Implementing and Administering Certificate Templates in Windows Server 2003

Topics on this Page

By David B. Cross and Brian Komar

Microsoft Corporation

Abstract

Windows Server 2003, Enterprise Edition allows the creation and deployment of customized certificate templates, known as version 2 certificate templates. This white paper details the process of designing and deploying custom certificate templates.

Acknowledgements

David Cross, Program Manager, Microsoft Corporation.

Mike Danseglio, Technical Writer, Microsoft Corporation

Carsten B. Kinder, Senior Consultant, Microsoft Germany

Introduction

Scope

The scope of this white paper is to discuss the best practices in designing, administering, and implementing version 2 Certificate Templates using Windows Server 2003, Enterprise Edition and Enterprise Certification Authorities (CAs).

Terms Used in this White Paper

Application Constraints A constraint that limits what purposes a certificate can be used for in a qualified subordination configuration. A presented certificate must contain the required application constraint to be accepted by the partner organization.

Authority Information Access (AIA) A certificate extension that contains URL locations where the issuing CA’s certificate can be retrieved. The AIA extension can contain HTTP, FTP, LDAP, or FILE URLs.

Certificate Revocation List (CRL) A digitally signed list issued by a CA that contains a list of certificates issued by the CA that have been revoked. The list includes the serial number of the certificate, the date that the certificate was revoked, and the revocation reason. Applications can perform CRL checking to determine a presented certificate’s revocation status; also referred to as a base CRL.

CRL Distribution Point (CDP) A certificate extension that indicates where the certificate revocation list for a CA can be retrieved. This extension can contain multiple HTTP, FTP, FILE, or LDAP URLs for the retrieval of the CRL.

Delta Certificate Revocation List (delta CRL) A type of CRL that contains the list of certificates revoked since the last base CRL was published. Delta CRLs are often used in environments where numerous certificates are revoked to optimize bandwidth utilization.

Issuance Policy Constraints A constraint that defines what issuance practices must be followed for certificates to be trusted by your organization. Issuance policy object identifiers in your organization are mapped to the matching object identifiers in a partner organization, so that object identifiers in presented certificates are recognized by your Public Key Infrastructure (PKI).

Name Constraints A constraint that limits what names are permitted or excluded in certificate requests submitted to a CA.

Online Certificate Status Protocol (OCSP) A protocol that allows real-time validation of a certificate's status—the CryptoAPI makes a call to an OCSP responder and the OCSP responder provides an immediate validation of the revocation status for the presented certificate. Typically, the OCSP responder uses CRL checking for maintaining its status information.

Public Key Infrastructure (PKI) A PKI provides an organization with the ability to securely exchange data over a public network using public key cryptography, thus ensuring privacy by preventing the interception of communications. A PKI consists of Certification Authorities (CAs) that issue digital certificates, directories that store the certificates (including Active Directory in Windows 2000 and Windows Server 2003), and X.509 certificates that are issued to security entities on the network. The PKI provides validation of certificate-based credentials and ensures that the credentials are not revoked, corrupted, or modified.

Security Principal A user, security group, or computer account that can be assigned permissions in a Windows Server 2003 discretionary access control list (DACL).

Subject Key Identifier (SKI) A certificate extension included in CA certificates that contains a hash of the CA certificate's public key. This hash is placed in the Authority Key Identifier (AKI) extension of all issued certificates to facilitate chain building.

Certificate Template Overview

Windows 2000 introduced the concept of using certificate templates to define the format and content of a certificate. Certificate templates are used by Windows 2000 Enterprise CAs to define what certificates can be issued by the Windows 2000 Enterprise CAs. Associated with the certificate template is a discretionary access control list (DACL) that defines which security principals have permissions to read, enroll, and configure the certificate template. Enterprise CAs are integrated into Active Directory. The certificate templates and the DACLs of the certificate template objects are defined in Active Directory with a forest-wide validity. If more than one Enterprise CA is running in the Windows forest, permission changes would have an impact on all Enterprise CAs.

The certificate templates used by Windows 2000 Enterprise CAs are known as version 1 certificate templates. Windows 2000 shipped with a number of predefined version 1 certificate templates, but modification of these default certificate templates is not allowed. The only modification that is enabled is the changing of permissions to allow enrollment of the certificate template. The version 1 certificate templates are created by default when an Enterprise CA is installed.

Windows Server 2003 extends certificate templates by introducing version 2 templates. Version 2 templates allow customization of most settings in the template. Several preconfigured version 2 templates are supplied in the default configuration and more can be added as necessary. This allows complete configuration flexibility for administrators. Alternatively, a version 1 certificate template can be duplicated, resulting in a version 2 certificate template that can be modified and secured separately.

> **Note** Similar to Windows 2000, Windows Server 2003 supports only version 1 templates. Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition support both version 1 and version 2 templates. Certificates based on version 2 templates can only be issued by an Enterprise CA running Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition.

When a certificate template is defined, the definition of the certificate template must be available to all CAs in the forest. This is accomplished by storing the certificate template information in the Configuration naming context (CN=Configuration,DC=*ForestRootName*). The replication of this information depends on the Active Directory replication schedule, and the certificate template may not be available at all CAs until replication is completed. This storage and replication is accomplished automatically by Windows Server 2003 family computers.

Requirements

To set up a Windows Server 2003 CA, the Active Directory schema must be upgraded to the Windows Server 2003 schema. You cannot install a Windows Server 2003 CA into a Windows 2000–based schema.

The schema is updated to the Windows Server 2003 schema by running ADPREP /Forestprep at a Windows 2000 domain controller with the Windows Server 2003 CD-ROM in the CD-ROM drive.

Upgrading from Version 1 to Version 2 Certificate Templates

When you install Windows Server 2003 CA into a Windows Server 2003–based Active Directory, the current certificate templates are updated during the upgrade process. The update modifies default settings for the Windows 2000 version 1 certificate templates that implement better security defaults. If a Windows Server 2003, Enterprise Edition CA is installed in addition several, version 2 certificate templates are created.

The upgrade process of an Enterprise CA must be performed by an account that is a member of the forest root Domain Admins group and the Enterprise Admins universal group. This is because the upgrade makes modifications to the Configuration naming context in Active Directory. Specifically, the account performing the upgrade must have the following permissions through group memberships (these are the default permissions):

- Full control permissions over the "CN=Certificate Templates, CN=Public Key Services,CN=Services,CN=Configuration, DC=*ForestRootDomain*" container
- Full control permissions over the "CN=OID,CN=Public Key Services,CN=Services,CN=Configuration, DC=*ForestRootDomain* " container
- Full Control permissions for each certificate template object in the "CN=Certificate Templates, CN=Public Key Services,CN=Services,CN=Configuration, DC=*ForestRootDomain*" container

> **Note** Delegation over the Certificate Templates container will have no effect on individual certificate templates. In other words, the ACL on certificate templates is not inherited from the ACL on the container.

To upgrade the certificate templates, perform the following procedure after the upgrade for a Certification Authority to Windows Server 2003 or the installation of a new Windows Server 2003 CA on the network:

1. Upgrade to the Windows Server 2003 schema.
2. Log on as a user account that is a member of the forest root Domain Admins group and the Enterprise Admins group.
3. At a Windows Server 2003, Enterprise Edition CA (the CA can be running on Windows Server 2003, Windows Server 2003, Enterprise Edition, or Windows Server 2003, Datacenter Edition configured as a member-server or Domain Controller), run the Certificate Templates MMC console (certtmpl.msc).

   > **Note** Alternatively, the Certificate Templates MMC console can be run from a Windows XP Professional computer with the Windows Server 2003 Administration Pack (Adminpak.msi) installed. The same permissions apply as noted previously.

4. When prompted to write new certificate templates, click OK.

To verify that the upgrade is successful, open the Certificate Templates MMC console and confirm that there are 29 certificate templates. The Version # of templates should all exist and be in the format of xxx.xxx, for example, 100.2. Version 1 certificate templates use a single digit for the primary version number, for example, the Administrator certificate template version number is 3.1. Version 2 certificate template primary version numbers are three digits in length. For example, the Key Recovery Certificate Template version number is 105.0.

> **Note** An upgrade of the certificate templates is performed run if a new Windows Server 2003 CA is installed in the forest. If a Windows 2000 CA is upgraded to Windows Server 2003, the template upgrade is not performed automatically and will only be performed when the certificate templates MMC snap-in is opened for the first time. You can still verify that the update has taken place, but the process is performed automatically.

Default Templates

Once the upgrade to Windows Server 2003 certificate templates is completed, the following preconfigured certificate templates are listed in the Certificate Templates MMC console.

Name	Description	Key Usage	Subject Type	Published to AD
Administrator	Allows trust list signing and user authentication	Signature and encryption	User	Yes
Authenticated Session	Subject can authenticate to a Web server	Signature	User	No
Basic EFS	Used by Encrypting File System (EFS) to encrypt data	Encryption	User	Yes
CA Exchange	Used to store keys that are configured for private key archival	Encryption	Computer	No
CEP Encryption	Allows the holder to act as a registration authority (RA) for simple certificate enrollment protocol (SCEP) requests	Encryption	Computer	No
Code Signing	Used to digitally sign software	Signature	User	No
Computer	Allows a computer to authenticate itself on the network	Signature and encryption	Computer	No
Cross-Certification Authority	Used in cross-certification and qualified subordination	Signature	CrossCA	Yes
Directory E-mail Replication	Used to replicate e-mail within Active Directory	Signature and encryption	DirEmailRep	Yes
Domain Controller	All-purpose certificates held by domain controllers	Signature and encryption	DirEmailRep	Yes
Domain Controller Authentication	Used to authenticate Active Directory computers and users	Signature and encryption	Computer	No
EFS Recovery Agent	Allows the subject to decrypt files previously encrypted with EFS	Encryption	User	No
Enrollment Agent	Used to request certificates on behalf of another subject	Signature	User	No
Enrollment Agent (Computer)	Used to request certificates on behalf of another computer	Signature	Computer	No

	subject			
Exchange Enrollment Agent (Offline request)	Used to request certificates on behalf of another subject and supply the subject name in the request	Signature	User	No
Exchange Signature Only	Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for digitally signing e-mail	Signature	User	No
Exchange User	Used by Microsoft Exchange Key Management Service to issue certificates to Exchange users for encrypting e-mail	Encryption	User	Yes
IPSEC	Used by IP Security (IPSec) to digitally sign, encrypt, and decrypt network communication	Signature and encryption	Computer	No
IPSEC (Offline request)	Used by IP Security (IPSec) to digitally sign, encrypt, and decrypt network communication when the subject name is supplied in the request	Signature and encryption	Computer	No
Key Recovery Agent	This certificate can recover private keys archived on the certification authority.	Encryption	KRA	Yes
Root Certification Authority	Used to prove the identity of the root certification authority	Signature	CA	Yes

Name	Description	Key Usage	Subject Type	Published to AD	Template Version
Router (Offline request)	Used by a router when requested through SCEP from a CA that holds a CEP Encryption certificate	Signature and encryption	Computer	No	3.1
Smartcard Logon	Allows the holder to authenticate using a smart card	Signature and encryption	User	No	5.1
Smartcard User	Allows the holder to authenticate and protect e-mail using a smart card	Signature and encryption	User	Yes	9.1
Subordinate Certification Authority	Used to prove the identity of the root certification authority, issued by the parent or root certification authority	Signature	CA	Yes	4.1
Trust List Signing	The holder can digitally sign a trust list.	Signature	User	No	2.1
User	Certificate to be used by users for e-mail, EFS, and client	Signature and encryption	User	Yes	2.1

	authentication				
User Signature Only	Allows users to digitally sign data	Signature	User	No	3.1
Web Server	Proves the identity of a Web server	Signature and encryption	Computer	No	3.1

Administering Version 1 Certificate Templates

In Windows 2000, certificate management was very limited because only the templates security permissions could be set. This was done through advanced view of the Active Directory Sites and Services MMC snap-in.

With Windows Server 2003, certificate template management is done through the Certificate Templates MMC snap-in rather than through the Active Directory Sites and Services MMC snap-in.

Administering Version 2 Certificate Templates

Version 2 certificate templates allow you to define specific attributes for certificates that meet your organization's business needs. For example, certificate templates allow you to

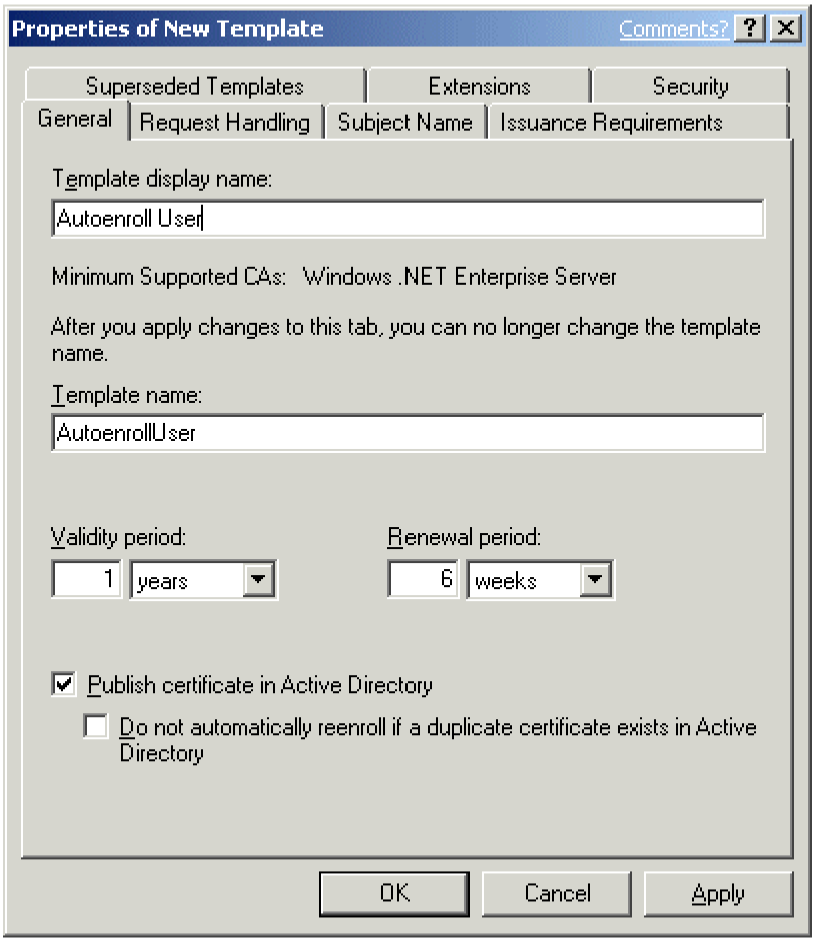
- Define whether the private key associated with a certificate can be exported.
- Define whether the certificate request must be approved by a certificate manager, and define how many managers must approve a request before the certificate is issued.
- Define what cryptographic service providers (CSPs) are supported by a certificate template.
- Define issuance and application policy for issued certificates.

The following sections detail the specific information that can be configured for a version 2 certificate template using the Certificate Templates MMC console (certtmpl.msc). To create a new certificate template, you start by duplicating an existing certificate template that is similar in functionality to the required certificate template. Selecting the correct initial template is important so that the current certificate template settings will serve as a starting point for your certificate template configuration.

> **Note** Since certificate templates exist only once within a forest, all changes made apply on a forest-wide level. If several CA's exist within one forest, templates can be assigned to CA's via the publishing mechanism. Nevertheless, all CA's within a forest use one set of templates.

The General Tab

The General tab (Figure 1) is the first tab that appears when you duplicate an existing certificate template.



Template display name: Autoenroll User

Minimum Supported CAs: Windows .NET Enterprise Server

After you apply changes to this tab, you can no longer change the template name.

Template name: AutoenrollUser

Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

If your browser does not support inline frames, click here to view on a separate page.

Figure 1 The General Tab

On the General tab, you can configure the following attributes of the certificate template:

- **Template display name** The display name shown in the Certificate Templates console, Certificates console, and in the Certification Authority console.
- **Template name** The name of the certificate template object created in the CN=Certificate Templates,CN=Public Key Services,CN=Services,DC=*ForestRootDomain* container.

> **Note** The template display name and template name attributes cannot be changed once the certificate template is created.

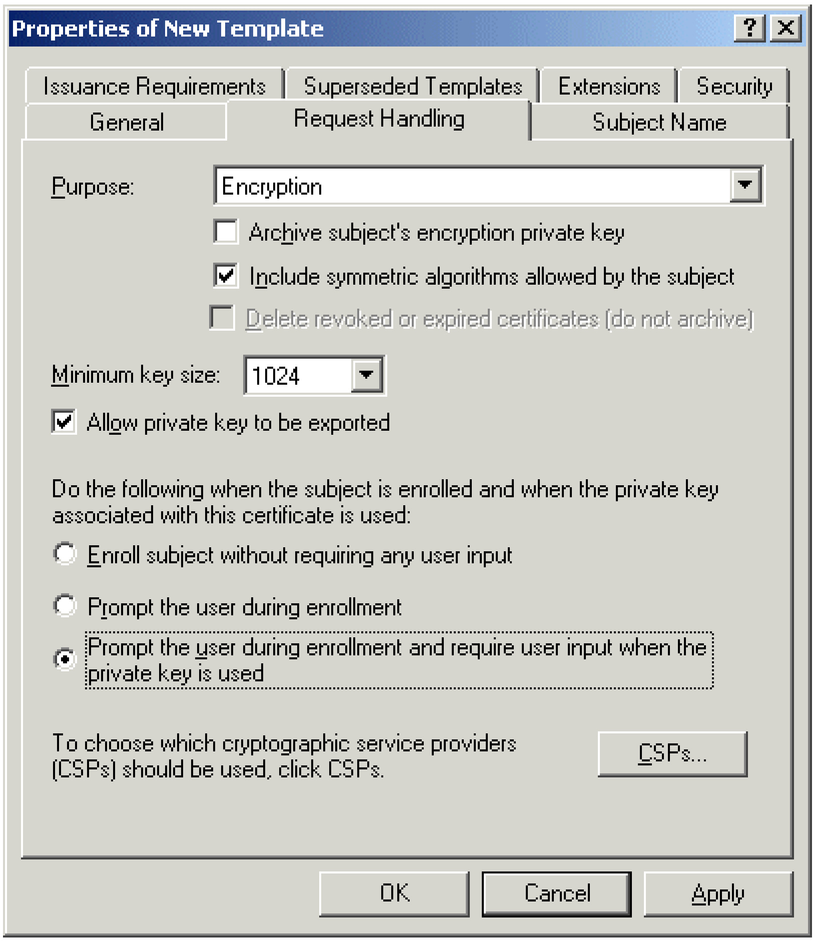
- **Validity period** Defines the validity period for an issued certificate. The validity period must not be defined to be greater than the validity period of the CA's certificate. The minimum renewal period is 80% of the certificate lifetime or 6 weeks, whichever is greater.
- **Renewal period** The time before the validity period expires when the certificate will be renewed if re-enrollment is supported for the certificate template.
- **Publish options** You can choose whether to publish the certificate to Active Directory based on the certificate template. The certificates are published as an attribute of the security principal contained in the subject of the issued certificate.
- **Reenrollment option** If the certificate template is published to Active Directory, you can prevent re-enrollment if a valid certificate of the same certificate template exists for the security principal indicated in the subject.

> **Note** Re-enrollment settings mainly affect auto-enrollment design in a Windows Server

2003 network. See the Windows 2000 Certificate Autoernollment in Windows XP white paper at http://www.microsoft.com/WindowsXP/pro/techinfo/administration/autoenroll/default.asp

The Request Handling Tab

The Request Handling tab (Figure 2) defines the purpose of the certificate template, the supported cryptographic service providers (CSPs), minimum key length, exportability, auto-enrollment settings, and whether strong private key protection should be required.



Properties of New Template

Purpose: Encryption

□ Archive subject's encryption private key

☑ Include symmetric algorithms allowed by the subject

□ Delete revoked or expired certificates (do not archive)

Minimum key size: 1024

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

○ Enroll subject without requiring any user input

○ Prompt the user during enrollment

● Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

If your browser does not support inline frames, click here to view on a separate page.

Figure 2 The Request Handling Tab

Certificate Purposes

The certificate purpose defines the intended primary use of the certificate. The certificate purpose can be one of four settings:

- **Encryption** A certificate with this purpose will contain cryptographic keys for encryption and decryption.
- **Signature** A certificate with this purpose will contain cryptographic keys for signing data only.
- **Signature and encryption** A certificate with this purpose covers all primary uses of a certificate's cryptographic key, including encryption of data, decryption of data, initial logon, or digitally signing data.
- **Signature and smartcard logon** A certificate with this purpose allows for initial logon with a smart card, and to digitally sign data; it cannot be used for data encryption.

Note The certificate purpose setting will determine whether key archival can be enabled for a certificate template. Key archival is only possible if the certificate purpose is set to Encryption or Signature and encryption. The recovery of a private key for digitally signing information may result in identity theft and is not supported. Key archival is not supported by most smart card CSPs.

Archive Settings

When subjects lose their private keys due to user profile corruption or stolen computers, any information that was persistently encrypted with the corresponding public key is inaccessible. To help avoid this, Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition have the ability to archive a subject's keys in its database when certificates are issued. These keys are encrypted and stored by the CA. If subjects lose their keys, the information can be retrieved from the database and securely provided to the subjects. This allows the encrypted information to be recovered instead of lost.

The following Key Archival settings are defined in the Request Handling tab:

- **Archive subject's encryption private key** If the issuing Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition certification authority is configured for key archival, the subject's private key will be archived.
- **Allow private key to be exported** When this option is specified, the subject’s private key can be exported for backup or transportation.
- **Deleting revoked or expired certificates (do not archive)** If a certificate is renewed due to expiration or revocation, the previously issued certificate is removed from the subject's certificate store. By default, the certificate is archived.
- **Include symmetric algorithms allowed by the subject** When the subject requests the certificate, they can supply a list of supported symmetric algorithms. This option allows the issuing certification authority to include those algorithms in the certificate, even if they are not recognized or supported by that server. The algorithms are used by applications like secure e-mail.

To enable key archival and recovery, the following configuration settings in the certificate template and at the Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition CA must be made:

- The specific certificate template must be configured to allow key archival.
- One or more key recovery agents must be identified on the certification authority and key recovery agent certificates must be issued to those agents.
- Key archival must be configured on the certification authority.

User Input Settings

The Request Handling tab also allows several user input settings to be defined for a certificate template. These settings include:

- **Enroll subject without requiring any user input** This option allows auto-enrollment without any user interaction and is the default setting for both machine and user certificates. This option must not be enabled for machine certificates.
- **Prompt the user during enrollment** Although useful when testing initial auto-enrollment deployments, typically, this option is disabled. By disabling this option, users do not have to provide any input for the installation of a certificate based on the certificate template.
- **Prompt the user during enrollment and require user input when the private key is used** This option enables the user to set a strong private key protection password on the user’s private key when the key is generated and requires the user to use it whenever the certificate and private key are used. This option must not be enabled for machine certificates or smart card user certificates.

Note To enable smart card auto-enrollment, the **Prompt the user during enrollment** option must be enabled so that the user is prompted to insert the smart card in the smart card reader when required.

> **Important** Strong private key protection with auto-enrollment is not supported or enabled for machine certificates and is only available on Windows XP Service Pack 1 client machines.

In addition, with Windows 2000 Service Pack 3 and Windows XP Service Pack 1, it is possible to force strong private key protection for all CSPs through the registry. Three new keys can be added to "HKLM\Software\Microsoft\Cryptography" in the registry:

ForceKeyProtection This key will force DPAPI to grey-out the option that would allow the user the choice of using a password when UI was selected. When set, the user MUST enter a password.

> **<"0">** = do not force UI on key protection
> **<"1">** = default to UI, but let user change selection
> **<"2">** = force UI on key protection, grey-out option for user

CachePrivateKeys Contains a 1, if (and only if) the following registry key is used:

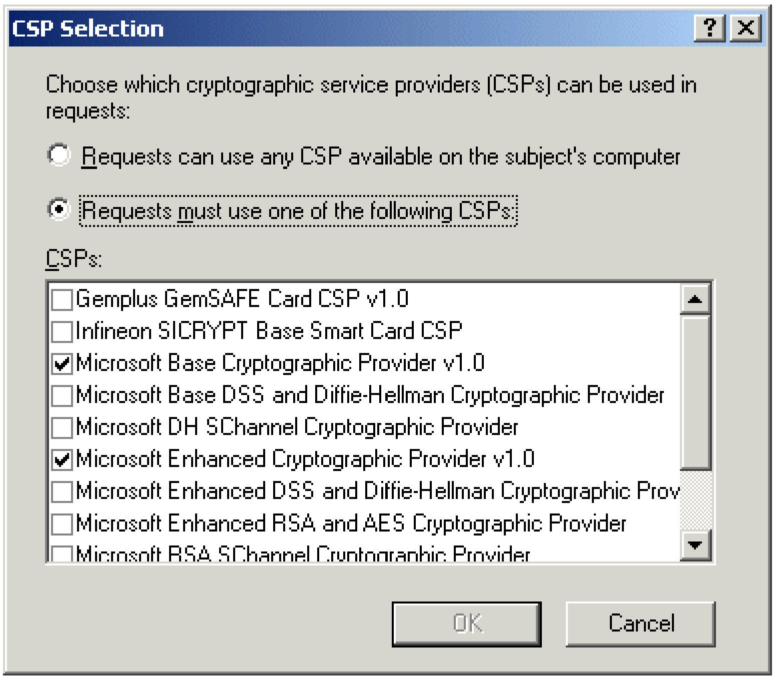
PrivateKeyLifetimeSeconds Contains the number of seconds that a key will remain cached without being used. The key cache timer will be reset on every successful use in the CSP.

> **Warning** Requiring the use of strong private key protection and user prompting on all new and imported keys will disable some applications, such as EFS which cannot display UI.

Other Request Handling Settings

In addition to key archival settings, some general options that affect all certificates, including those that do not enable key archival, can be defined. These include

- **Minimum key size** This specifies the minimum size, in bits, of the key that will be generated for this certificate.
- **Cryptographic service providers** This is a list of cryptographic service providers (CSPs) that will be used to enroll certificates for the given template. Selecting one or more CSPs configures the certificate to only work with those CSPs. If you do not select a specific CSP, the certificate enrollment will work with any installed CSP, but will use the first CSP from the enumeration list. The CSP must be installed on the client workstation for the CSP to be used during enrollment. If a specific CSP is chosen and not available on a client machine, enrollment will fail.



CSP Selection

Choose which cryptographic service providers (CSPs) can be used in requests:

○ Requests can use any CSP available on the subject's computer

● Requests must use one of the following CSPs:

CSPs:

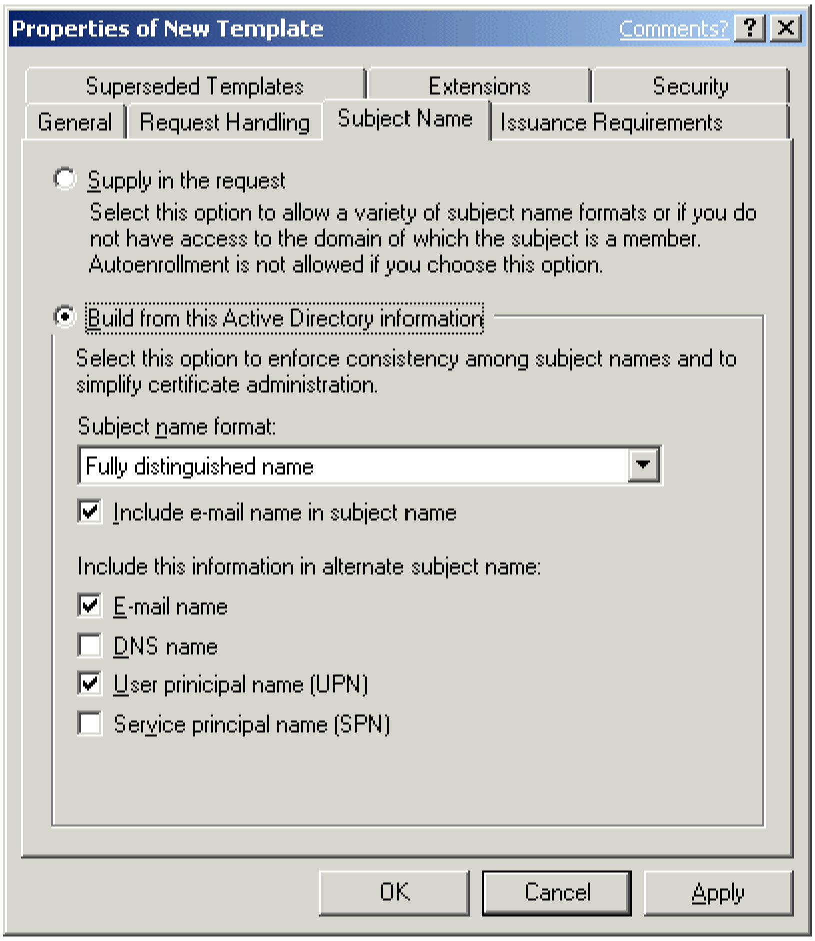
☐ Gemplus GemSAFE Card CSP v1.0
☐ Infineon SICRYPT Base Smart Card CSP
☑ Microsoft Base Cryptographic Provider v1.0
☐ Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
☐ Microsoft DH SChannel Cryptographic Provider
☑ Microsoft Enhanced Cryptographic Provider v1.0
☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Prov
☐ Microsoft Enhanced RSA and AES Cryptographic Provider
☐ Microsoft RSA SChannel Cryptographic Provider

> **Note** You can add third-party CSPs by installing the manufacturer's CSP-related files.

The newly installed CSP will appear in the list of available CSPs when the certificate templates snap-in is opened after CSP installation.

The Subject Name Tab

When establishing a certificate template, the subject name must be defined. This is included in the issued certificate template and must uniquely identify the subject. The subject name can either be built automatically during the certificate request using the authentication name of the subject, or explicitly defined by the subject and included in the certificate request (Figure 3).



○ Supply in the request
Select this option to allow a variety of subject name formats or if you do not have access to the domain of which the subject is a member. Autoenrollment is not allowed if you choose this option.

● Build from this Active Directory information
Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format: Fully distinguished name

☑ Include e-mail name in subject name

Include this information in alternate subject name:

☑ E-mail name
☐ DNS name
☑ User prinicipal name (UPN)
☐ Service principal name (SPN)

If your browser does not support inline frames, click here to view on a separate page.

Figure 3 The Subject Name Tab

A number of options can be included with the subject name, as well as specific configuration settings for the subject name when the subject name is built from Active Directory information during the certificate request process. The format of the subject name can be defined as

- **None** Does not enforce any name format for this field.
- **Common name** The certification authority creates the subject name from the common name (CN) of the requestor obtained from Active Directory. These should be unique within a domain, but may not be unique within an enterprise.
- **Fully distinguished name** The certification authority creates the subject name from the fully distinguished name obtained from Active Directory. This guarantees that the name is unique within an enterprise.

In addition, you can choose to include the e-mail name in the subject name. This information is populated from the E-mail attribute of an account, and is included with either the common name or fully distinguished name as part of the subject name.

In addition to the subject name, you can also choose what name formats are included in the alternate subject name attributes of issued certificates. The alternate subject name formats that are available include

- **E-mail name** If the e-mail name field is populated in the Active Directory user object, that e-mail name will be used for user accounts.

  > **Note** The e-mail name is required for user certificates. If the e-mail name is not populated for a user in Active Directory, the certificate request by that user will fail.

- **DNS name** The fully qualified domain name (FQDN) of the subject that requested the certificate is used for computer accounts.
- **User principal name (UPN)** The user principal name is part of the Active Directory user object and will be used for user accounts.
- **Service principal name (SPN)** The service principal name is part of the Active Directory computer object and will be used for computer accounts.

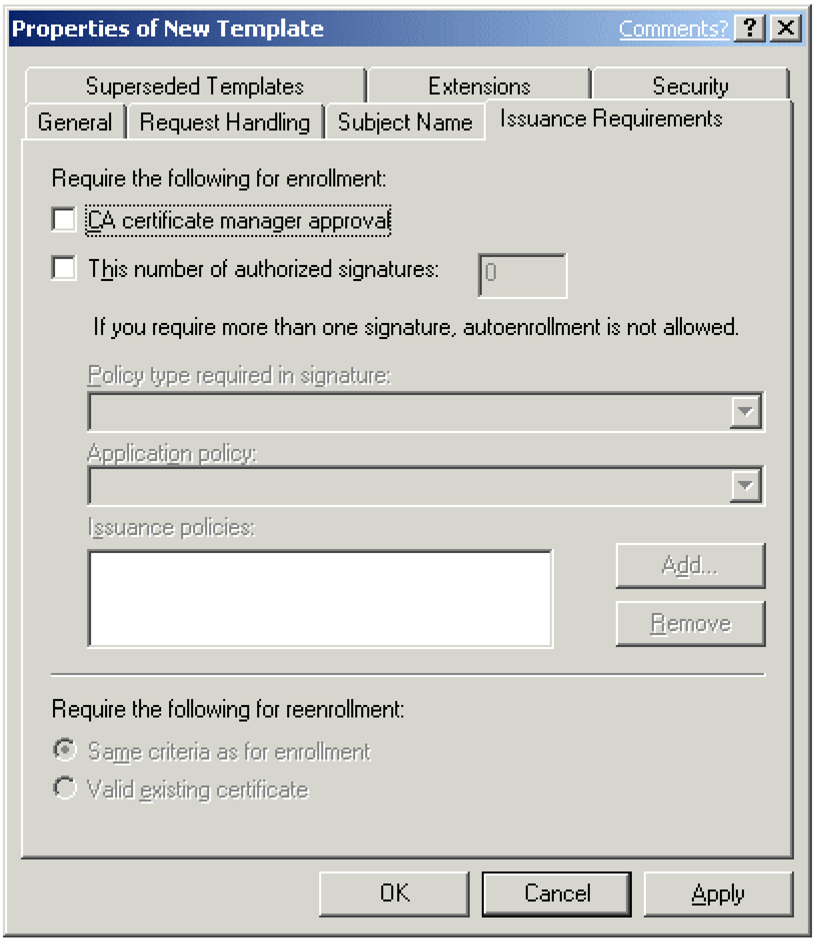
If the Subject Name option is set to **Supply in the request**, you should set one or more Issuance Requirements for the template to prevent subjects from requesting certificates using any subject name. This would allow subjects to impersonate other subjects easily. Issuance requirements ensure that the certificate request is inspected and validated before the certificate is issued.

The only case in which a subject can request a certificate with a different subject name is when the request holds a certificate based on the Enrollment Agent template. The Enrollment Agent template allows a subject to request a certificate on behalf of another subject.

> **Note** No user interface exists on the client to supply a subject name in the certificate request. If you require the ability to provide the subject name, you must perform the certificate request programmatically using the XEnroll.dll ActiveX control.

The Issuance Requirements Tab

The Issuance Requirements tab (Figure 4) allows higher assurance level certificates to be placed in a pending state until the certificate is reviewed before issuance. This allows for multiple signers of a CMC request to exist. For more information on CMC, see RFC 2797 Certificate Management Messages over CMS.



Require the following for enrollment:

□ CA certificate manager approval

□ This number of authorized signatures: 0

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature:

Application policy:

Issuance policies:

Require the following for reenrollment:

● Same criteria as for enrollment

○ Valid existing certificate

If your browser does not support inline frames, click here to view on a separate page.

Figure 4 The Issuance Requirements Tab

When CA certificate manager approval is enabled, the certificate is placed into a pending state, rather than being issued immediately. In its pending state, the certificate request can be reviewed by certificate managers, ensuring a higher level of assurance for the issued certificate.

The following settings configure the authentication and signature requirements for issuance certificates that are based on a template:

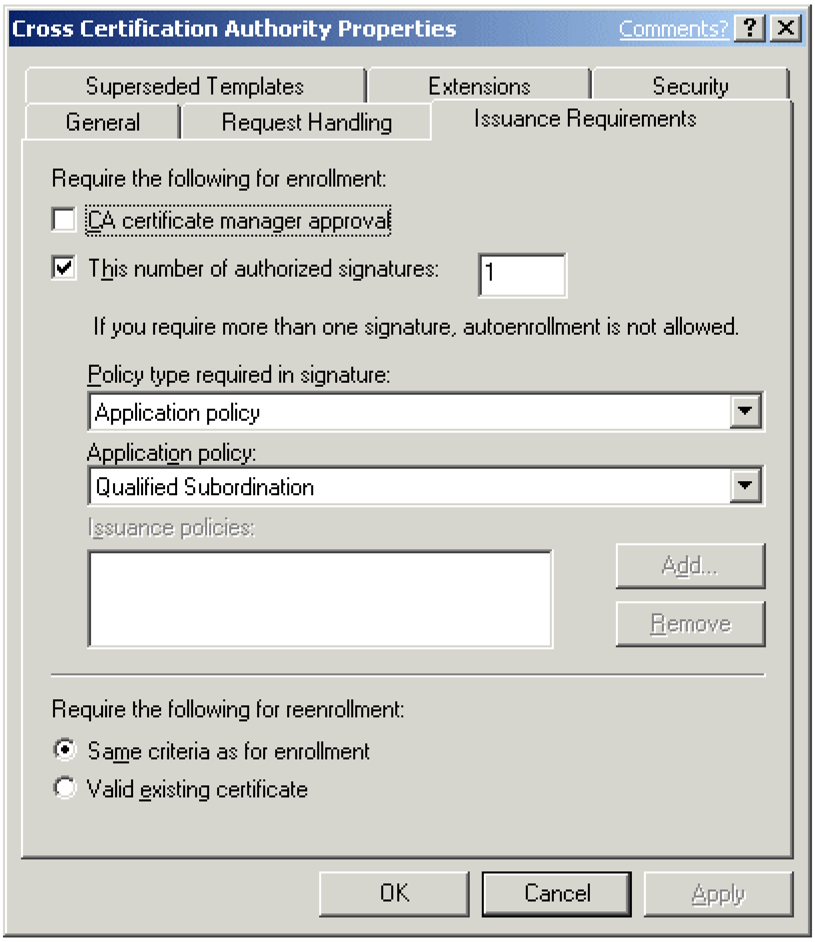
- **CA certificate manager approval** All certificates are placed into the pending container for a certificate manager to issue or deny. Any defined certificate manager can issue or deny a certificate request of this type.
- **This number of authorized signatures** This setting requires the CMC certificate request to be digitally signed by one or more authorized parties before it can be issued.

> **Note** Defining the number of authorized signatures enables several other configuration parameters.

- **Policy type required in signature** This option is only enabled when the number of authorized signatures value is set. This option defines which specific application policy, issuance policy, or both are required in the signing certificate. This is how the certification authority determines whether the signature is appropriate for authorizing the issuance of the subject's certificate.
- **Application policy** This option specifies the application policy that must be included in the signing certificate used to sign the certificate request. It is enabled when Policy type required in signature is set to either Application policy or both application and issuance policy.

- **Issuance policy** This option specifies the issuance policy that must be included in the signing certificate used to sign the certificate request. This option is enabled when Policy type required in signature is set to either Issuance policy or both application and issuance policy.

An example of where issuance requirements are defined is for the issuance of Cross-Certification Authority certificates. This certificate template requires that the signing certificate includes the Qualified Subordination Application Policy OID as shown in Figure 5.



Require the following for enrollment:

☐ CA certificate manager approval

☑ This number of authorized signatures: 1

If you require more than one signature, autoenrollment is not allowed.

Policy type required in signature: Application policy

Application policy: Qualified Subordination

Issuance policies:

Require the following for reenrollment:

● Same criteria as for enrollment

○ Valid existing certificate

If your browser does not support inline frames, click here to view on a separate page.

Figure 5 Issuance Requirements for a Cross-Certification Authority Certificate

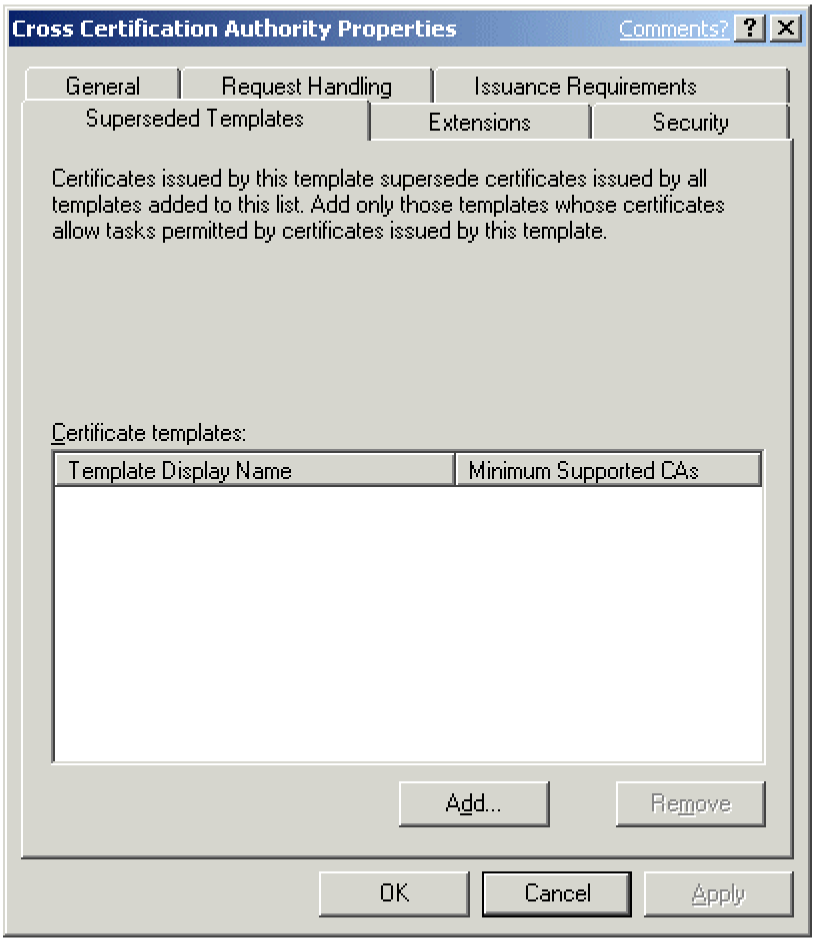
As you can see, the Cross-Certification Authority certificate request must be signed by a certificate containing the Qualified Subordination OID.

In addition, you can also determine whether the same issuance requirements are upheld for certificate renewal, or if the existence of a valid existing certificate of the same template in the certificate store meets the minimum requirements for certificate issuance.

> **Note** For information on including application and issuance policy OIDs in an issued certificate, see The Extensions Tab section.

The Superseded Templates Tab

The Superseded Templates tab (Figure 6) allows you to supersede existing certificate templates with a modified version 2 certificate template.



Certificates issued by this template supersede certificates issued by all templates added to this list. Add only those templates whose certificates allow tasks permitted by certificates issued by this template.

Certificate templates:

Template Display Name	Minimum Supported CAs

If your browser does not support inline frames, click here to view on a separate page.

Figure 6 The Superseded Templates Tab

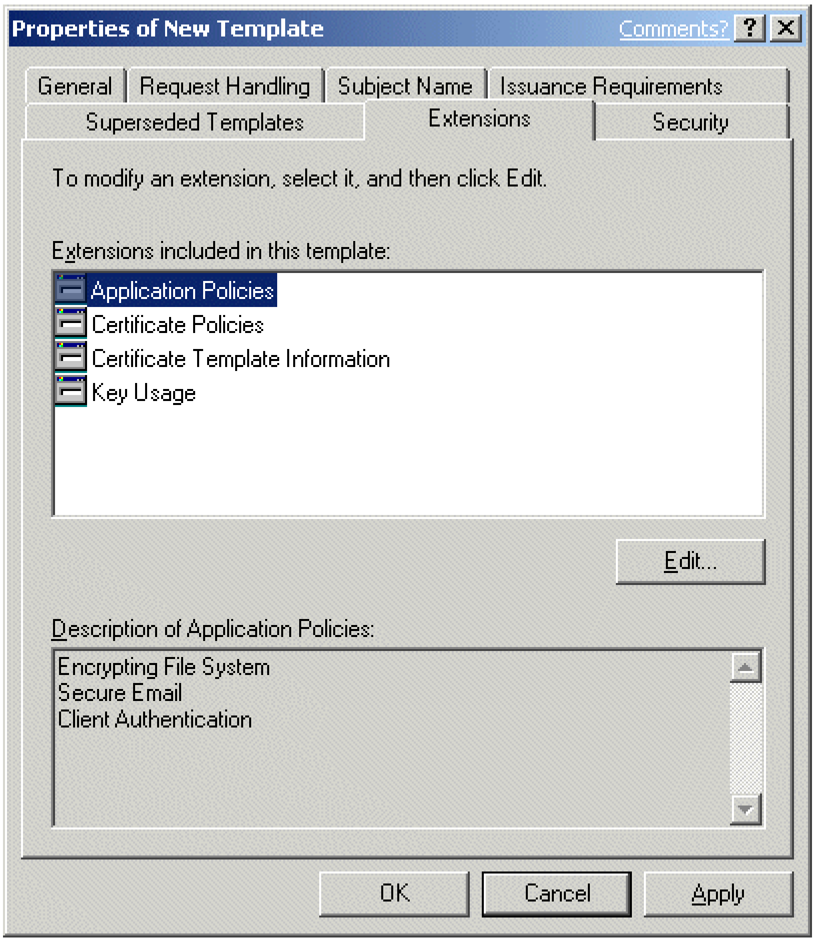
The Superseded Templates tab allows you to redeploy version 2 certificates and ensure that the updated certificates replace previous versions of the certificate or other certificate templates that were used for the same purposes. You can supersede

- A version 1 certificate template with a version 2 certificate template
- A version 2 certificate template with a version 2 certificate template
- Multiple existing certificate templates with a common version 2 certificate template

> **Note** You can force the application of the updated certificate template by forcing all certificate holders to re-enroll the updated certificate template. For more information, see the Re-Enroll Certificate Holders section.

The Extensions Tab

The Extensions tab (Figure 7) allows you to define specific application policies, issuance policies, certificate subject types, and key usage attributes for a certificate template. The following sections detail the specifics on each form of extension defined in a certificate template.



To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Certificate Policies
- Certificate Template Information
- Key Usage

Description of Application Policies:

Encrypting File System
Secure Email
Client Authentication

If your browser does not support inline frames, click here to view on a separate page.

Figure 7 The Extensions Tab

Application Policies

Application policies enable you to decide which certificates can be used for certain purposes. You can issue certificates widely without being concerned that they are misused for an unintended purpose.

Application policies are settings that inform a target that the subject holds a certificate that can be used to perform a specific task. They are represented in a certificate by an object identifier (OID) that is defined for a given application. This object identifier is included in the issued certificate. When a subject presents its certificate, it can be examined by the relying party to verify the application policy and determine if it can perform the requested action.

> **Note** Application policies are similar to the *extended key usage* attribute in version 1 certificate templates. Because some implementations of PKI applications may not understand application policies, both application policies and enhanced key usage sections appear in certificates issued by a Microsoft CA.

The following table shows some of the more commonly used application policies and their related OIDs.

Application Policy	OID
Client Authentication	1.3.6.1.5.5.7.3.2
CA Encryption Certificate	1.3.6.1.4.1.311.21.5
Smart Card Logon	1.3.6.1.4.1.311.20.2.2
Document Signing	1.3.6.1.4.1.311.10.3.12
File Recovery	1.3.6.1.4.1.311.10.3.4.1
Key Recovery	1.3.6.1.4.1.311.10.3.11

Microsoft Trust List Signing	1.3.6.1.4.1.311.10.3.1
Qualified Subordination	1.3.6.1.4.1.311.10.3.10
Root List Signer	1.3.6.1.4.1.311.10.3.9

Certificate Policies

Certificate policies, also referred to as issuance policies, define the level of assurance for an issued certificate. A CA processes each certificate request by a defined set of rules. The certification authority may issue some certificates with no proof of identification and require subjects of another type to submit some proof. This provides different levels of assurance for different certificates. These levels of assurance are represented in certificates as issuance policies.

> **Note** Certificate policies refer to the certificate policies extension identifier described in RFC 2459.

An issuance policy is a group of administrative rules that are implemented when issuing certificates. They are represented in a certificate by an OID that is defined at the certification authority. This OID is included in the issued certificate. When a subject presents its certificate, it can be examined by the target to verify the issuance policy and determine if that level of issuance policy is sufficient to perform the requested action.

An issuance policy describes the conditions under which a certificate is issued. This provides a level of assurance that the subject's certificate request was verified in a specific way.

One or more issuance policies may be selected for a certificate template. Because these issuance policies are simply text labels with an associated object identifier, no options are associated with them. The only special issuance policy is **All issuance policies**, which indicates that this policy includes all others. This is normally reserved for certificates held by certification authorities.

Issuance policies are often used when configuring Qualified Subordination (cross-certification) between PKI hierarchies to ensure that certificates recognized by another organization's PKI meet issuance requirements required by your organization.

Certificate Template Information

The certificate template information, also referred to as the Certificate subject type, defines the purpose of a certificate template. Six subject types are recognized by Windows Server 2003 CAs:

- Key recovery agent
- Directory e-mail replication
- Cross-certified certification authority
- Certification authority (CA)
- Computer
- User

The certificate template information extension cannot be edited. If you require a specific subject type to be applied to a certificate, you should clone from a certificate template that includes the required subject type. Some of the internal flags that are defined for specific subject types limit the display of the certificate template to computers or users. Choosing to clone an incorrect certificate template will prevent the certificate template from being displayed to the desired enrollment audience. For example, a computer certificate template cannot be enrolled for use by a user account.

Key Usage

A certificate enables the subject to perform a specific task. To help control the usage of a certificate outside its intended purpose, restrictions are automatically placed on certificates. Key usage is a restriction method and determines what a certificate can be used for. This allows the administrator to issue certificates that can only be used for specific tasks or certificates that can be used for a broad range of functions. If no key usage is specified, the certificate can be used for any purpose.

For signatures, key usage can be limited to one or more of the following purposes:

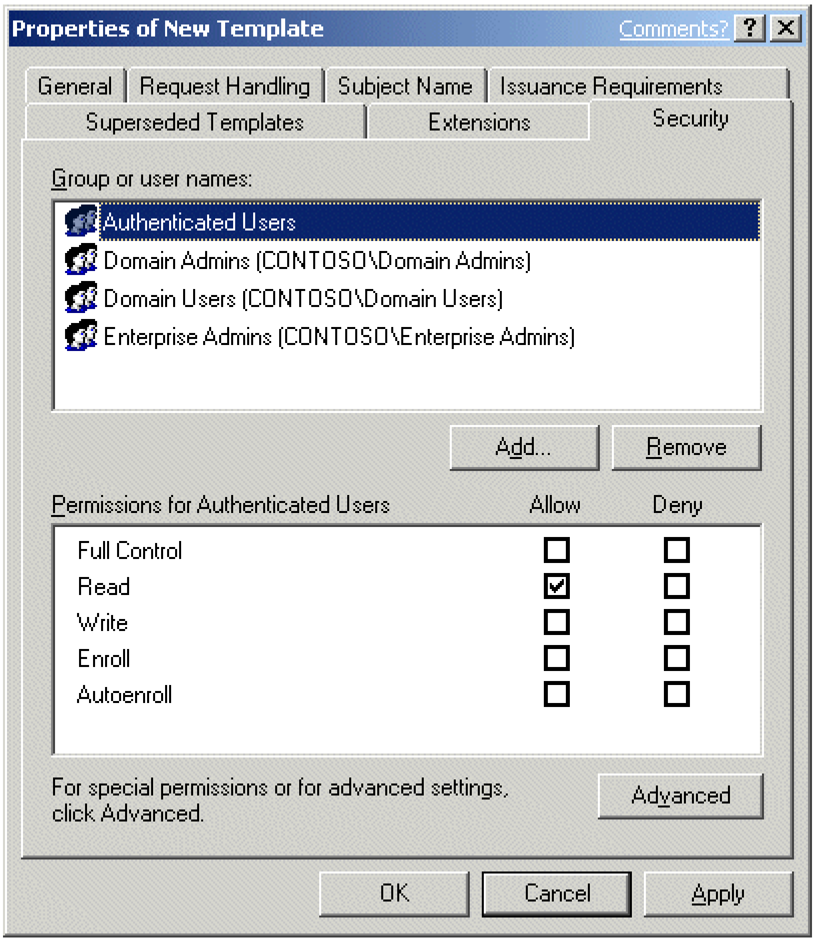
- Digital signature
- Signature is a proof of origin (nonrepudiation)
- Certificate signing
- CRL signing

For encryption key usage, the following options are available:

- Key exchange without key encryption
- Key exchange only with key encryption

The Security Tab

The Security tab (Figure 8) allows you to define the DACL for a specific certificate template. The permissions that you assign to the certificate template define which security principals can read, modify, enroll, or auto-enroll for a specific certificate template.



Group or user names:

- Authenticated Users
- Domain Admins (CONTOSO\Domain Admins)
- Domain Users (CONTOSO\Domain Users)
- Enterprise Admins (CONTOSO\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	□	□
Autoenroll	□	□

For special permissions or for advanced settings, click Advanced.

If your browser does not support inline frames, click here to view on a separate page.

Figure 8 The Security Tab

The permissions that you can assign to a certificate template include

- **Full Control** This permission allows a security principal to modify all attributes of a certificate template, including the permissions for the certificate template.
- **Read** This permission allows a security principal to see the certificate template when enrolling for certificates. It is required for a security principal to enroll or auto-enroll a certificate; it is required by the certificate server to find the certificate templates in Active Directory.
- **Write** This permission allows a security principal to modify the attributes of a certificate template,

including the permissions assigned to the certificate template.

- **Enroll** This permission allows a security principal to enroll for a certificate based on the certificate template. To enroll for a certificate, the security principal must also have Read permissions for the certificate template.
- **Autoenroll** This permission allows a security principal to receive a certificate through the auto-enrollment process. Auto-enrollment permissions require that the user has both Read and Enroll permissions in addition to the Auto-enroll permission.

> **Note** It is recommended that certificate template permissions be assigned only to global groups or universal groups. Because the certificate template objects are stored in the Configuration naming context, you cannot assign permissions using domain local groups. To simplify administration, it is never recommended to assign certificate template permissions to individual user or computer accounts.

It should be considered a best practice to keep Read permission assignment for the Authenticated Users group. This permission assignment allows all users and computers to view the certificate templates in Active Directory. This includes the CA running under the SYSTEM context of a machine account to view the certificate templates when issuing certificates to users and computers.

> **Note** A version 2 certificate template can be distributed to Windows ME and Windows 2000 with Service Pack 2 clients through the Web enrollment pages.

Deploying Certificate Templates

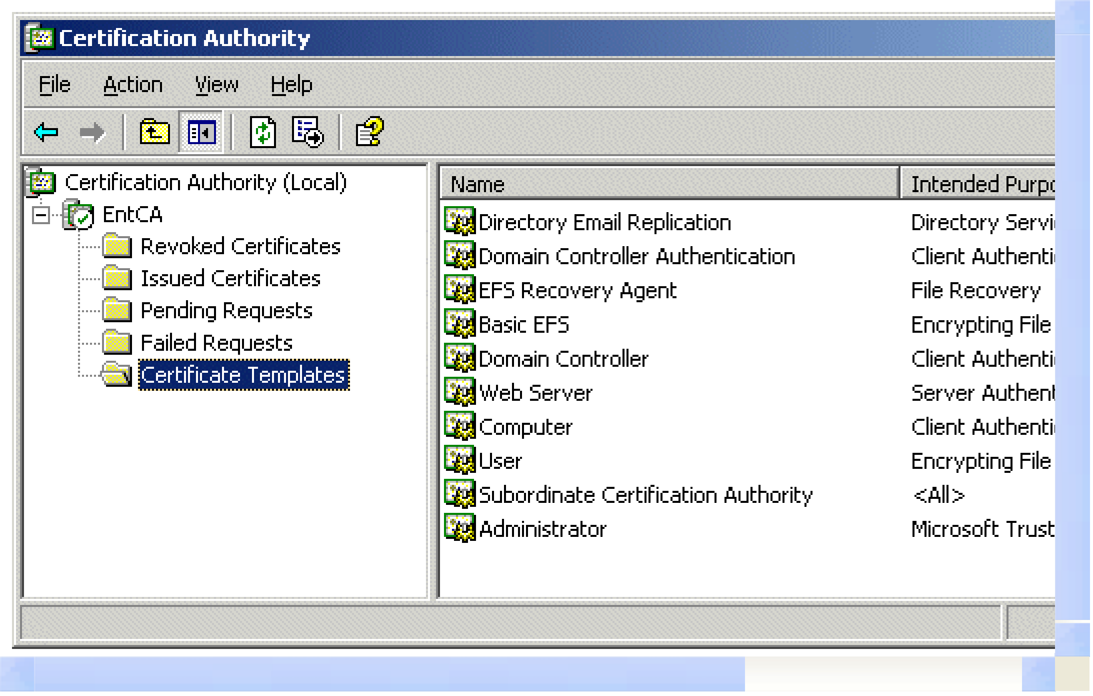
After creating a version 2 certificate template, the next step is to deploy the certificate template. Deployment includes publishing the certificate template at one or more Certification Authorities, defining which security principals have Enroll permissions for the certificate template, and deciding whether to configure auto-enrollment for the certificate template.

Publishing Certificate Templates

Once a certificate template is created in the Certificate Templates MMC and the certificate template has replicated to all domain controllers in the forest, it can now be published for deployment. The main decision in publishing certificate templates is deciding which Certification Authority or Authorities will issue the certificates based on this certificate template.

> **Note** Remember that version 2 certificate templates can only be issued by Enterprise CAs running on Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition.

An Enterprise CA can only issue certificates based on certificate templates that exist in the Certificate Templates container in the Certification Authority MMC console (Figure 9).



Name	Intended Purpo
Directory Email Replication	Directory Servi
Domain Controller Authentication	Client Authenti
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File
Domain Controller	Client Authenti
Web Server	Server Authent
Computer	Client Authenti
User	Encrypting File
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust

If your browser does not support inline frames, click here to view on a separate page.

Figure 9 Defining the Certificate Templates Published at the EntCA Certification Authority

Permission Design

Certificate templates are published to the configuration naming context, which is stored on every domain controller in the forest in the path CN=Certificate Templates, CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRootDomain*. Each certificate template exists as an object in the configuration naming context and has an associated DACL, which defines what specific operations a security principal can do with the certificate.

Use the following recommendations for permissions assignments:

- Assign permissions only to global groups or to universal groups. Certificate templates are defined in the configuration naming context. Permissions should only be assigned to global groups or to universal groups. It is not recommended to assign permissions to domain local groups. They are only recognized in the domain where the domain local group exists and can result in inconsistent application of permissions. It is recommended to never assign permissions directly to an individual user or computer account.
- To enable auto-enrollment, a user or computer must belong to domain groups that are granted Read, Enroll, and Autoenroll permissions.
- To enable enrollment via the Certificates MMC console, through Web-based enrollment, or through auto-renewal, set either domain or universal groups with **Read** and **Enroll** permissions.
- For certificate renewal, a user or computer must belong to a domain security group with Read and Enroll permissions. This is true whether the certificate is manually renewed or the renewal is implemented using auto-enrollment.
- Restrict Write and Full Control permissions to CA managers to ensure that the templates are not improperly configured.

Auto-Enrollment Considerations

Auto-enrollment allows a CA administrator to configure users and computers to automatically enroll for certificates, retrieve issued certificates, and renew expiring certificates without requiring subject interaction. The auto-enrollment process can be configured to function as a background task that does not require any user input.

To properly configure subject auto-enrollment, the administrator must plan the configuration of the certificate template that will use auto-enrollment. Several settings in the certificate template directly affect the behavior of subject auto-enrollment, as follows:

- **User input requirements** On the Request Handling tab (Figure 2) of the desired certificate template, the Require user input for auto-enrollment check box changes the behavior of auto-enrollment. When this check box is selected, subjects are prompted for any necessary information for obtaining or renewing a certificate. When this check box is cleared, auto-enrollment operates silently, without any notice to the subject.

  > **Note** Because smart cards must prompt the user for their PIN, this option must be selected when a smart card CSP is selected.

- **Limit the number of CSPs for an auto-enrollment certificate template** If more than one smart card CSP is selected on the Request Handling tab (Figure 2), users may receive more than one dialog box when a Windows XP client retrieves the auto-enrolled certificate and begins to install it on the smart card. It is recommended that only one CSP be selected from this list for each template.
- **Do not enable subject creation based on request information** If the Supply in the request option is enabled on the Subject Name tab (Figure 3), auto-enrollment is disabled. This is because enabling the option prompts the subject to interactively create the subject name in the request, which will not work with auto-enrollment.
- **Do not require more than one authorized signature for issuance** Configuring more than one authorized signature in the Issuance Requirements tab (Figure 4) of the desired certificate template disables subject auto-enrollment based on this template. If the authorized signatures value is set to one, the requestor must sign the request with a private key from a valid certificate in their certificate store. This certificate must contain the application and/or issuance policies specified in the Application policy and Issuance policies lists on the same tab. If an appropriate certificate exists in the requestor's certificate store, auto-enrollment signs the request with this certificate's private key and will obtain and install the requested certificate automatically. For example, to increase the security for EFS certificate distribution, you can create a custom version 2 certificate template that requires the existence of the Smart Card Logon OID (1.3.6.1.4.1.311.20.2.2) in the signing certificate's Application policy.
- On the Issuance Requirements tab (Figure 4) of the desired certificate template, the Valid existing certificate option may affect subject auto-enrollment. This option tells the CA that the subject does not need to meet issuance requirements when renewing a valid certificate. Subjects who may have been unable to auto-enroll for the initial certificate may be able to use auto-enrollment to renew that certificate. For example, a user whose distinguished name has changed may still auto-enroll a certificate based on an existing valid certificate, rather than on their new credentials.

  > **Note** For more information on configuring auto-enrollment, see the Certificate Autoenrollment in Windows XP white paper at http://www.microsoft.com/WindowsXP/pro/techinfo/administration/autoenroll/default.asp

Delegating Template Management

You can delegate the ability to manage individual certificate templates or to create any certificate templates by defining appropriate permissions to global groups or universal groups that a user belongs to.

To delegate modification of a specific certificate template, assign a global or universal group the Read and Write permissions on the Security tab (Figure 8) of the certificate template. If you also wish to delegate administration permissions to the security groups, assign Full Control permissions so that the security group can modify the DACL for the certificate template.

To delegate the ability to create certificate templates to users who are not members of the Domain Admins group in the forest root domain, or members of the Enterprise Admins group, it is necessary to define the appropriate permissions in the Configuration naming context of the Active Directory.

To delegate the administration of all certificate templates, including the ability to duplicate and create new certificate temples, you must make the following permission assignments to a global or universal group that the user is a member of:

- CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRoot* container = Full Control permissions
- Full Control permissions to every certificate template in the CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRoot* container. The permissions assigned to the Certificate Templates container are not inherited by the individual Certificate Templates.
- Full control permissions to the CN=OID,CN=Public Key Services,CN=Services,CN=Configuration,DC= *ForestRoot* container.

> **Note** To create or duplicate existing certificate templates, users only need the Create Child permission for the CN= Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC=*ForestRoot* and CN=OID, CN=Public Key Services,CN=Services,CN=Configuration,DC= *ForestRoot* containers.

Planning Considerations

This section looks at the topics that must be considered when planning all aspects of version 2 certificate templates. The section provides design guidelines for the creation of certificate templates and best practices to implement when working with certificate templates.

Design Guidelines

When creating a version 2 certificate template, consider the following design guidelines:

- **Defining the subject name** The holder of the private key associated with a certificate is known as the *subject*. This can be a user, a computer, a program, or virtually any object or service. Because the subject can vary greatly depending on who or what it is, you need some flexibility when providing the subject name in the certificate request. A Windows Server 2003 CA can either build the subject name automatically or request it from the subject. If it automatically provides the subject name, it obtains the information from Active Directory. You can configure this process to include or exclude information that is useful in the environment. If it is configured to manually provide the subject name, the subject supplies that information in the certificate request using the Web-based enrollment pages.
- **Defining the certificate lifetime** Certificate-based cryptography uses public-key cryptography to protect and digitally sign data. Over time, it is theoretically possible to collect data protected with the public key and attempt to derive the private key from it. Given enough time and resources, this private key could be compromised, effectively rendering all protected data unprotected. Because certificates can be compromised over time, a finite certificate lifetime should be established.
- **Determining certificate usage** It is possible to issue many specific certificates that can only be used for a single purpose or to issue fewer certificates that have broad usage. This decision depends on the environment, the level of administration desired, and the possible effects on the subjects, as well as the effects of multiple certificates on applications that will use them.

  One strategy of certificate administration creates a number of granular templates—one for each job function, such as file encryption or code signing. Subjects can then enroll for each certificate as needed for the appropriate function. This allows subjects to start with few certificates and only obtain new certificates that they need over time. The drawback to this strategy is that the subject may end up with a large number of certificates and private keys that become harder to manage over time.

  Alternatively, you could create a few broad certificate templates that encompass job functions for most common groups of subjects. For example, if most employees use their certificates for mail signing and encryption as well as file encryption, create one template that allows all those functions in the same certificate. This allows most subjects to obtain a single, all-purpose certificate. The drawback to this strategy is that there is no granular control of the usage of the certificates. The administrator cannot decide that subgroups cannot encrypt mail without modifying the template or changing the strategy.

- **Determining which CSP to implement** A version 2 certificate template allows you to define one or more cryptographic service providers (CSPs) as usable by a template. This allows the administrator to control what types of cryptography subjects can use within an enterprise. This is very useful when security is of paramount importance. Because subjects use the CSP for both portions of any cryptographic service—either encryption and decryption or signing and confirming signature—it is necessary to ensure that all subjects can use the same CSP. The easiest way to do this is to configure each certificate template to identify exactly one CSP. Which CSP should be identified is up to the administrator and depends on the level of security required, the intended purposes of the certificate, and the presence of security hardware, such as smart cards.
- **Determining key length** Each CSP provides one or more cryptographic algorithms for encryption or digital signature. You can define a minimum key size allowed for a certificate template. In general, larger keys provide more protection over shorter keys for the same algorithm, but larger keys take longer to generate and use. You should select a minimum key size that ensures the necessary amount of protection without affecting performance.
- **Determining smart card usage** Each type of smart card has at least one associated CSP that must be implemented by the certificate template to allow the smart card to be used. If the correct smart card CSP is not associated with the template, the smart card will not be recognized and the template will fail. Ensure that you enable all smart card CSPs for the smart cards deployed in your environment within the certificate template.
- **Planning deployment methods** Certificates are typically deployed manually or automatically. Manual enrollment can take place using either the Web enrollment pages, the Certificates MMC console, or through CryptoAPI or CAPICOM programming interfaces. Auto-enrollment requires the configuration described in the Auto-Enrollment Considerations section.
- **Planning Key Archival** Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition CAs can provide key archival of private keys. When planning key archival settings for a certificate template, consider the following settings:
  - **Enabling archival of the subject's private key** This option is only available when the issuing CA is running Windows Server 2003, Enterprise Edition or Windows Server 2003, Datacenter Edition, and the CA is configured for key archival.
  - **Define whether the private key can be exported** If this option is enabled, the subject can export the private key for backup purposes or move the private key and certificate to another computer. If key archival is centralized, you may not want to enable this option because it allows the key to be recovered in a decentralized manner.

Best Practices

When planning certificate template deployment, use the following best practices:

- Do not delete the Certificate Publishers security group.

  The Certificate Publishers security group contains each certification authority's computer account and is used when publishing certificate templates to Active Directory. If this group is removed, the certification authority may not publish certificates to Active Directory correctly. To avoid this, the group should not be deleted and its membership should not be modified.

- Add the CA machine accounts to every Cert Publishers group.

  The Cert Publishers group is a domain local group that exists in every domain in the forest. In each domain, all CA computer accounts should be added to the Cert Publishers group.

- Do not exceed the certificate lifetime of the issuing certification authority.

  Certificate lifetimes work as a subset of the certification authority's (CA) certificate lifetime. All certificates, including the CA certificate, have an expiration date after which they are no longer valid. As a result, a certificate cannot be issued with a lifetime that exceeds the lifetime of the issuing CA. Issuing such a certificate would allow it to be valid for longer than the issuing CA certificate, which violates certificate chaining rules. A CA will therefore continue to issue certificates until the CA's certificate expires or until the requested template's renewal period is greater than the CA's certificate remaining lifetime. If a certificate template requires a lifetime greater than the lifetime of the CA certificate, the validity period of the issued certificate is truncated to the amount of time left in the lifetime of the CA certificate.

- Plan certificate templates before deployment.

  Certificates can be issued to subjects in many ways, including manual enrollment, auto-enrollment, and Web enrollment. In addition, there are many certificate strategies including issuing one all-inclusive certificate to all subjects and issuing several application-specific certificates to subjects as needed. Because there are so many options, planning should be done well in advance of certificate deployment.

- Upgrade the certificate templates in Active Directory before upgrading from Windows 2000.

  Windows Server 2003, Enterprise Edition and Windows Server 2003, Datacenter Edition certification authorities use newer versions of certificate templates than those used by Windows 2000 CAs. These templates must be upgraded before the certification authorities are upgraded to ensure proper operation.

- Duplicate new templates from existing templates closest in function to the intended template.

  New certificate templates are duplicated from existing templates. Many settings are copied from the original template. Because of this, duplicating one template to another of a totally different type may carry over some unintended settings. When duplicating a template, examine the subject type of the original template and ensure that you duplicate one that has a similar function to that of the intended template. Although most settings for certificate templates can be edited once the template is duplicated, the subject type cannot be changed.

- Determine publication points for certificate templates.

  Determine which CAs will issue specific certificate templates based on both the administration model implemented by the organization and the usage of the certificate template. For example, if the administration model is a project-based management model, it would be appropriate to only assign the certificate template to CAs associated with the project. On the other hand, if the certificate template is widely used throughout the organization, it may be appropriate to have all CAs issue the certificate template to provide fault tolerance if a CA is unavailable.

- Minimize the number of issued certificates.

  Consider using multi-purpose certificates that can be used for more than one job task rather than issuing separate certificates for each job task that must be performed. This reduces the number of issued certificates and reduces the complexity when a user must select which certificate to present to an application.

Walkthroughs

Creating a Version 2 Certificate Template

To create a new version 2 certificate template

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click an existing certificate that will serve as the starting point for the new certificate, and then click Duplicate Template.
4. On the General tab, enter the Template display name and the template name, and then click OK.
5. Define any additional attributes for the newly created version 2 certificate template.

Defining Application and Issuance Policies

When you create a version 2 certificate template, you can define which application and issuance policies are included in the issued certificates. Defining application and issuance policies requires the completion of three tasks:

- Acquiring Object Identifiers for the application and issuance policies
- Defining the application and issuance policies

- Mapping issuance policies between PKI hierarchies

Acquiring Object Identifiers

If you define a custom application policy or issuance policy, you must obtain an object identifier for the policy.

To acquire an object identifier

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task as described in the Delegating Template Management section.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template you wish to modify, and then click Properties.
4. On the Extensions tab, click Application Policies, and then click Edit.
5. In the Edit Application Policies Extension dialog box, click Add.
6. In Add Application Policy, ensure that the application you are creating does not exist, and then click New.
7. In the New Application Policy dialog box, provide the name for the new application policy, note the generated OID, and then click OK.

> **Note** You could also add new object identifiers by editing Certificate Policies rather than Application Policies.

Establishing Application Policies

Once you have defined any custom application policies, you can then associate the application policy with the certificate template using the following procedure:

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click Properties.
4. On the Extensions tab, click Application Policies, and then click Edit.
5. In Edit Application Policies Extension, click Add.
6. In Add Application Policy, click the desired application policy, and then click OK.

Establishing issuance Policies

Once you have defined any custom issuance policies, you can then associate the issuance policy with the certificate template using the following procedure:

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click Properties.
4. On the Extensions tab, click Certificate Policies, and then click Edit.
5. In Edit Issuance Policies Extension, click Add.
6. In Add Issuance Policy, click New.
7. Provide the requested information.

Mapping Issuance Policies between PKI Hierarchies

When performing qualified subordination, it may be necessary to associate issuance policies in your organization with issuance policies defined in another organization. The policy mappings are defined in the policy.inf file used to generate the Cross-Certification Authority certificate.

In the policy.inf file, you must include a [PolicyMappingsExtension] that maps the policies listed in the policy.inf file with policies defined in the other PKI hierarchy. The following code example shows a section of a policy.inf file that maps issuance policies for high, medium, and low assurance between two organizations.

```
[PolicyStatementExtension]
Policies = HighAssurancePolicy, MediumAssurancePolicy, LowAssurancePolicy
CRITICAL = FALSE

[HighAssurancePolicy]
OID = 1.3.6.1.4.1.311.21.8.256.257.258.259.1.402

[MediumAssurancePolicy]
OID = 1.3.6.1.4.1.311.21.8.256.257.258.259.1.401

[LowAssurancePolicy]
OID = 1.3.6.1.4.1.311.21.8.256.257.258.259.1.400

[PolicyMappingsExtension]
1.3.6.1.4.1.311.21.8.256.257.258.259.1.400 =
1.3.6.1.4.1.311.21.8.354.232.582.111.1.400
1.3.6.1.4.1.311.21.8.256.257.258.259.1.401 =
1.3.6.1.4.1.311.21.8.354.232.582.111.1.401
1.3.6.1.4.1.311.21.8.256.257.258.259.1.402 =
1.3.6.1.4.1.311.21.8.354.232.582.111.1.402
critical = yEs
```

This example maps the OIDs for the high assurance, medium assurance, and low assurance policies to OIDs that exist in the other organization's PKI. The other organization must define a policy.inf file that maps the OIDs in the opposite direction so that the OIDs are recognized by both organizations.

Configuring Permissions for a Certificate Template

This section explains how to define permissions for specific certificate templates and also for delegating permission for the management of certificate templates.

Allowing for Enrollment

To define permissions to allow a specific security principal to enroll for certificates based on a certificate template

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click Properties.
4. On the Security tab, ensure that Authenticated users is assigned Read permissions.

   This ensures that all authenticated users on the network can see the certificate templates.
5. On the Security tab, click Add. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and then click OK.
6. On the Security tab, select the newly added security group, and then assign Allow permissions for the Read and Enroll permissions.
7. Click OK.

Allowing for Auto-Enrollment

To define permissions to allow a specific security principal to auto-enroll for certificates based on a certificate template

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click Properties.

4. On the Security tab, click Add. Add a global group or universal group that contains all security principals requiring Enroll permissions for the certificate template, and then click OK.
5. On the Security tab, select the newly added security group, and then assign Allow permissions for the Read, Enroll, and Auto-enroll permissions.
6. Click Apply.

> **Note** For more information on configuring certificate auto-enrollment, see the Certificate Autoenrollment in Windows XP white paper at http://www.microsoft.com/WindowsXP/pro/techinfo/administration/autoenroll/default.asp

Allowing Creation and Modification of any Certificate Template

To delegate administration of all templates (which includes the ability to duplicate and create new templates)

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the ADSIEdit console (Adsiedit.msc).
3. In the console tree, right-click ADSI Edit, and then click Connect to.
4. In the Connection dialog box, in the Connection Point section, click Naming Context, select Configuration Container from the list below Naming Context, and then click OK.
5. In the console tree, expand ADSI Edit.
6. In the console tree, expand Configuration Container.
7. In the console tree, expand CN=Configuration,DC=*ForestRootDomain* (where *ForestRootDomain* is the LDAP distinguished name of your forest root domain).
8. In the console tree, expand CN=Services.
9. In the console tree, expand CN=Public Key Services.
10. In the console tree, right-click CN=Certificate Templates, and then click Properties.
11. In the CN=Certificate Templates Properties dialog box, on the Security tab, click Add. Add a global or universal group that contains the users you wish to delegate certificate creation and management permissions to, and then click OK.
12. On the Security tab, select the newly added security group, ensure that the security group is assigned Allow permissions for the Full Control permission, and then click OK.
13. In the console tree, right-click CN=OID, and then click Properties.
14. In the CN=OID Properties dialog box, on the Security tab, click Add. Add a global or universal group that contains the users you wish to delegate certificate creation and management permissions to, and then click OK.
15. On the Security tab, select the newly added security group, ensure that the security group is assigned Allow permissions for the Full Control permission, and then click OK.
16. Close ADSI Edit.
17. Ensure that the security group assigned full control permissions to the CN=Certificate Templates and CN=OID containers is also assigned full control permissions for all certificate templates listed in the Certificate Templates MMC console (Certtmpl.msc).

Publishing a Certificate Template

To define which certificate templates are issued by a Certification Authority

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. From Administrative Tools, open the Certification Authority MMC console.
3. In the console tree, expand *CAName* (where *CAName* is the name of your Enterprise CA).
4. In the console tree, select the Certificate Templates container.

> **Note** If working with a Windows 2000 CA, the container is named Policy Settings.

5. Right-click Certificate Templates, and then click New, Certificate Template to Issue.

6. In the Enable Certificate Templates dialog box, select the certificate template(s) you wish the CA to issue, and then click OK.

> **Note** If a certificate template is not listed in the Enable Certificate Templates dialog box, the CA is either already configured to issue the certificate template, or replication of the certificate template is not completed to all domain controllers in the forest.

The newly selected certificate template(s) will appear in the details pane.

Removing a Certificate Template from a CA

Removing a certificate template only unlinks a certificate from a CA instead of deleting it physically from the certificate template store.

To remove a certificate template from the certificate templates currently issued by a Certification Authority

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. From Administrative Tools, open the Certification Authority MMC console.
3. In the console tree, expand *CAName* (where *CAName* is the name of your Enterprise CA).
4. In the console tree, select the Certificate Templates container.

> **Note** If working with a Windows 2000 CA, the container is named Policy Settings.

5. In the details pane, right-click the certificate template you wish to remove from the CA, and then click Delete.
6. In the Disable Certificate Templates dialog box, click Yes.

The certificate template no longer appears in the details pane.

Replace an Existing Certificate Template with a New Certificate Template

This process, also referred to as superseding an existing template, defines which existing templates a version 2 certificate is replacing.

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template you want to change, and then click Properties.
4. Click the Superseded Templates tab.
5. Click Add.
6. Click one or more templates to supersede, and then click OK.

Re-Enroll Certificate Holders

If you make modifications to a certificate template that you wish implemented immediately for all existing certificate holders, you can force re-enrollment by using the following procedure:

1. Log on as a member of the Enterprise Admins or the forest root domain's Domain Admins group, or as a user who has been granted permission to perform this task.
2. Open the Certificate Templates MMC console (Certtmpl.msc).
3. In the details pane, right-click the certificate template that you wish to re-enroll for all certificate holders, and then click Reenroll all Certificate Holders.

Appendix A: Wireless Certificates

Windows XP introduced native support for 802.1x and wireless networks. To enable strong security, both users and machines need authentication certificates to authenticate to a RADIUS (IAS Server) authorization point. Windows 2000 Certificate Authorities support 802.1x certificate requirements for machines with the version 1 "Machine" certificate template and user certificates with any of the certificate templates that contain the Client Authentication EKU. If version 2 templates are used for machine auto-enrollment, it is important to configure the certificate template properly. When the "Machine" template is cloned to a version 2 template, the administrator MUST ensure that the DNS name is included in the subject name (CN) of the certificate. The Windows XP wireless client requires the DNS name of the machine to be contained in the subject for proper usage and authentication to the IAS server (RADIUS).

> **Important** If the DNS fully qualified domain name is longer than 64 characters, the name will be truncated during certificate enrollment and the name will be invalid for wireless authentication.

For more information, see the white paper at http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/default.asp

Appendix B: References

- Troubleshooting Certificate Status and Revocation
  http://www.microsoft.com/TechNet/security/prodtech/pubkey/tshtcrl.asp
- Certificate Autoenrollment in Windows XP
  http://www.microsoft.com/WindowsXP/pro/techinfo/administration/autoenroll/default.asp
- PKI Enhancements in Windows XP Professional and Windows Server 2003
  http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp
- Data Protection and Recovery in Windows XP
  http://www.microsoft.com/windowsxp/pro/techinfo/administration/recovery/default.asp
- Windows Server 2003, Enterprise Edition Help documentation

Appendix C: Certificate Template Schema Additions

The Certificate Templates container contains the certificate templates that are defined within an Active Directory forest. Each certificate template is of the class pKICertificate. Each Certificate Template is managed by using the Certificate Templates MMC snap-in. Windows 2000 includes 24 default certificate templates; Windows Server 2003 includes 29 default templates. Each template is stored in the following location in the Configuration naming context:

> CN=<name of template>,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configuration,DC= *ForestRootDomain*

Version 1 Certificate Template Attributes

The following version 1 certificate templates attributes are defined in the Active Directory schema.

Attribute	Description
Cn	Common name of the certificate type.
distinguishedName	Distinguished name of the certificate type.
displayName	Display name of a cert type.
pKIExtendedKeyUsage	Array of extended key usage OIDs.
pKIDefaultCSPs	Default CSP list. DWORD, CSP name.
pKICriticalExtensions	List of critical extensions.
revision	Major version of the templates.
templateDescription	Obsolete attribute.
flags	General enrollment flags.
pKIDefaultKeySpec	Specifications of the Default Key length and construct.
NTSecurityDescriptor	Security Descriptor name.
pKIKeyUsage	Key Usage extension.
pKIMaxIssuingDepth	Basic Constraints. DWORD value.

pKIExpirationPeriod	Validity period. Negative FILETIME value.
pKIOverlapPeriod	Renewal period. Negative FILETIME value.

Version 2 Certificate Template Attributes

The following version 2 certificate templates attributes are defined in the Active Directory schema.

Attribute	Description
msPKI-Template-Schema-Version	Schema version of the templates.
msPKI-Template-Minor-Revision	Minor version of the templates.
msPKI-RA-Signature	Number of RA signatures required on a request referencing this template.
msPKI-Minimal-Key-Size	Minimal key size required.
msPKI-Template-Cert-Template-OID	OID of this template.
msPKI-Supersede-Templates	Name of the template that this template supersedes.
msPKI-RA-Policies	RA issuer policy OIDs required.
msPKI-RA-Application-Policies	RA application policy OIDs required.
msPKI-Certificate-Policy	The certificate issuer policy OIDs are placed in the OID_CERT_POLICIES extension by the policy module.
msPKI-Certificate-Application-Policy	Certificate application policy OIDs.
msPKI-Enrollment-Flag	Enrollment flags.
msPKI-Private-Key-Flag	Private key flags.
msPKI-Certificate-Name-Flag	Subject name flags.

Flags

The following enrollment flags are defined in the Active Directory schema.

Flag	Description
CT_FLAG_INCLUDE_SYMMETRIC_ALGORITHMS • **0x00000001**	Include the S/MIME symmetric algorithms in the requests.
CT_FLAG_PEND_ALL_REQUESTS • **0x00000002**	All certificate requests are pended.
CT_FLAG_PUBLISH_TO_KRA_CONTAINER • **0x00000004**	Publish the certificate to the KRA (key recovery agent container) in Active Directory.
CT_FLAG_PUBLISH_TO_DS • **0x00000008**	Publish the resultant certificate to the userCertificate property on the user object in Active Directory.
CT_FLAG_AUTO_ENROLLMENT_CHECK_USER_DS_CERTIFICATE • **0x00000010**	The Auto-enrollment client will not enroll for a new certificate if the user has a certificate previously published to the userCertificate attribute in Active Directory with the same template

	name.
CT_FLAG_AUTO_ENROLLMENT • **0x00000020**	This cert is appropriate for auto-enrollment.
CT_FLAG_PREVIOUS_APPROVAL_VALIDATE_REENROLLMENT • **0x00000040**	A previously issued certificate will valid subsequent enrollment requests.
CT_FLAG_DOMAIN_AUTHENTICATION_NOT_REQUIRED • **0x00000080**	Obsolete.
CT_FLAG_USER_INTERACTION_REQUIRED • **0x00000100**	User interaction is required to enroll using auto-enrollment.
CT_FLAG_ADD_TEMPLATE_NAME • **0x00000200**	Obsolete.
CT_FLAG_REMOVE_INVALID_CERTIFICATE_FROM_PERSONAL_STORE • **0x00000400**	Remove invalid (expired or revoked) certificate from personal store on the local client machine during auto-enrollment.

The following subject name flags are defined in the Active Directory schema.

Flag	Description
CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT • **0x00000001**	The enrolling application must supply the subject name.
CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT_ALT_NAME • **0x00010000**	The enrolling application must supply the subjectAltName in request.
CT_FLAG_SUBJECT_REQUIRE_DIRECTORY_PATH • **0x80000000**	Subject name should be full DN (distinguished name) based on the Active Directory path.
CT_FLAG_SUBJECT_REQUIRE_COMMON_NAME • **0x40000000**	Subject name should be the common name.
CT_FLAG_SUBJECT_REQUIRE_EMAIL • **0x20000000**	Subject name includes the e-mail name.
CT_FLAG_SUBJECT_REQUIRE_DNS_AS_CN • **0x10000000**	Subject name includes the DNS name as the common name.
CT_FLAG_SUBJECT_ALT_REQUIRE_DNS • **0x08000000**	Subject alt name includes the DNS name.
CT_FLAG_SUBJECT_ALT_REQUIRE_EMAIL • **0x04000000**	Subject alt name includes the e-mail name.
CT_FLAG_SUBJECT_ALT_REQUIRE_UPN • **0x02000000**	Subject alt name requires UPN.
CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID • **0x01000000**	Subject alt name requires directory GUID (used by domain controllers).
CT_FLAG_SUBJECT_ALT_REQUIRE_SPN • **0x00800000**	Subject alt name requires SPN (service principal name).

CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID • **0x01000000**	Subject alt name requires directory GUID.
CT_FLAG_SUBJECT_ALT_REQUIRE_SPN • **0x00800000**	Subject alt name requires SPN.

The following template private key flags are defined in the Active Directory schema.

Flag	Description
- Private Key Flags	
CT_FLAG_ALLOW_PRIVATE_KEY_ARCHIVAL • 0x00000001	Archival of the private key is allowed/required.
CT_FLAG_EXPORTABLE_KEY • 0x00000010	Mark the private key as exportable.

The following template general flags are defined in the Active Directory schema:

Flag	Description
CT_FLAG_MACHINE_TYPE • 0x00000040	Machine cert type.
CT_FLAG_IS_CA • 0x00000080	CA certificate type.
CT_FLAG_IS_CROSS_CA • 0x00000800	Cross-CA certificate type.
CT_FLAG_IS_DEFAULT • 0x00010000	Default cert type that is set on all V1 templates that cannot be changed.
CT_FLAG_IS_MODIFIED • 0x00020000	The type has been modified (read only).
CT_MASK_SETTABLE_FLAGS • 0x0000ffff	Obsolete.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

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

Other product and company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation · One Microsoft Way · Redmond, WA 98052-6399 · USA

Contact Us | **E-mail this Page** | **TechNet Newsletter**