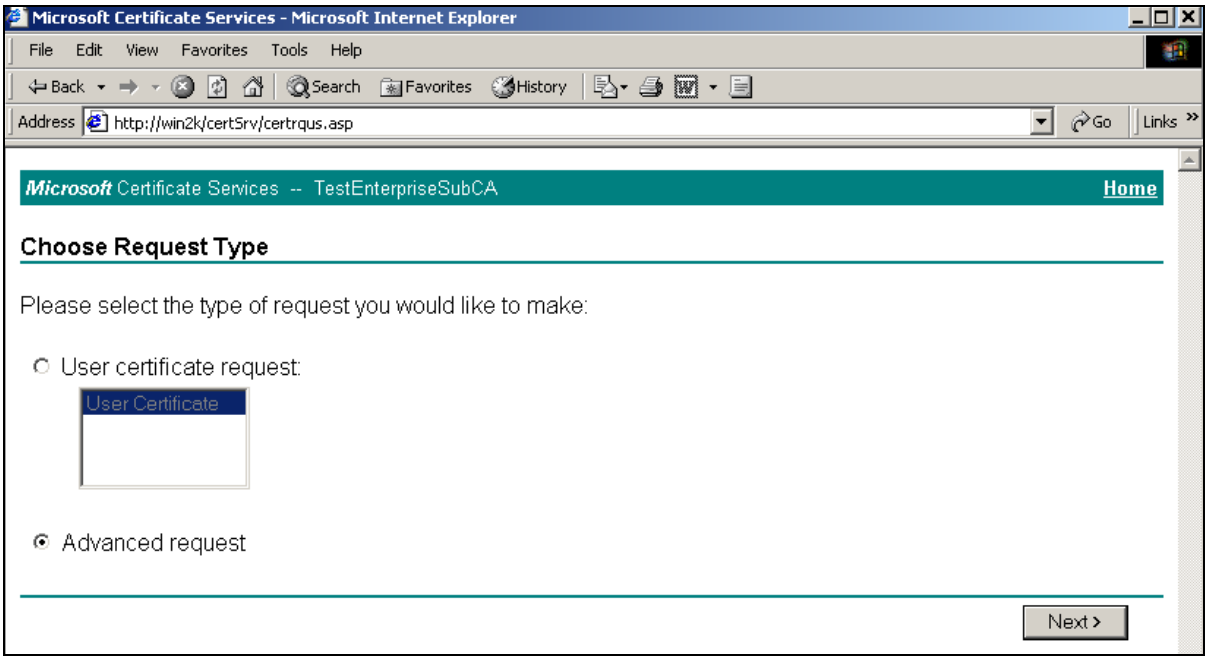


**Figure 35 Selecting Request Type**

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 36** and **Figure 37** are available when **Advanced request** is selected. When connecting to an enterprise CA, a **Certificate Template** drop-down box is available that lists templates for certificates the CA is permitted create. All other fields on the form are optional, however, as stated previously, it is recommended you choose the Microsoft Enhanced CSP to enable support for large key sizes. The CA, based on the template chosen, provides the information for these optional fields. There are two exceptions where the requester is required to complete all of the fields, when selecting the WebServer or IPSec Offline templates.

For standalone CAs, an **Extended Key** usage field is available in place of the template drop-down box. Choose the **Extended Key** usage that most closely fits the intended purpose of the certificate. All fields in the form are required to be filled in when requesting a certificate from a stand-alone CA.

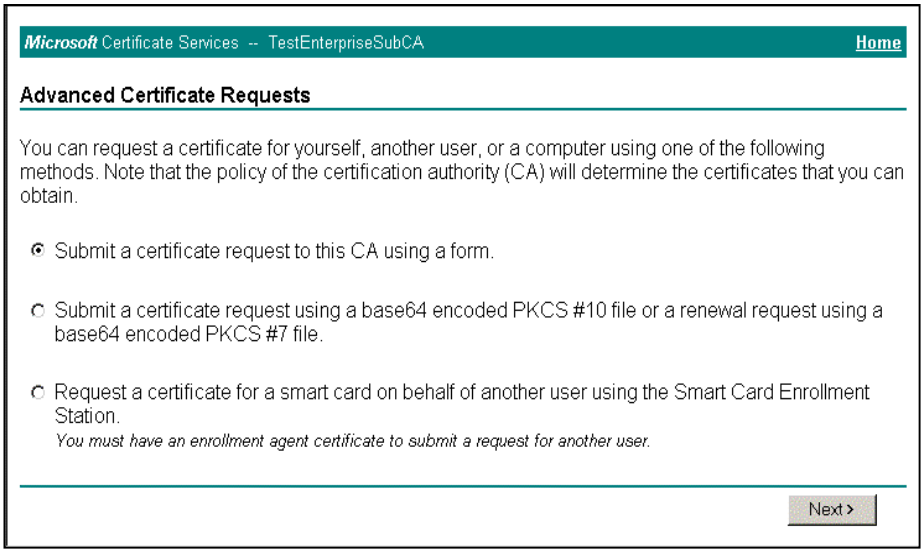


**Figure 36 Advanced Certificate Request Options**

Following is a description of some of the options available on the Advanced Certificate Request form (refer to **Table 3** to determine the appropriate settings for these fields):

- **CSP**: Change the default Cryptographic Service Provider (CSP) to the Microsoft Enhanced Cryptographic Provider v1.0 or the CSP that supports an implemented special hardware device (such as a smart card).
- **Key Size**: The key size will depend on your configuration. Choose the largest key size that is compatible with your configuration. Keep in mind, key sizes above 2048 take longer to generate and may not be compatible with older applications.
- **Key Usage**: Determines how the certificate will be used, i.e., for encryption, signing, or both.
- **Hash Algorithm**: The default setting is appropriate for most applications. Unless it is a requirement to change it, leave the default setting.

- **Use local machine store**. Choosing this option will place the keys and the certificate in a local machine store, making them available to system processes. Select this option if an IPSec certificate is requested.

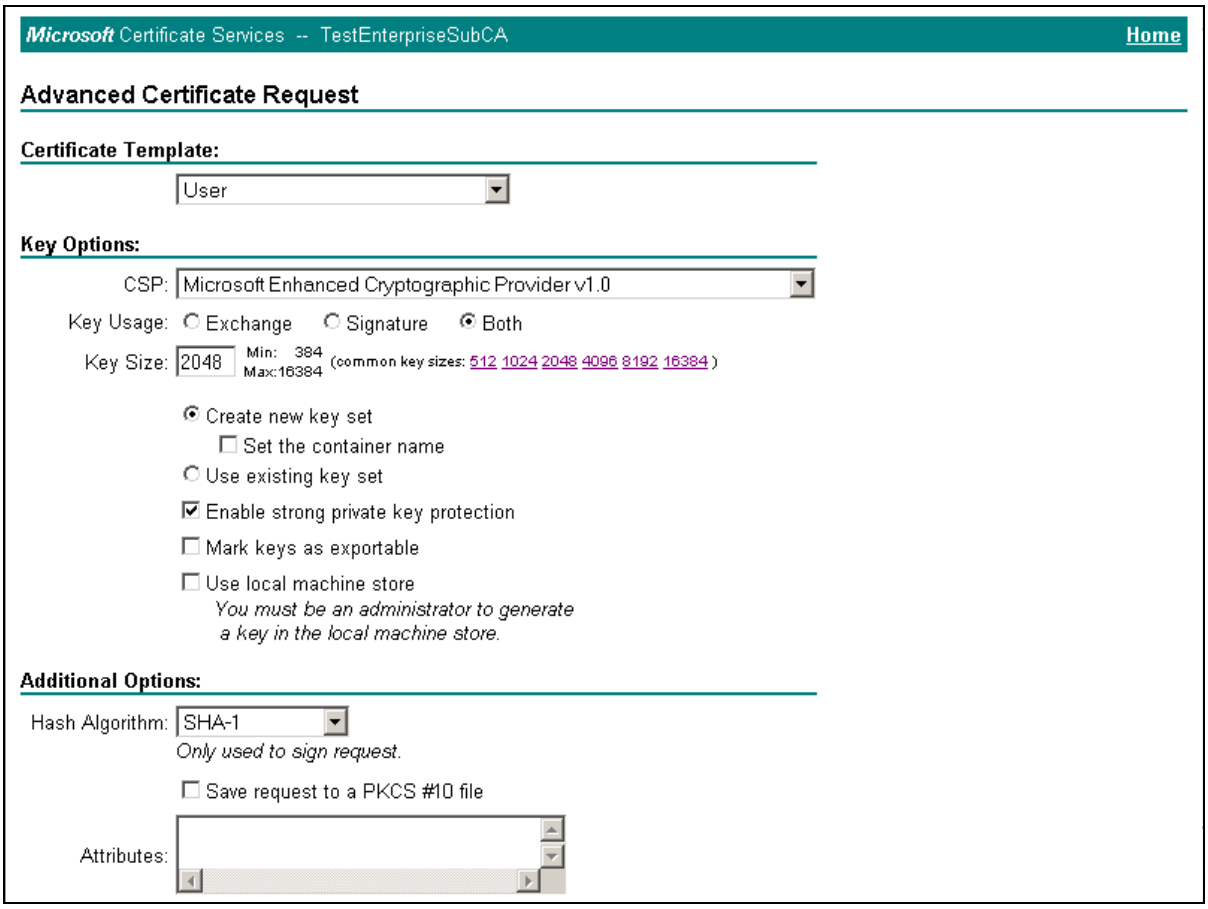


**Figure 37 Example of Advanced Certificate Request Form**

## Securing Certificate Service Web Pages

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

- In the ISM, expand the **Default Web site** and locate the CertSrv virtual directory
- Right-click **CertSrv** and select **Properties**
- Select the **Directory Security** tab
- Click **Edit** under the **Anonymous access and authentication control**

- Make sure **Integrated Windows authentication** is the **ONLY** option selected and click **OK,** and close all dialog boxes.

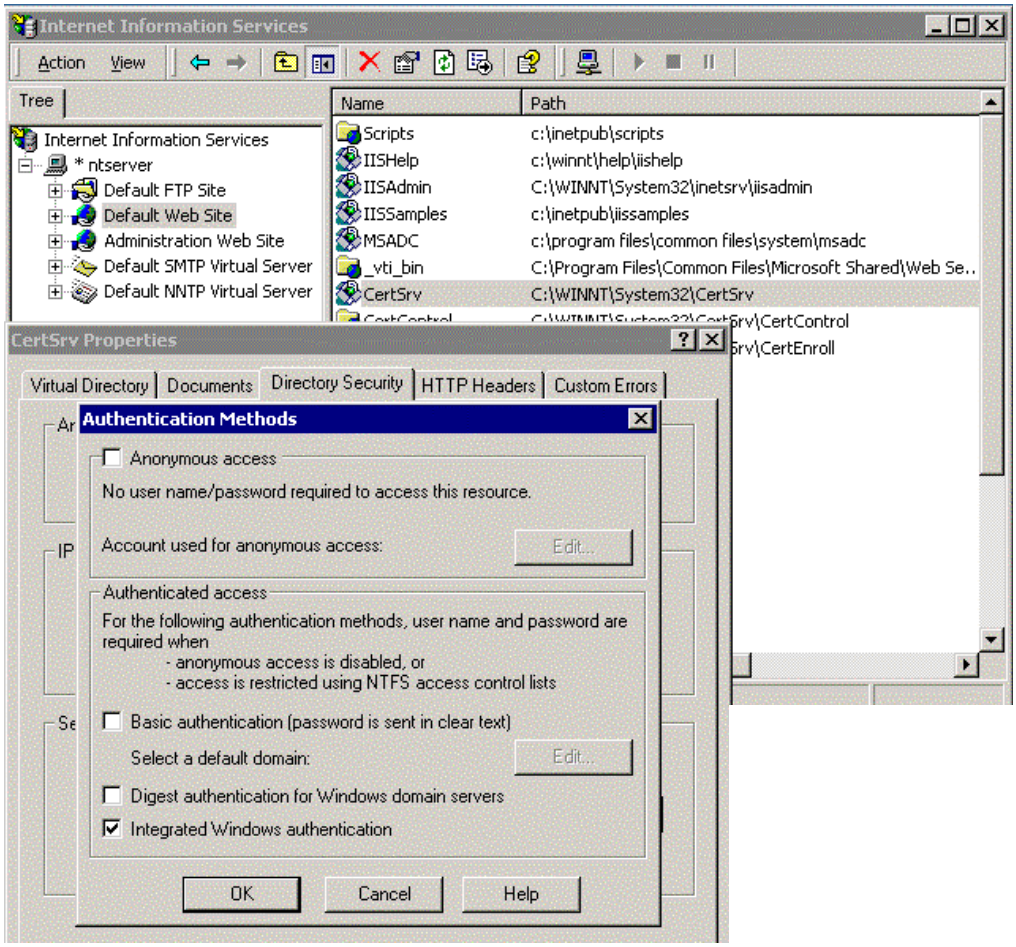


**Figure 38 Securing Certificate Service Web Pages**

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 39**)
- 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 40**).
- The next window lists the options you chose to backup. Click **Finish** and the backup will take place. (See **Figure 41**).

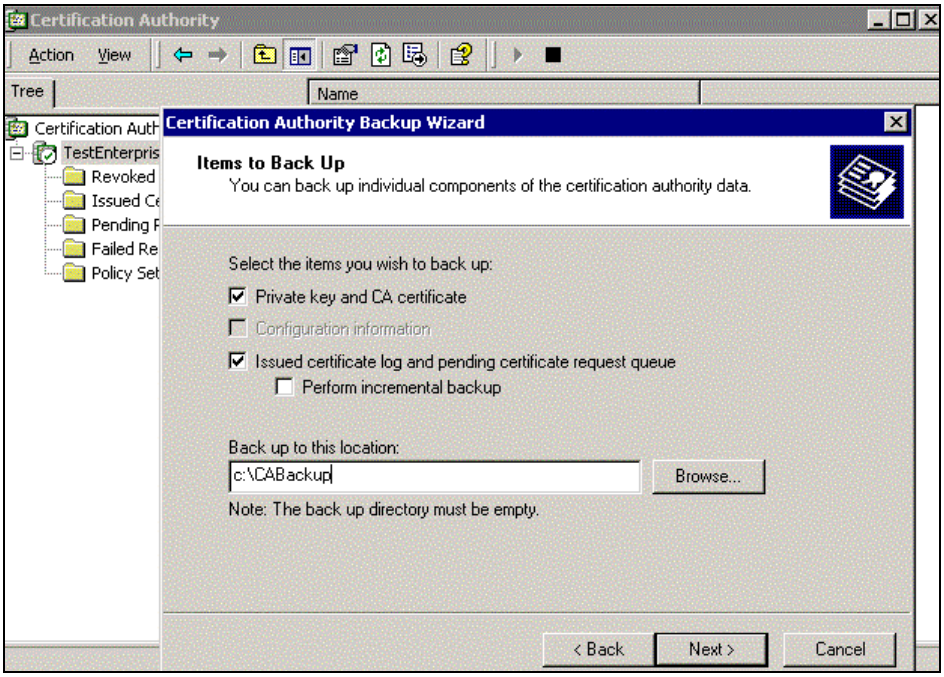


**Figure 39 Selecting Items to Back-up**

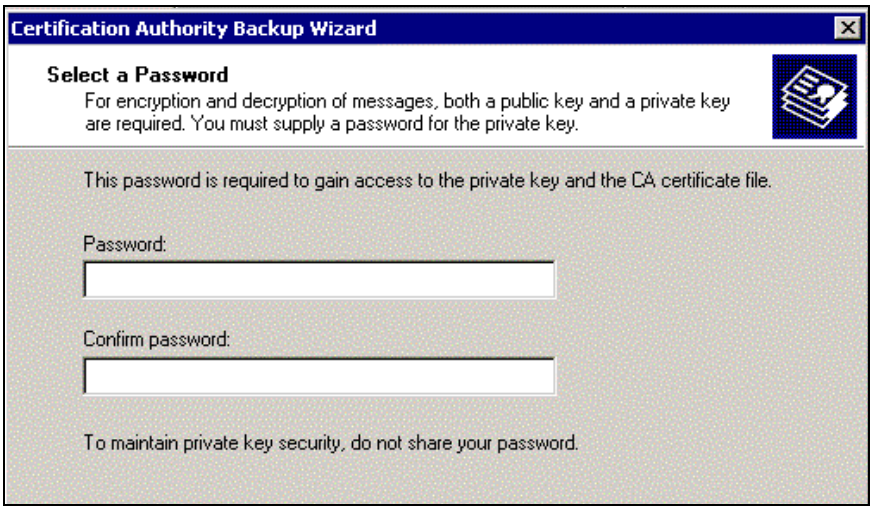


**Figure 40 Selecting a Password for CA Backup**


**Figure 41 Completion of CA Backup Wizard**

## Restoring Certificate Services

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

- If Certificate Service 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

# Further Information (Reference Resources)

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

Microsoft's Certificate Services Help pages

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

# Revisions:

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

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

2.1 - Enhanced explanation of PKI and certificate chaining. Added information on the DSStore tool and iisconfig command, included where to find more information on these resources

2.1.1 - Added information on how to configure CRL distribution points.