Windows 2000 Server

Chapter 16 - Windows 2000 Certificate Services and Public Key Infrastructure

Microsoft® Windows® 2000 includes both Certificate Services, which is easily administered through the Certification Authority console, a snap-in for Microsoft Management Console (MMC), and a comprehensive public key infrastructure. Understanding the components of Windows 2000 Certificate Services and the public key infrastructure is the starting point for designing, deploying, and maintaining a public key infrastructure that meets all of your public-key security needs.

In This Chapter

Related Information in the Resource Kit

- For more information about the concepts of public key infrastructure and public key technology, see "Cryptography for Network and Information Security" in this book.
- For more information about security solutions that use public key technology, see "Choosing Security Solutions That Use Public Key Technology" in this book.
- For more information about planning and deploying your public key infrastructure, see "Planning Your Public Key Infrastructure" in the *Microsoft® Windows® 2000 Server Resource Kit Deployment Planning Guide.*

Benefits of the Public Key Infrastructure

The Windows 2000 public key infrastructure (also known as a PKI) provides the framework of services, technology, protocols, and standards that enable you to deploy and manage a strong information security system that is based on public key technology. You can deploy your public key infrastructure to support a wide range of network and information security needs.

The Windows 2000 public key infrastructure includes Certificate Services for issuing and managing digital certificates and Microsoft CryptoAPI version 2 for secure cryptographic operations and private key management. The public key infrastructure is fully integrated with the Active Directory™ directory service in Windows 2000, and with distributed security services.

The discussion in this chapter focuses on the individual components and features of the Windows 2000 public key infrastructure. For more information about public key infrastructure and public key technology, see "Cryptography for Network and Information Security" in this book.

Strong Security with Public Key Technology

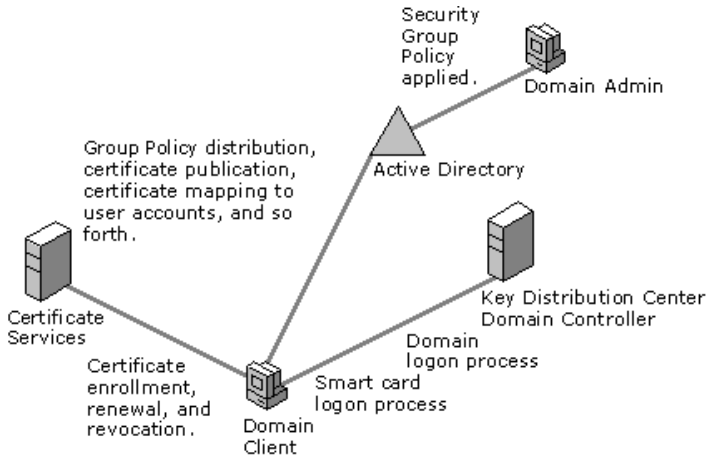
The Windows 2000 public key infrastructure enables you to deploy strong security solutions that use digital certificates and public key technology. Security solutions can include the following:

- Secure mail, which uses certificates and the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol to ensure the integrity, origin, and confidentiality of e-mail messages.
- Secure Web sites, which use certificates and certificate mapping to map certificates to network user accounts for controlling user rights and permissions for Web resources.
- Secure Web communications, which use certificates and the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to authenticate servers, to optionally authenticate clients, and to provide confidential communications between servers and clients.
- Software code signing, which uses certificates and digital signing technology (such as Microsoft® Authenticode®) to ensure the integrity and authorship of software that is developed for distribution on an intranet or on the Internet.
- Smart card logon process, which uses certificates and private keys stored on smart cards to authenticate local and remote access network users.
- Internet Protocol security (IPSec) client authentication, which has the option to use certificates to authenticate clients for IPSec communications.
- Encrypting File System (EFS), which uses certificates for both EFS user and EFS recovery agent operations.
- Custom security solutions, which use certificates to provide confidentiality, integrity, authentication, or nonrepudiation.

For more information about security solutions that use public key technology, see "Choosing Security Solutions That Use Public Key Technology" in this book.

Integration with Active Directory and Distributed Security Services

Windows 2000 Certificate Services form the core of the Windows 2000 public key infrastructure. Enterprise certificate services are integrated with Active Directory and distributed security services, as shown in Figure 16.1.



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

Figure 16.1 Certificate Services in Windows 2000

You can install Windows 2000 Certificate Services to create enterprise certification authorities (CAs) for issuing and managing digital certificates. Active Directory contains information that enterprise CAs require, such as user account names, security group memberships, and certificate templates. Active Directory also contains information about each enterprise CA that is installed in the domain. Certificate requests are usually sent to enterprise CAs that process the requests to either deny or approve them. Issued certificates are distributed to Active Directory and to the requestor's computers. CAs also publish certificate revocation lists to Active Directory.

In addition, Active Directory stores Public Key Group Policy for distribution to all computers that are within the scope of the policy. Public Key Group Policy enables you to control which CAs are to be trusted in the enterprise, to specify alternative EFS recovery agents, and to configure automatic enrollment and renewal of certificates for Windows 2000based computers — all from a central administration point.

Active Directory also supports mapping certificates to network user accounts for authenticating clients and controlling access to network resources. Using smart cards for the user logon process is a special case of certificate mapping that extends the Kerberos v5 authentication protocol to include authentication of users on the basis of certificates and private keys that are stored on smart cards. Using smart cards for the user logon process provides enhanced security for user authentication and a single set of user credentials for logging on locally or remotely over a network.

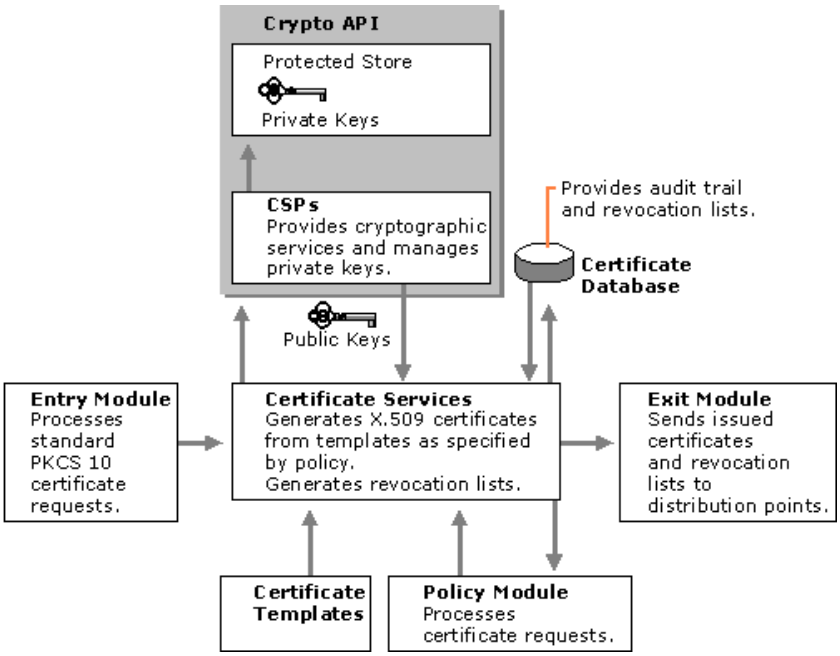
Major Components of the Public Key Infrastructure

The major components of the Windows 2000 public key infrastructure include the following:

- Windows 2000 Certificate Services for issuing and managing digital certificates.
- Microsoft CryptoAPI and cryptographic service providers (CSPs) for providing cryptographic operations and private key management.
- Certificate stores for storing and managing certificates in the enterprise.

Windows 2000 Certificate Services

Figure 16.2 shows a functional block diagram of Windows 2000 Certificate Services.



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

Figure 16.2 Certificate Services Functional Diagram

The components of Windows 2000 Certificate Services work in conjunction with Microsoft CryptoAPI and cryptographic service providers (CSPs) to perform a variety of tasks, including the following:

- Process certificate requests (entry module).
- Verify whether requestors are qualified to receive certificates (policy module).
- Create and issue certificates for qualified requestors (Certificate Services engine).
- Generate a private key and distribute it to the requestor's protected store (CSPs and Microsoft CryptoAPI).
- Manage the private key for all cryptography operations (CSPs and Microsoft CryptoAPI).
- Distribute the certificates that are issued to qualified requestors and, optionally, publish certificates to Web pages, public folders, or Active Directory (exit module).
- Publish periodic certificate revocation lists to Active Directory and, optionally, to Web pages or public folders (exit module).
- Store all certificate transactions for the audit trail (certificate database).

  Note In Windows 2000, all cryptographic functions and private key management are performed by Microsoft CryptoAPI in conjunction with CSPs. Any system service or application can request cryptographic services by using Microsoft CryptoAPI.

Entry Module

The default entry module processes standard PKCS (Public Key Cryptography Standards) 10 certificate requests made through remote procedure calls (RPCs) or the Hypertext Transfer Protocol (HTTP). The entry module is a dynamic-link library (DLL) that cannot be customized. Windows 2000 services usually use RPCs to submit certificate requests to enterprise CAs. However, the Web Enrollment Support pages use Hypertext Transfer Protocol (HTTP) to submit certificate requests to CAs.

Certificate requests to Certificate Services are placed in a pending queue until they are approved or denied by the policy module.

Note You can develop custom certificate enrollment applications that submit RPC or HTTP requests to Certificate Services. For more information about developing custom applications for Windows 2000 Certificate Services and about the required certificate request format, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Policy Modules

The policy module determines whether a certificate request must be approved, denied, or queued (left pending) for a later decision by the administrator about whether or not to issue the certificate. Windows 2000 Certificate Services includes a default policy module that incorporates CA policy for both enterprise and stand-alone CAs. You can also build custom policy modules for special needs.

Enterprise CA Policy Enterprise CA policy always issues a certificate or denies a request immediately. Enterprise CA policy uses Active Directory to determine the identity of the requester, and then automatically determines whether the requester has security permissions to receive a certificate of the type that is being requested.

Stand-alone CA Policy By default, stand-alone CA policy sends certificate requests to a pending queue so that an administrator can approve or deny them. You have the option of setting stand-alone CA policy to automatically approve all certificate requests. However, because a stand-alone CA does not verify the identity of requesters who are using Active Directory, there is no way to verify the identity and validity of the certificate requester automatically. Therefore, setting a stand-alone CA to approve certificate requests automatically can pose a significant security risk.

Custom Policy Modules The policy module is a fully customizable DLL. For more information about how to customize policy modules, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources . You can change the installed policy module by using the Certification Authority console. You can also develop your own policy modules or acquire a third-party policy module when one is available.

Note It is recommended that you use custom policy modules with stand-alone CAs only. Enterprise CAs require the enterprise policy module to ensure proper integration with Active Directory. Using a custom policy module with an enterprise CA can produce both problems and unpredictable results.

When Certificate Services determines whether to grant certificate requests, the policy module can check information in the request against various sources for verification, such as a directory service, an external legacy database, or credit information from an outside authority. The policy module also can send alerts to the appropriate administrator if manual (offline) approval of the request is required.

The policy module can insert additional certificate attributes or extensions that might be required by a client application. For example, information such as a job title and a signing limit into certificates can be inserted and used by an online purchasing form to determine whether the user can sign for the amount requested.

The policy module can use additional information included in the certificate request to incorporate requested attributes in the issued certificate. For example, certificate requests to stand-alone CAs must include all information about the requested certificate; so the policy module incorporates this information into each certificate that is issued. However, enterprise CAs use certificate templates to specify certificate attributes; so certificate requests to enterprise CAs require less information.

Certificate Templates

For enterprise CAs, certificate templates define the attributes for certificate types. You can configure enterprise CAs to issue specific certificate types to authorized users and computers. When a CA creates a certificate, the certificate template is used to specify its attributes, such as the authorized uses for the certificate, the cryptographic algorithms that are to be used with it, the public key length, and the certificate lifetime. Certificate templates are stored in Active Directory and provide information for each of the certificate types that are listed in Table 16.1.

Table 16.1 Certificate Types for Enterprise CAs

Certificate Type	Purpose of the Issued Certificate
Administrator	Used for authenticating clients and for EFS, secure mail, certificate trust list (CTL) signing, and code signing.
Authenticated Session	Used for authenticating clients.
Basic EFS	Used for EFS operations.
CEP Encryption (offline request)	Used to enroll Cisco Systems, Inc. routers for IPSec authentication certificates from a Windows 2000 CA.
Code Signing	Used for code signing operations.
Computer	Used for authenticating clients and servers.
Domain Controller	Used for authenticating domain controllers. When an enterprise CA is installed, this certificate type is installed automatically on domain controllers to support the public key operations that are required when domain controllers are supporting Certificate Services.
EFS Recovery Agent	Used for EFS encrypted-data recovery operations.
Enrollment Agent	Used for authenticating administrators that request certificates on behalf of smart card users.
Enrollment Agent (computer)	Used for authenticating services that request certificates on behalf of other computers.
Exchange Enrollment Agent (offline request)	Used for authenticating Microsoft® Exchange Server administrators that request certificates on behalf of secure mail users.
Exchange Signature Only (offline request)	Used by Exchange Server for client authentication and secure mail (used for signing only).
Exchange User (offline request)	Used by Exchange Server for client authentication and secure mail (used for both signing and confidentiality of mail).
IPSec	Used for IPSec authentication.
IPSec (offline request)	Used for IPSec authentication.
Root Certification Authority	Used for root CA installation operations. (This certificate template cannot be issued from a CA and is used only when installing root CAs.)

Router (offline request)	Used for authentication of routers.
Smart Card Logon	Used for client authentication and logging on with a smart card.
Smart Card User	Used for client authentication, secure mail, and logging on with a smart card.
Subordinate Certification Authority (offline request)	Used to issue certificates for subordinate CAs.
Trust List Signing	Used to sign CTLs.
User	Used for client authentication, EFS, and secure mail (used for both signing and confidentiality of mail).
User Signature Only	Used for client authentication and secure mail (used for signing only).
Web Server (offline request)	Used for Web server authentication.

Many certificate templates are provided for online requests from enterprise CAs. Online certificate templates are used to issue certificates to requestors that have Windows 2000 accounts and that support obtaining certificates directly from an enterprise CA. Certificate templates for offline requests are used to issue certificates to requestors that do not have Windows 2000 accounts or that do not support obtaining certificates directly from an enterprise CA. When a certificate is issued for online requests, identification information about the requestor is obtained from the requestor's Windows 2000 user account for inclusion in the certificates that are issued. Offline requests must include the requestor's identification information in the certificate request when the request is submitted. When you use the Certificate Services Web Enrollment Support pages to request offline certificates from an enterprise CA, enter the identification information (name, e-mail address, department, and so forth), in the Web form before you submit the request to the CA.

For example, you might use the Web Enrollment Support pages to obtain a Web Server certificate for a third-party Web server, and then install the certificate on the appropriate server computer. Likewise, you might obtain an offline IPSec certificate, and then manually install the certificate on a non-Windows 2000 IPSec client. The Subordinate Certification Authority certificate template is an offline template because the identification information for the subordinate CA is entered during the installation process.

An enterprise CA only issues the certificate types that are specified by its certificate issuing policy. By default, Windows 2000 enterprise CAs are installed so that they are ready to issue several types of certificates. You can modify the default configuration by using the Certification Authority console in MMC to specify the types of certificates that are to be issued by each CA.

Stand-alone CAs do not use certificate templates. Therefore, certificate requests to them must include all of the information that is necessary to define the type of certificate that is to be issued. When Windows 2000 services submit certificate requests to stand-alone CAs, the requests include the information that is necessary to define the type of certificate that is being requested. You can use the Web Enrollment Support pages for stand-alone CAs to submit certificate requests to stand-alone CAs for a variety of types of certificates.

Certificate Database

The certificate database records all certificate transactions. It tracks all certificate requests and records whether they were granted or denied. It records information for the issued certificate, such as the serial number and expiration date. It provides a complete audit trail for each certificate from request to expiration. It also flags and tracks certificates that are revoked by CA administrators. You can use the Certification Authority console to manage the audit trail.

Because the certificate database is a transaction database, it includes certificate log files, which record all certificate transactions. By default, the certificate database and the certificate log files are installed at the following location:

`<Drive:>\WINNT\System32\CertLog`

where *<Drive:>* is the letter of the disk drive where the CA is installed.

At the time you install the CA, you have the option of choosing another location to install either the database or the logs, including storing the database and log files separately on different drives.

Exit Modules

The exit module packages the issued certificate in the appropriate transport mechanism or protocol and distributes it to the location specified in the request. Certificate requests can specify that the certificate be distributed to Lightweight Directory Access Protocol (LDAP) directory services, file systems, or URLs. An exit module also delivers certificate revocation lists (CRLs) to CRL distribution points.

The default enterprise exit module publishes certificates and CRLs to Active Directory, and the default stand-alone exit module publishes certificates and CRLs to the local file system. However, Windows 2000 Certificate Services supports multiple exit modules and you can use the Certification Authority console to install them for a CA. For example, you can install exit modules that send certificates and CRLs in e-mail messages or send them to public folders on the network. You can also install exit modules that post certificates to legacy open database connectivity (ODBC) databases or to third-party Lightweight Directory Access Protocol (LDAP) directory services.

Like the policy module, the exit module is a DLL and is fully customizable. For more information about customizing exit modules, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources . You can change the installed exit module by using the Certification Authority console. You also can develop your own exit modules or acquire third-party exit modules.

Certification Authority Console

The Certification Authority console is an MMC snap-in that you can use to manage multiple CAs, performing a variety of administrative tasks that include the following:

- Starting and stopping the CA.
- Backing up and restoring the CA.
- Changing exit and policy modules.
- Viewing the CA certificate.
- Installing or reinstalling a CA certificate for the CA.
- Setting security permissions and delegating administrative control for the CA.
- Revoking certificates.
- Viewing or modifying certificate revocation list (CRL) distribution points.
- Scheduling and publishing CRLs.
- Configuring the types of certificates that are to be issued by the CA.
- Viewing information about certificates that have been issued.

- Viewing information about certificates that have been revoked.
- Viewing pending certificate requests.
- Approving or denying pending certificate requests.
- Viewing failed certificate requests.
- Renewing the CA's certificate.

For more information about how to use the Certification Authority console to manage a CA and perform specific administration tasks, see Certificate Services Help.

To add a Certification Authority console to MMC

1. Open MMC.
2. Click **Console**, and then click **Add/Remove Snap-in** or press CTRL+M.

   The **Add/Remove Snap-in** dialog box appears.
3. Click **Add**.

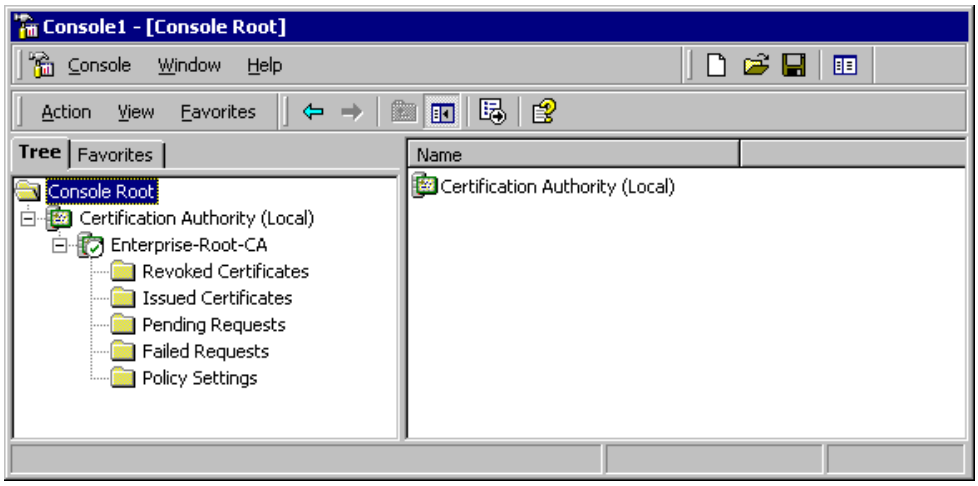
   The **Add Standalone Snap-in** dialog box appears.
4. Select **Certification Authority** from the list of snap-ins, and then click **Add**.

   The **Certification Authority** dialog box appears.
5. Choose one of the following:
   - To manage the CA that is running on the local computer, select the **Local computer** check box, and then click **Finish**.
   - To manage the CA that is running on another computer, select the **Another computer** check box, and then type the domain name of the computer that runs the CA or click **Browse** to select the computer from a list. Then click **Finish**.

   You can click **Add** in the **Add Standalone Snap-in** dialog box again to add more Certification Authority consoles.

   The **Add/Remove Snap-in** dialog box displays the snap-ins that you have added and that are to be installed in MMC.
6. When you have finished adding snap-ins, in the **Add Standalone Snap-in** dialog box, click **Close.**
7. In the **Add/Remove Snap-in** dialog box, click **Close**.

Figure 16.3 shows an example of a Certification Authority console that has been added to MMC. This console manages the CA on the local computer.



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

Figure 16.3 Certification Authority Console

The Certification Authority (Local) console node has been expanded to show all of the containers for an enterprise CA named Enterprise-Root-CA. These containers are used as follows:

Revoked Certificates Click this container to show information about all revoked certificates for this CA. To manually publish CRLs, right-click the Local node. Click **All Tasks**, and then click **Publish**. To change the CRL publication schedule, right-click the Local node, and then click **Properties**. To view a certificate, double-click the certificate. Use the dialog boxes that appear to publish the CRL, change the CRL publication schedule, or view the certificate.

Issued Certificates Click this container to show information about all certificates that have been issued by this CA. To revoke a certificate, right-click the certificate, and then click **All Tasks**. Then click **Revoke Certificate**. To view a certificate, double-click the certificate. Use the dialog boxes that appear to revoke or view certificates.

Pending Requests Click this container to show information about all certificates that are pending for this CA. To approve a pending certificate request, click this container, and then right-click the certificate request. Click **All Tasks**, and then click **Issue**. To deny a pending certificate request, click this container and then right-click the certificate request. Click **All Tasks**, and then click **Deny**. Use the dialog box that appears to deny the certificate request.

Failed Requests Click this container to show the information about all certificate requests that have failed. The information in the Request Disposition Message column explains why the request failed.

Policy Settings (Enterprise CAs Only) Select this container to show the types of certificates that the enterprise CA can issue. To remove one of the types of certificates, select the type you want to delete, and then press DELETE. To add another type of certificate, right-click the container. Click **New**, and then click **Certificate to Issue**. Use the dialog box that appears to add the types of certificates that you want to issue.

When you click a container (such as the Failed Requests container), by default, many of the columns that can be displayed in the details pane of the console are hidden.

To change the columns that are displayed in the details pane for a container

1. Right-click the container, click **View,** and then click **Choose Columns**.

   The **Modify Columns** dialog box appears.

2. Use the **Modify Columns** dialog box to add, remove, or change the order in which columns appear, and then click **OK**.

   For more information about how to use the Modify Columns dialog box, see Certificate Services Help.

Microsoft CryptoAPI and Cryptographic Service Providers

Microsoft CryptoAPI provides a secure interface for the cryptographic functionality that is supplied by the installable cryptographic service provider (CSP) modules. CSPs perform all cryptographic operations and manage private keys. CSPs can be implemented in software as well as in hardware. Windows 2000 Certificate Services uses CryptoAPI and CSPs to perform all cryptographic and private key management operations. CryptoAPI and CSP services are available to all services and applications that require cryptographic services. For more information about CryptoAPI and CSPs, see the Microsoft Security Advisor link and the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Hardware and Software Cryptographic Service Providers

CSPs can be software-based, hardware-based, or a combination of both. Hardware-based cryptography and key management is more secure than software-based cryptography and key management because cryptographic operations and private keys are isolated from the operating system. However, hardware-based CSPs (such as smart card CSPs) often store only a limited number of private keys and can take a long time to generate keys.

Software CSPs usually provide more flexibility than hardware CSPs, but at the cost of somewhat less security. Nevertheless, software-based CSPs can provide ample security to meet a wide range of needs. You usually use hardware-based CSPs only for special security applications, such as for logging on with smart cards or for secure Web communications with FORTEZZA Crypto Cards.

Vendors can develop hardware or software CSPs that support a wide range of cryptographic operations and technologies. However, Microsoft must certify and digitally sign all CSPs. CSPs do not work in Windows 2000 unless they have been digitally signed by Microsoft.

Microsoft Cryptographic Service Providers

Windows 2000 includes the following Microsoft CSPs.

Microsoft Base Cryptographic Provider Provides a broad set of basic cryptographic functionality. It is not subject to United States government cryptography export restrictions and can be exported to other countries (subject to general United States export restrictions, as well as the import restrictions of other countries). The Base CSP uses RSA technology, which is licensed from RSA Data Security, Inc.

Microsoft Enhanced Cryptographic Provider Provides the same capabilities as the Microsoft Base Cryptographic Provider, but in addition, provides stronger security by supporting longer key lengths and additional cryptographic algorithms. This CSP is subject to government-imposed cryptography export restrictions and might not be available in your locality. The enhanced CSP also uses RSA technology.

Microsoft DSS Cryptographic Provider Provides data signing and signature verification capability by using the Secure Hash Algorithm (SHA) and Digital Signature Algorithm (DSA). It is not subject to United States government cryptography export restrictions and can be exported to other countries (subject to general United States export restrictions, as well as the import restrictions of other countries).

Microsoft Base DSS and Diffie-Hellman Cryptographic Provider Provides a superset of the DSS Cryptographic Provider and also supports Diffie-Hellman key exchange, hashing (message digests), data signing, and signature verification by using the SHA and DSA algorithms. This CSP is subject to government-imposed export restrictions on cryptography and might not be available in your locality.

Schannel Cryptographic Providers The Microsoft RSA/Schannel Cryptographic Provider, the Microsoft DSS Cryptographic Provider, and the Diffie-Hellman/Schannel Cryptographic Provider offer various cryptographic services that are required for data integrity, session key exchange, and authentication during secure Web communications with the SSL and TLS protocols. These CSPs are not subject to United States government cryptography export restrictions and can be exported to other countries (subject to general United States export restrictions, as well as the import restrictions of other countries).

FIPS 140-1 Level 1 Certification

The Windows 2000 Microsoft CSPs have received the Federal Information Processing Standard (FIPS) 140-1 Level 1 certification by the National Institute of Standards and Technology (NIST). The requirements for FIPS 140-1 Level 1 certification are contained in the FIPS 140-1 publication, which is published by NIST. For more information about how to obtain the FIPS140-1 publication, contact NIST. For more information about FIPS 140-1, see "Choosing Security Solutions That Use Public Key Technology" in this book.

Base vs. Enhanced Cryptographic Service Providers

The Microsoft Base Cryptographic Provider (Base CSP) is provided for export in compliance with United States government export restrictions on cryptography. The Microsoft Enhanced Cryptographic Provider (Enhanced CSP), however, is subject to United States government export restrictions on cryptography and is available only for localities where the export of strong cryptography is permitted. For more information about restrictions on cryptography, see "Cryptography for Network and Information Security" in this book, and see the Microsoft Security Advisor link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Table 16.2 highlights differences between the Base CSP and the Enhanced CSP. The public key lengths shown in the table are the default key lengths.

Table 16.2 Comparison of Microsoft Base CSP and Microsoft Enhanced CSP

Algorithm	Base CSP	Enhanced CSP
RSA public key signature algorithm	Key length: 512 bits.	Key length: 1,024 bits.
RSA public key exchange algorithm	Key length: 512 bits.	Key length: 1,024 bits.
RC2 block encryption algorithm	Key length: 40 bits.	Key length: 128 bits. Salt length: Settable.
RC4 stream encryption algorithm	Key length: 40 bits.	Key length: 128 bits. Salt length: Settable.
DES	Not supported.	Key length: 56 bits.
Triple DES (2-key)	Not supported.	Key length: 112 bits.
Triple DES (3-key)	Not supported.	Key length: 168 bits.

For both the Base CSP and the Enhanced CSP, public keys that are used for digital signatures can be up to 16,384 bits long. However, public keys that are used for key encryption and key exchange (to protect secret keys) are limited to a maximum of 1,024 bits for the Base CSP and 16,384 bits for the Enhanced CSP. In addition, the symmetric keys for the encryption algorithms in the Base CSP are limited to shorter key lengths, resulting in significantly weaker cryptographic security. Overall, the key lengths and the encryption algorithms in the Enhanced CSP provide far stronger cryptographic security.

For both the Base CSP and the Enhanced CSP, public keys used for signing or key exchange can be a minimum of 384 bits long. However, the use of 384-bit public keys is not recommended. The minimum recommended length of public keys is 512 bits; however, public keys of at least 1,024 bits are recommended whenever this is feasible. Signing keys that exceed 1,024 bits in length can produce strong digital signatures. However, because they also can increase the computational load significantly and require large amounts of time to sign data, they also can adversely affect computer performance and, thus, might not be feasible. The default public-key length of the Base CSP is 512 bits, and the default public key length of the Enhanced CSP is 1,024 bits. Windows 2000 Certificate Services usually uses the default public-key lengths of the CSP, unless you choose another key length that is supported by the CSP in advanced options.

The Enhanced CSP is compatible with the Base CSP, except that the CSPs can generate only RC2 or RC4 keys of the default key length. The default symmetric key length for RC2 and RC4 in the Base CSP is 40 bits. The default symmetric length for RC2 and RC4 in the Enhanced CSP is 128 bits. Therefore, the Enhanced CSP cannot create keys with Base CSP–compatible key lengths. However, the Enhanced CSP can import RC2 and RC4 keys of up to 128 bits. Therefore, the Enhanced CSP can import and use 40-bit keys that were generated by using the Base CSP.

Smart Card Cryptographic Service Providers

Windows 2000 includes smart card CSPs from two vendors: Gemplus SCA and Schlumberger Limited. The Gemplus GemSAFE Card CSP and the Schlumberger CSP support cryptographic operations for the Gemplus and Schlumberger PC/SC-compliant smart cards, respectively. Additional smart card CSPs might be developed and certified for use with Windows 2000. For current information about smart card CSPs that are currently available, see the Microsoft Security Advisor link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Cryptography Export Restrictions

CSPs are subject to cryptography export restrictions. Some governments, including the United States government, currently place export restrictions on encryption technology. Other governments also place import restrictions on encryption technology. The availability of CSPs varies according to the export or import restrictions for a specific geographical area.

All Windows 2000 products support a maximum of 40-bit or 56-bit symmetric key encryption and are exportable to most localities worldwide. If you qualify to use and deploy nonexportable cryptography, you can obtain the Encryption Pack compact disc (CD) from Microsoft and use it to convert exportable Windows 2000 products into nonexportable, strong cryptography products. The Microsoft Enhanced Cryptographic Provider for Windows 2000 is available on this CD, which is not exportable.

For more information about the availability of the Encryption Pack CD and current cryptography export policies for Microsoft products, see the Microsoft Security Advisor link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Certificate Stores

In Windows 2000, public-key objects such as certificates, CRLs, and CTLs are stored in certificate stores for use by users, services, and computers. The Windows 2000 certificate stores include physical stores and logical stores.

The *physical certificate stores* are where public-key objects such as certificates, CRLs, and CTLs are physically stored either locally in the system registry of the computer or remotely in Active Directory. Many of the public-key objects in the physical stores are shared among users, services, and computers through the use of logical certificate stores.

Logical certificate stores group certificates together in logical, functional categories for users, computers, and services. Logical certificate stores contain pointers to the physical certificate stores. Use the Certificates console (an MMC snap-in) to manage certificates in certificate stores. Changes to the logical certificate stores are made to the appropriate physical stores that are located in either the system registry or Active Directory. Because you use only the logical certificate store for a user, service, or computer, you neither have to keep track of where the certificates are actually stored, nor do you have to edit the system registry to manage the certificate stores.

The use of logical certificate stores eliminates the necessity of storing duplicates of common public key objects, such as trusted root certificates, CTLs, and CRLs for users, computers, and services. Users and services share many public key policy objects in common with the local computer. The common public-key objects are stored in sections of the registry of the local computer. However, some certificates, CTLs, or CRLs, are issued for use only by an individual service, user, or local computer. Therefore, users, computers, and services also have individual stores that provide a place to store certificates, CTLs, or CRLs that are not shared in common. For example, a user can request and obtain a certificate or a CRL, which appears in the individual's logical store and is physically stored in the user's unique certificate store in the registry. Such individual user certificates and CRLs are not shared with local computers or with services.

In addition, some public-key objects, such as trusted root certificates and CTLs, can be distributed through Public Key Group Policy. Public key objects that are distributed through Group Policy are stored in special areas of the system registry and appear in the logical stores for users, computers, and services. When you use Group Policy, separate CTLs can be created for users and computers. The CTLs for users are not shared with services or the computer. However, the CTLs for computers are shared with users and services.

The logical certificate stores include the following categories for users, computers, and services:

Personal. Contains individual certificates for the user, service, or computer. For example, when an enterprise CA issues you a User certificate, the certificate is installed in the Personal store for your user account.

Trusted Root Certification Authorities. Contains certificates for root CAs. Certificates with a certification path to a root CA certificate are trusted by the computer for all valid purposes of the certificate.

Enterprise Trust. Contains CTLs. Certificates with a certification path to a CTL are trusted by the computer for purposes specified in the CTL.

Intermediate Certification Authorities. Contains certificates for CAs that are not trusted root certificates (for example, certificates of subordinate CAs), but that are required to validate certification paths. This store also contains CRLs for use by the user, service, or computer.

Active Directory User Object. Contains certificates that are published in Active Directory for the user. This store appears in the Certificates console for users only, not for computers or services.

Request. Contains pending or rejected certificate requests. This store appears only in the Certificates console after a certificate request has been made for the user, computer, or service.

SPC. Contains certificates for software publishers that are trusted by the computer. Software that has been digitally signed by publishers with certificates in this store is downloaded without prompting the user. By default, this store is empty. When Microsoft® Internet Explorer downloads software that has been signed by a software publisher for the first time, users are prompted to choose whether they want to trust all software that is signed by this publisher. If a user chooses to trust all software signed by the publisher,

the publisher's software publisher certificate (SPC) is added to the SPC store. This store appears in the Certificates console for the local computer only, not for users or services.

Features of the Public Key Infrastructure

The Windows 2000 public key infrastructure and Windows 2000 Certificate Services include the following key features:

- Certificates console (an MMC snap-in)
- Certification authority trust model
- Windows 2000 enterprise (and stand-alone) certificate authorities
- Certificate life cycle
- Certificate enrollment and renewal methods
- Public Key Group Policy
- Certificate revocation lists
- Preinstalled trusted root CA certificates
- Smart card support
- Certificate mapping
- Roaming profile support

Certificates Console

The Certificates console is an MMC snap-in, which you can use to manage the certificate stores for users, computers, and services.

You can use the Certificates console to perform the following tasks:

- View information about certificates, such as certificate contents and the certification path.
- Import certificates into a certificate store.
- Move certificates between certificate stores.
- Export certificates and, optionally, export private keys (if key export is enabled).
- Delete certificates from certificate stores.
- Request certificates from an enterprise CA for the Personal certificate store.

For more information about how to use the Certificates console to do these tasks, see Certificate Manager Help.

To add a Certificates console to MMC

1. Open MMC.
2. Click **Console**, and then click **Add/Remove Snap-in**.

   – Or –

   Press CTRL+M.

   The **Add/Remove Snap-in** dialog box appears.
3. Click **Add**.

   The **Add Standalone Snap-in** dialog box appears.
4. Select **Certificates** from the list of snap-ins, and then click **Add**.

   The **Certificates Snap-in** dialog box appears.
5. Select one of the following accounts:
   - **My user account**
   - **Service account**
   - **Computer account**

   The Certificates console manages the certificate stores for this account.
6. Click **Next**.

   If you selected **My user account**, the **Add Standalone Snap-in** dialog box appears. You can click **Add** to add another snap-in.

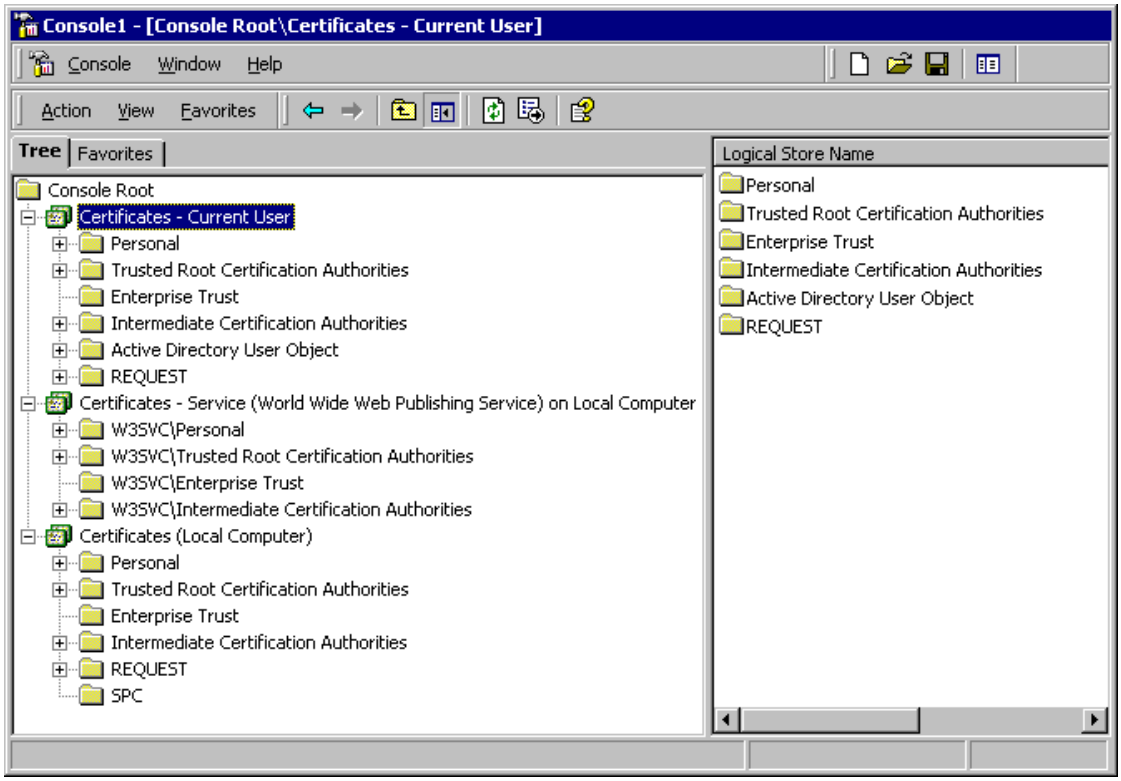
   If you selected **Service account** or **Computer account**, the **Select Computer** dialog box appears. To manage the local computer, click **Next**. To manage another computer, either type the domain name of the computer in **Another computer**, or click **Browse** to select the computer from a list. Then click **Next**.

   If you selected **Computer account**, the **Add Standalone Snap-in** dialog box appears. You can click **Add** to add another snap-in.

   If you selected **Service account**, the **Certificates Snap-in** dialog box appears. Select a service from the **Services account** list, and click **Finish**. When the **Add Standalone Snap-in** dialog box appears, you can click **Add** to add another snap-in.
7. When you are finished adding snap-ins, in the **Add Standalone Snap-in** dialog box, click **Close**.

   The **Add/Remove Snap-in** dialog box appears and displays the snap-ins that you are installing in MMC.
8. In the **Add/Remove Snap-in** dialog box, click **Close**.

Figure 16.4 shows an example of three Certificates console nodes that have been added to MMC. The first Certificates console node manages certificates for the logged on user. The second Certificates console node manages certificates for the World Wide Web Publishing service for the local computer. The third Certificates console node manages certificates for the local computer itself.



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

Figure 16.4 Certificates Console

The Certificates console nodes in Figure 16.4 have been expanded to show the logical certificate stores. This is called the Logical display mode. You also have the option of viewing certificates by their physical stores or by their purpose.

To change the display mode, select the Certificates console (such as the Certificates - Current User console). Click **View** and then click **Options**. When the **View Options** dialog box appears, you can choose from the display mode options that are described in Table 16.3.

Table 16.3 View Options Dialog Box

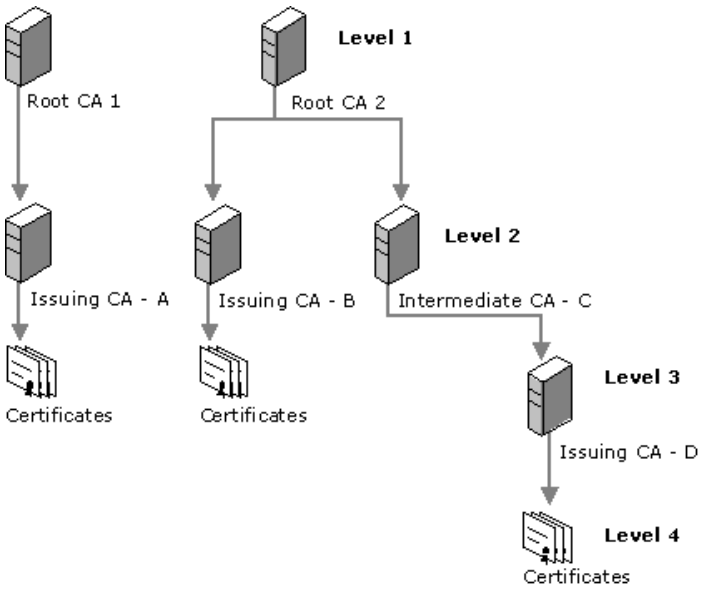
Option	Description
Certificate purpose	Select this option to view certificates in the Purposes display mode, in which certificates are grouped by the intended purpose of the certificates, such as Encrypting File System, File Recovery, and Code Signing.
Logical certificate stores	Select this option to view certificates in the Logical display mode, in which certificates are grouped by the logical store where they are located. This is the default display mode.
Physical certificate stores	Select this option to view the physical stores in addition to the logical stores. This option is available for the Logical display mode only.
Archived certificates	Select this option to view archived certificates. When certificates expire or are renewed, Windows 2000 maintains archives of the certificates and their private keys. Retaining archived certificates is recommended because you might need to use the certificate and its private key later. For example, you might have to verify digital signatures for old documents that were signed with a key for a currently expired or renewed certificate.

Certification Authority Trust Model

The Windows 2000 public key infrastructure supports a hierarchical CA trust model and CTLs. To control what certificates are trusted in the enterprise, you can deploy Windows 2000 Certificate Services to create CA trust hierarchies and you can create CTLs.

Certification Authority Hierarchies

The Windows 2000 public key infrastructure supports a hierarchical CA trust model, called the *certification hierarchy,* to provide scalability, ease of administration, and compatibility with a growing number of commercial third-party CA services and public key-aware products. In its simplest form, a certification hierarchy consists of a single CA. However, the hierarchy usually contains multiple CAs that have clearly defined parent-child relationships. Figure 16.5 shows some possible CA hierarchies.



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

Figure 16.5 Certification Hierarchies

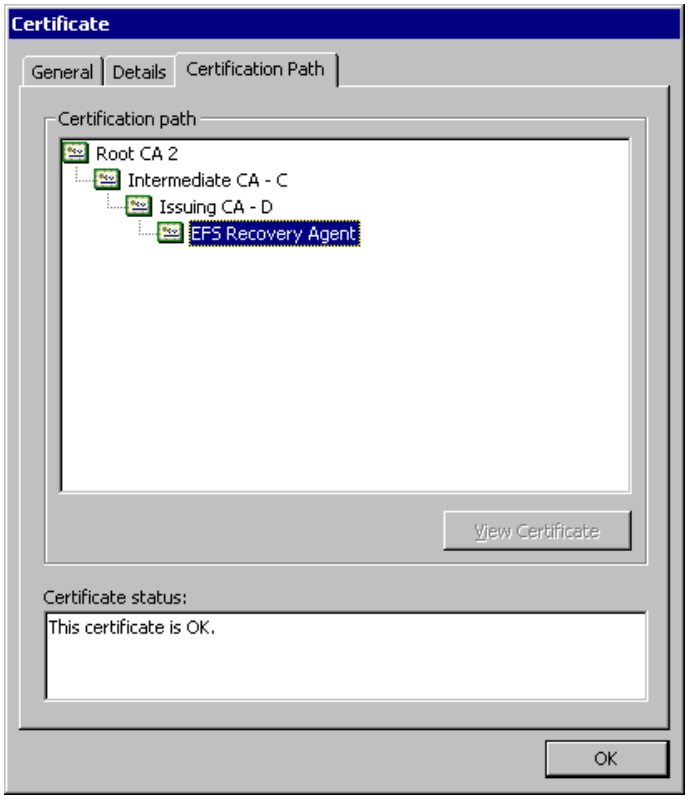
You can deploy multiple CA hierarchies to meet your needs. The CA at the top of the hierarchy is called a *root CA*. Root CAs are self-certified by using a self-signed CA certificate. Root CAs are the most trusted CAs in the organization and it is recommended that they have the highest security of all. There is no requirement that all CAs in an enterprise share a common top-level CA parent or root. Although trust for CAs depends on each domain's CA trust policy, each CA in the hierarchy can be in a different domain.

Child CAs are called *subordinate CAs*. Subordinate CAs are certified by the parent CAs. A parent CA certifies the subordinate CA by issuing and signing the subordinate CA certificate. A subordinate CA can be either an intermediate or an issuing CA. An *intermediate CA* issues certificates only to subordinate CAs. An *issuing CA* issues certificates to users, computers, or services.

There is no restriction with regard to how deep the certification hierarchy can be. However, for many organizations, a three-level certification hierarchy (root CA, intermediate CA, and issuing CA) meets most needs.

Certification Path

A certification hierarchy forms a trust chain, called the *certification path*, from the certificate back to the root CA. Figure 16.6 illustrates a certification path for a four-level path that corresponds to the three-level CA hierarchy in Figure 16.5.



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

Figure 16.6 Trusted Certification Path

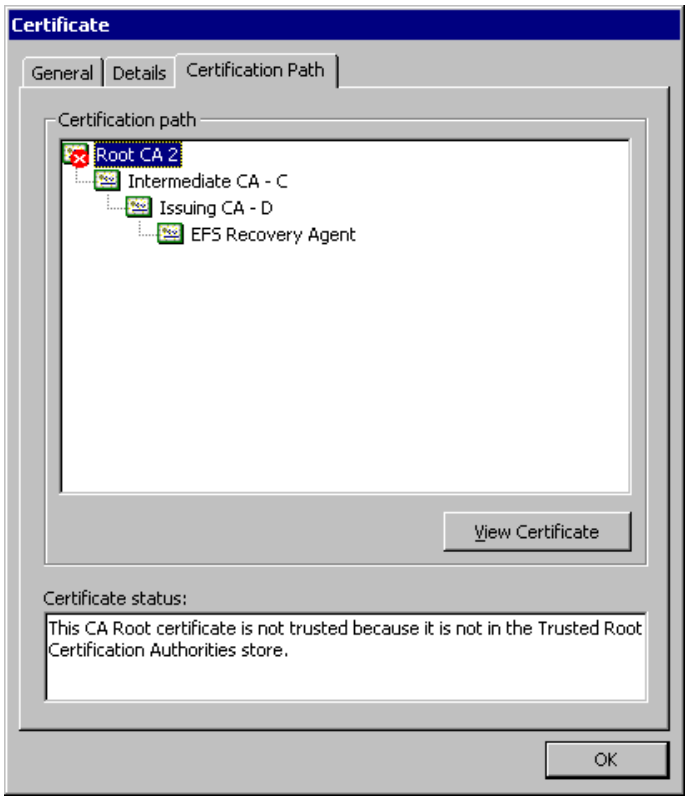
In the example, an EFS Recovery Agent certificate that was issued by Issuing CA - D has a certification path to Root CA 2 at the top of the path. The EFS Recovery Agent certificate is trusted because the certificate for Root CA 2 is contained in the Trusted Root Certification Authorities store.

The certification path links each certificate in the chain back to the root CA. Certificates that have a valid certification path to a root certificate that is in the Trusted Root Certification Authorities store are trusted for all purposes listed in the certificate. If the root CA's certificate for a certification path is not in the Trusted Root Certification Authorities store, the certification path is not trusted until the certificate of the root CA is added to the Trusted Root Certification Authorities store.

Before it trusts a certificate, Microsoft CryptoAPI validates the certification path from the certificate to the certificate of the root CA by checking each certificate in the path. Each certificate contains information about the parent CA that issued the certificate. CryptoAPI retrieves the certificate of each parent CA in the path from either the Intermediate Certification Authorities store or the Trusted Root Certification Authorities stores (if the certificates are present in the stores), or from an online location (such as an HTTP or LDAP address) that is specified in the certificate. If CryptoAPI discovers a problem with one of the certificates in the path, or if it cannot find a certificate, it does not trust the certification path.

When CryptoAPI retrieves a subordinate CA certificate for certificate path validation and the certificate is not located in the Intermediate Certification Authorities store, the API stores the certificate in the Intermediate Certification Authorities store for future reference. However, for computers that operate offline, such as portable computers that are used by mobile users, you might have to import subordinate CA certificates into the Intermediate Certification Authorities store to ensure that nonroot CA certificates are available to validate certification paths.

Figure 16.7 shows an example of a nontrusted certification path where the root certificate is not in the Trusted Root Certification Authorities store.



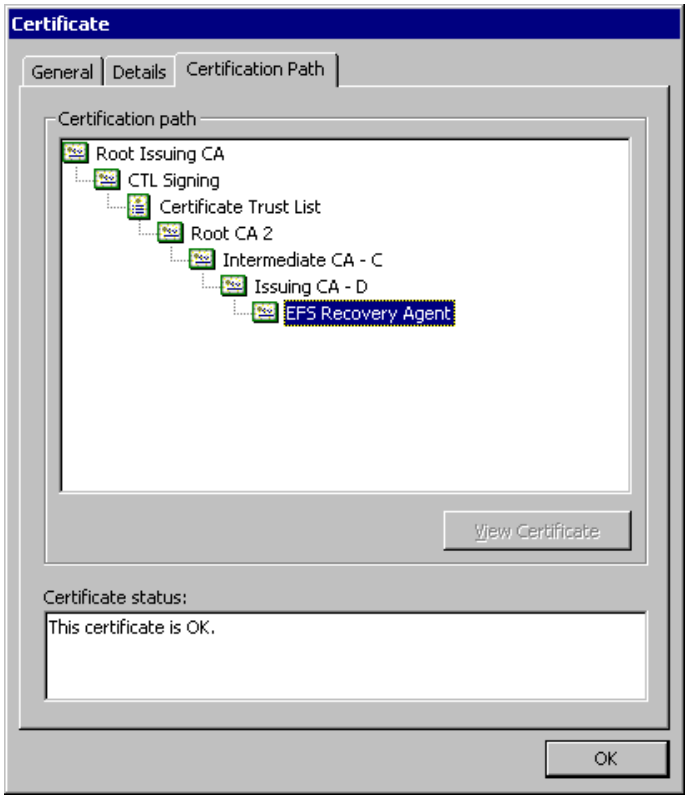
If your browser does not support inline frames, click here to view on a separate page.

Figure 16.7 Nontrusted Certification Path

By default, certificates that are issued by trusted CAs are trusted for all of the intended purposes that are listed in the certificate. You can use the **Certificate Details** dialog box to restrict the purposes for which local certificates can be used. You can also use CTLs to establish trust for certificates and restrict the purposes for which certificates are trusted.

Certificate Trust Lists

You can use the Certificate Trust List wizard that is available from the Public Key Policy section of the Group Policy console (an MMC snap-in) to create CTLs. By using CTLs, you can choose to trust certificates that have certification paths to root CAs that are listed in the CTL. You can create CTLs for computers and users. CTLs for computers apply to all computers, users, and services within the scope of the Group Policy. However, CTLs for users apply only to users within the scope of the Group Policy. Figure 16.8 shows an example of a certification path with a CTL.



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

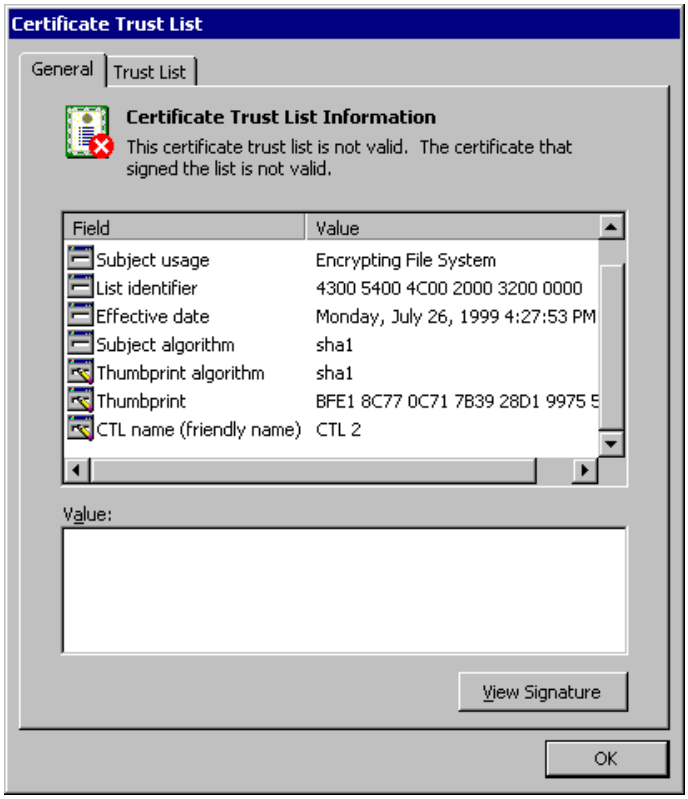
Figure 16.8 Trusted Certification Path with a CTL

In the example, the certification path from EFS Recovery Agent to Root CA 2 is identical to the certification path shown in Figure 16.6, but the certificate for Root CA 2 is not in the Trusted Root Certification Authorities store. The certification path also includes the CTL, the trust list signing certificate ("CTL Signing" in the example), and the root CA certificate that issued the signing certificate ("Root Issuing CA" in the example). The EFS Recovery Agent certificate is trusted because the certificate for Root Issuing CA (which issued the CTL Signing certificate) is contained in the Trusted Root Certification Authorities store.

A CTL must be signed by an administrator who has a valid certificate for trust list signing, such as the Administrator and Trust List Signing certificates that can be issued by enterprise CAs. By default, CTLs are valid until the trust list signing certificate expires and the CTL becomes invalid. However, to limit the time that certificates are trusted, you have the option of specifying a shorter lifetime for the CTL.

By default, members of the Domain Admins and Enterprise Admins security groups are granted permissions to enroll for Administrator and Trust List Signing certificates. To change the default certificate enrollment settings, modify the ACLs for the Administrator and Trust List Signing certificate templates.

For the CTL to be valid, the trust list signing certificate must have a certification path to a root CA in the Trusted Root Certification Authorities store. Figure 16.9 shows an example of a CTL that is invalid because the trust list signing certificate is invalid. This might be the situation because either the certification path for the trust list signing certificate does not validate to a trusted root certificate or the trust list signing certificate has expired.



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

Figure 16.9 Invalid CTL

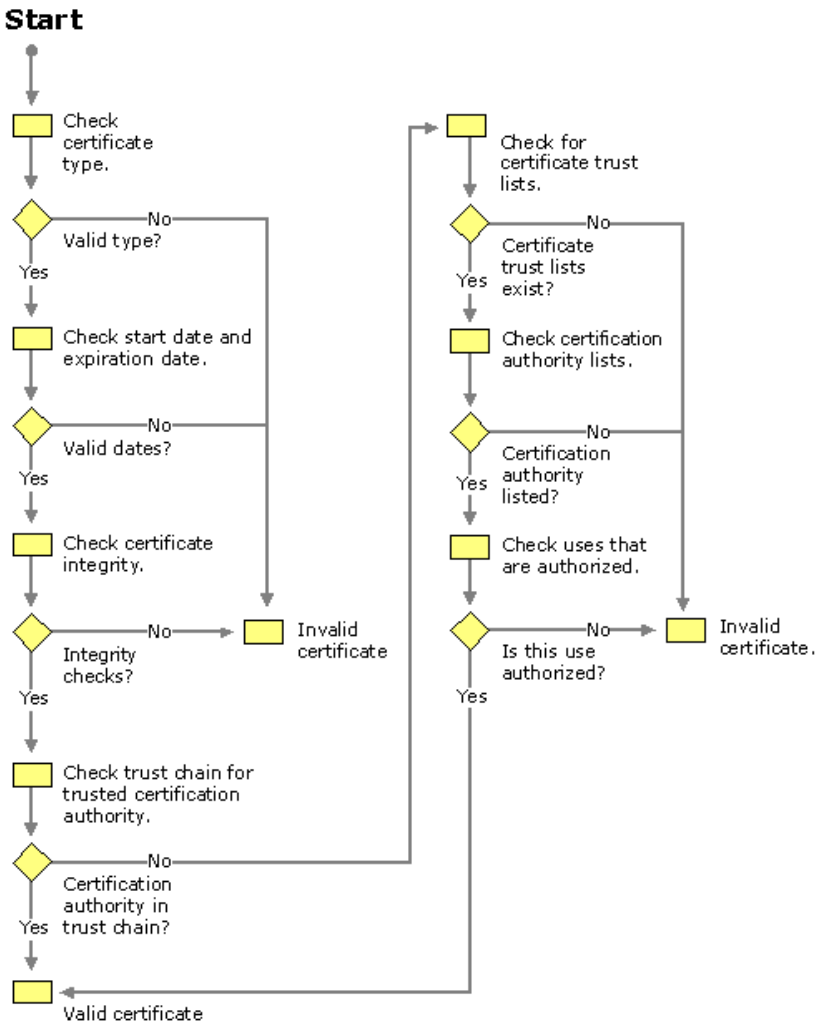
CTLs are stored in the Enterprise Trust store and you can use the Certificates console to view them.

In addition, you can use CTLs to restrict the purposes for which certificates can be used. For example, even though a certificate permits the purposes of software code signing, secure mail, and client authentication, you can use a CTL to restrict certificate use to client authentication only. CTLs are frequently used to restrict trust for certificates that are issued and managed by other organizations. For example, you might configure a CTL to trust a business partner's CA for only code signing and client authentication on an extranet that you manage.

Internet Information Services (IIS) also supports CTLs for secure Web sites. For more information about CTLs with IIS, see "Choosing Security Solutions That Use Public Key Technology" in this book.

Certificate Validation Process

Before it trusts certificates, Windows 2000 performs a validation check to ensure that certificates are valid and that they have a valid certification path. Figure 16.10 shows the basic certificate validation process.



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

Figure 16.10 Basic Certificate Validation Process

Certificates can be invalid or are not trusted for a variety of reasons, including the following:

- The start and expiration dates are improper or expired.
- The certificate format is improper (does not conform to the X.509 version 3 standard for digital certificates).
- The information in certificate fields is improper or incomplete.
- The certificate's digital thumbprint and signature fail the integrity check, indicating that the certificate has been tampered with or corrupted.
- The certificate is listed as revoked in a published certificate revocation list.
- The issuing CA is not in either a trusted certification hierarchy or a CTL.
- The root CA for the certification path is not in the Trusted Root Certification Authorities store.
- The certificate is not permitted for the intended use as specified in a CTL.

An expired CA certificate in the certification path does not invalidate the path. In the Windows 2000 public key infrastructure, a certification path can be valid as long as the CA certificate was valid at the time the certificate was issued. For example, a third-party CA might issue a certificate with a lifetime that extends past the CA certificate's expiration date. After the CA's certificate expires, the certification path for the certificate is still valid and the certificate is trusted as long as all other validation criteria are met.

Benefits of Multiple-Level Certification Hierarchies

Consider deploying multiple-level certification hierarchies that include root CAs, intermediate CAs, and issuing CAs. Multiple-level trust hierarchies provide many benefits.

General Benefits

Deploying multiple-level certification hierarchies provides the following general benefits:

- They require trust in a relatively small number of root CAs that you can centrally control and maintain to ensure high security and integrity for root CAs.
- They reduce the cost and impact of a failed or compromised CA.
- They provide flexibility so business units can deploy and manage intermediate CAs to meet their public-key security needs.
- They provide flexibility so business units can deploy and manage issuing CAs to distribute certificate load and provide duplication of certificate services.

Administrative Benefits

Deploying multiple-level certification hierarchies provides the following administrative benefits:

- It enables flexible configuration of the CA security environment (key strength, physical protection, protection against network attacks, and so forth). You can tailor the CA environment to provide a balance between security and usability. For example, for a root CA, you might choose to use special purpose cryptographic hardware, maintain it in a locked vault, and operate it in offline mode. However, for an issuing CA, crypto-hardware, locked vaults, and offline operations are costly, make the CA difficult to use, and reduce the performance and effectiveness of the CA.
- It enables relatively frequent renewals of keys and certificates for those intermediate and issuing CAs that are at high risk for compromise, without requiring a change to established root trust relationships.
- It enables you to "turn off" a subsection of the CA hierarchy without affecting established root trust relationships or the rest of the hierarchy. For example, you can easily shut down an issuing CA that services one site, without affecting other certificate services for that site and without affecting certificate services for other sites.

Benefits of Multiple Issuing Certification Authorities

Deploying multiple issuing CAs provides several benefits, including the following:

- You can specify separate certificate policies for different groups of users or computers. You can deploy separate issuing CAs to administer separate certificate policies for each group of users and computers.
- You can specify separate certificate policies based on organizational divisions, such as a user's or computer's role in the organization. You can deploy issuing CAs to administer separate certificate policies based on such organizational divisions.
- You can specify separate certificate policies based on geographic divisions, such as the locations of users and computers at multiple physical sites.
- You can distribute certificate load and provide redundant services by deploying multiple issuing CAs to distribute the certificate load, meeting site, network, and server connectivity and load requirements. For example, slow or noncontinuous network links between sites might require issuing CAs at each site for acceptable certificate services performance and usability requirements. You can also deploy multiple issuing CAs to provide duplicate services so that if one CA fails, another issuing CA is available to provide uninterrupted service.

Windows 2000 Certification Authorities

Windows 2000 Server and Certificate Services support two types of CAs: enterprise CAs and stand-alone CAs. A root CA or a subordinate CA can be installed as either an enterprise CA or a stand-alone CA.

Enterprise Certification Authorities

Enterprise CAs are integrated with Active Directory. Enterprise CAs publish certificates and CRLs to Active Directory. Enterprise CAs use certificate template information, user account information, and security group information that are stored in Active Directory to approve or deny certificate requests. For a certificate request to be approved, the requestor must have Enroll permissions granted by the security ACLs of the certificate template for the certificate type that was requested. When a certificate is issued, the enterprise CA uses information in the certificate template to generate a certificate with the appropriate attributes for that certificate type.

It is recommended that you install most issuing CAs as enterprise CAs to gain the benefits of integration with Active Directory, including automated certificate approval and automatic computer certificate enrollment. Furthermore, only enterprise CAs can issue certificates for logging on with smart cards because this process requires that smart card certificates be mapped automatically to the user accounts in Active Directory and because it uses certificate templates.

Stand-alone Certification Authorities

Stand-alone CAs do not require Active Directory and do not use certificate templates. For stand-alone CAs, all information about the requested certificate type must be included in the certificate request. The Web Enrollment Support pages that are installed for stand-alone CAs, support requests for a variety of certificate types.

By default, all certificate requests submitted to stand-alone CAs are held in the Pending Queue until the CA administrator approves them. You can configure stand-alone CAs to issue certificates automatically upon request, but this adds a significant security risk and usually is not recommended.

If you want to automate certificate requests for stand-alone CAs, consider developing custom policy modules that securely approve or deny certificate requests. For example, you might develop a custom policy module that automatically grants certificates to authenticated requestors based on security information about the requestor that is contained in a legacy database or a third-party directory service. Stand-alone CAs cannot issue certificates for the smart card logon process, but they can issue other types of certificates for smart cards. For example, you can use the Web Enrollment Support pages for a stand-alone CA to issue secure mail and secure Web browser certificates to requestor's smart cards.

By default, stand-alone CAs publish CRLs to the following location:

`<Drive:>\WINNT\System32\Certsrv\Certenroll`

where <*Drive:*>\ is the letter of the disk drive where the CA is installed.

The use of stand-alone CAs for high-volume issuing usually incurs a high administrative cost because administrators must manually review and approve or deny each certificate request. Therefore, stand-alone issuing CAs are intended primarily for use with public key security applications on extranets and the Internet, when users do not have Windows 2000 accounts and the volume of certificates to be issued and managed is relatively low.

You must, however, install stand-alone CAs to issue certificates when you are using a third-party directory service or when Active Directory is not available. Furthermore, stand-alone CAs can provide more flexibility for planning and managing the certificate life cycle by using root CA and intermediate CAs.

Certificate Life Cycle

The certificate life cycle includes the following events:

- CAs are installed and their certificates are issued.
- Certificates are issued by CAs.
- Certificates are revoked (as necessary).
- Certificates are either renewed or allowed to expire.
- The CAs' certificates are renewed before they expire.
- The CA is revoked or retired.

Issued certificates expire at the end of their lifetime, but they can be renewed as necessary. You also can renew CAs before the CA's certificate expires to ensure continuous certificate services in your enterprise.

Windows 2000 CAs require nested validity dates for the certificate life cycle. A Windows 2000 CA cannot issue certificates with a lifetime

that extends beyond the end date for the CA's certificate validity. If the lifetime specified for a requested certificate type exceeds the expiration date of the CA's certificate, the CA truncates the lifetime of the issued certificate to match the validity end date for the CA's certificate. Therefore, nested validity dates are an important consideration when you are planning the certificate life cycle for Windows 2000 Certificate Services CAs. Third-party CAs might not require nested lifetimes for the certificate life cycle.

The certificate lifetimes of certificates that are issued by enterprise CAs are determined differently than the lifetime of certificates that are issued by stand-alone CAs. An enterprise CA issues certificates with lifetimes that are based on the certificate template for the requested certificate type. A stand-alone CA issues certificates with a lifetime that is determined by system registry settings for the CA. Furthermore, the lifetime of CA certificates is affected by several other factors. In addition, take into account how long private keys can be safely used so that you do not exceed the maximum safe lifetime of the keys.

Nested Validity Dates

Windows 2000 enterprise CAs and stand-alone CAs require nested validity dates for all CA certificates and all issued certificates. For example, if a Windows 2000 root CA's certificate end date is January 2, 2010, no Windows 2000 child CA in the chain below the root can issue a certificate with a date that is past January 2, 2010. If a Windows 2000 intermediate CA has a certificate end date of January 2, 2006, no Windows 2000 child CA can issue certificates with an end date that is past January 2, 2006. If a Windows 2000 issuing CA has a certificate end date of January 2, 2002, no certificate the CA issues can have an end date that is past January 2, 2002.

If a Windows 2000 CA's certificate has an end date of January 2, 2002, and it receives a request to issue a one-year certificate on August 1, 2000, the CA issues the one-year certificate with an end date of July 31, 2001. However, if the CA receives a request to issue a one-year certificate on August 1, 2001, the CA issues the certificate with an end date of January 2, 2002.

A Windows 2000 CA with a certificate life of five years ending on January 2, 2005, can issue one-year certificates until January 2, 2004, or two-year certificates until January 2, 2003. After January 2, 2003, the CA does not issue two-year certificates; it truncates the validity end date to January 2, 2005. Likewise, after January 2, 2004, the CA truncates the validity end date of both one-year and two-year certificates to January 2, 2005.

You usually renew Windows 2000 CAs with new CA certificates before they are constrained by nested validity dates. To avoid the constraints of nested validity dates, deep certification hierarchies with Windows 2000 Certificate Services might require frequent renewals for issuing CAs.

Certificates Issued by Stand-alone Certification Authorities

For stand-alone CAs, the lifetime of issued certificates is determined by the following registry entries:

```
HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \CertSvc \ConfigurationStand-aloneCA\ValidityPeriod
HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \CertSvc \ConfigurationStand-aloneCA\ValidityPeriodUnits
```

Caution Do not use a registry editor to edit the registry directly unless you have no alternative. The registry editors bypass the standard safeguards provided by administrative tools. These safeguards prevent you from entering conflicting settings or settings that are likely to degrade performance or damage your system. Editing the registry directly can have serious, unexpected consequences that can prevent the system from starting and require that you reinstall Windows 2000. To configure or customize Windows 2000, use the programs in Control Panel or Microsoft Management Console (MMC) whenever possible.

Where *Stand-aloneCA* is the name of the installed CA, the value of **ValidityPeriod** is either "Days," "Weeks," "Months," or "Years," and **ValidityPeriodUnits** is the number of days, weeks, months or years that constitute the lifetime of certificates issued by the CA. For example, when the value of **ValidityPeriod** is "Years" and the decimal value of **ValidityPeriodUnits** is "2," the CA issues certificates with a lifetime of two years.

By default, stand-alone CAs issue certificates with lifetimes of one year. (The default settings are: **ValidityPeriod** = Years and **ValidityPeriodUnits** = 1,) To specify another lifetime for certificates that are issued by a stand-alone CA, edit the registry for the stand-alone CA, and enter the appropriate values for **ValidityPeriod** and **ValidityPeriodUnits**.

All certificates that the stand-alone CA issues have the lifetime specified by the values of the **ValidityPeriod** and **ValidityPeriodUnits** registry entries. Therefore, if you want to issue certificates with different lifetimes, you must deploy either enterprise CAs, multiple stand-alone CAs, or third-party CAs.

Certificates Issued by Enterprise Certification Authorities

For enterprise CAs, the maximum lifetime of certificates that are issued is determined by the settings of **ValidityPeriod** and **ValidityPeriodUnits** in the registry. The default settings are: **ValidityPeriod** = Years and **ValidityPeriodUnits** = 2. Therefore, the maximum lifetime of certificates that are issued by an enterprise CA is two years unless you modify the registry settings.

In addition, the lifetime of each certificate type is determined by its certificate template. The lifetime for many certificate types is one year. However, the following certificate templates specify a lifetime of two years:

- CEP Encryption (offline request)
- Enrollment Agent
- Enrollment Agent (computer)
- Enrollment Agent (offline request)
- IPSec
- IPSec (offline request)
- Router (offline request)
- Web Server

The following certificate templates specify a lifetime of five years:

- Domain Controller
- Subordinate Certification Authority

These certificates are usually issued for two years (the maximum default lifetime of certificates issued by enterprise CAs). To enable an enterprise CA to issue certificates for five years, you must change the settings of **ValidityPeriod** and **ValidityPeriodUnits** for the CA to five years or more.

In addition, you can modify **ValidityPeriod** and **ValidityPeriodUnits** of a CA to reduce the maximum lifetime of certificates that it issues. For example, to reduce the maximum lifetime of all certificates issued by a CA to six months, you can change **ValidityPeriod** to "Month" and **ValidityPeriodUnits** to "6". You can also deploy custom certificate services to meet special certificate lifetime needs for your organization.

Certification Authorities' Certificates

For enterprise root CAs and enterprise stand-alone root CAs, the CA certificates are installed with a default lifetime of two years. However, during CA installation, you can specify a different lifetime for the CA. You can specify the root CA's lifetime in days, weeks, months, or years. For example, you might specify a root CA lifetime of 20 years because you use a large private key and provide high

security for the CA. You might also want to specify short lifetimes of days or weeks when you are testing the deployment of Certificate Services.

During the installation of subordinate CAs, the system enables you to request a subordinate CA certificate from an active parent CA, or you have the option of creating a certificate request file and then submitting the request offline to a parent CA. For online requests from an active CA, when the request is approved, the subordinate CA is issued a subordinate CA certificate automatically by the parent enterprise CA. For offline requests, you must use the Web Enrollment Support pages to submit the certificate request file to the parent CA. After the subordinate CA certificate is issued, you must use the Certification Authority console to install the certification path file to certify and start the CA.

The lifetime of a subordinate CA certificate is determined by the parent CA that approves the certificate request and issues it. If the parent CA is an enterprise CA, the default lifetime of the subordinate CA's certificate is two years, unless the **ValidityPeriod** and **ValidityPeriodUnits** values are changed in the registry for the parent CA. You can change the registry to specify a shorter or longer lifetime for certificates that are issued by the parent CA, but the maximum lifetime for subordinate CA certificates is five years as specified by the Subordinate Certification Authority certificate template. If the parent CA is a stand-alone, the lifetime of the subordinate CA's certificate is determined by the values of the **ValidityPeriod** and **ValidityPeriodUnits** entries in the registry of the parent CA.

Consider using stand-alone CAs for root and intermediate CAs to provide the most flexibility for defining certificate life cycles. If you specify long lifetimes for CAs and later discover that they are at greater risk than originally anticipated, it is easy to renew CAs in the certification hierarchy with shorter lifetimes as necessary to reduce risk.

Using stand-alone CAs for root and intermediate CAs can provide other benefits as well. If you operate stand-alone CAs offline (not connected to the network) and maintain them in secure physical environments, the risk of attacks is reduced. You also can regulate the installation process to carefully control the CAs that are installed and trusted in the enterprise.

Administering offline certificate requests for both stand-alone root and intermediate CAs is usually cost effective because the CAs are used infrequently to process relatively few certificate requests. You might, however, occasionally connect to the network only as long as necessary to publish CRLs or to process infrequent online certificate requests for subordinate CA certificates.

Example of a Certificate Life Cycle

Table 16.4 describes an example of a certificate life cycle that an organization might plan for Windows 2000 CAs and standard Microsoft CSPs.

Table 16.4 Windows 2000 Certificate Life Cycle

Purpose of Certificate	Certificate Life	Private Key Life
Stand-alone root CA. (4,096-bit key)	20 years	Renew at least every 10 years to ensure that intermediate CA certificates can be issued with lifetimes of 10 years. Renew by using a new key at least every 20 years.
Stand-alone intermediate CA for all certificates except smart card certificates. (3,072-bit key)	10 years	Renew at least every 5 years to ensure that child issuing CAs can be issued for a full 5 years. Renew by using a new key at least every 10 years.
Enterprise issuing CA for all certificates except smart card certificates. (2,048-bit key)	5 years	Renew at least every 3 years to ensure that Web server certificates can be issued for a full 2 years. Renew by using a new key at least every 5 years.
Enterprise issuing CA 2 for smart card certificates. (2,048-bit key)	5 years	Renew at least every four years to ensure that certificates can be issued for a full year. Renew by using a new key at least every 5 years.
Enterprise issuing CA 3 for all other certificates besides smart cards, secure mail, and secure browser certificates. (2,048-bit key)	5 years	Renew at least every 4 years to ensure that certificates can be issued for a full year. Renew by using a new key at least every 5 years.
Secure mail and secure browser certificates.	1 year	Renew by using a new key at least every 2 years.
Smart card certificates. (1,024-bit key)	1 year	Renew by using a new key at least every 2 years.
Administrator certificates. (1,024-bit key)	1 year	Renew by using a new key at least every 2 years.
Secure Web server certificates. (1,024-bit key)	2 years	Renew by using a new key at least every 2 years.
Business partners' users certificates for an extranet. (512-bit key)	6 months	Renew by using a new key at least every year.

Note The certificate life cycle described in Table 16.4 is provided only as an example and is not intended to be a recommendation. Your certificate life cycle can differ from the example in many ways, including the length of certificate lifetimes, key lengths, and key lifetimes.

In Table 16.4, all certificates are issued by Windows 2000 CAs except for the certificates for the business partners' users (for the extranet), which are issued by the CA of the business partner. The certificates of the business partner are trusted in the extranet domain by using CTLs. Stand-alone CAs are used to provide flexible lifetimes for CAs where this is appropriate. Renewing certificates with new keys limits the time that keys are in use and reduces the risk of key compromise.

Because of the constraints of nested validity dates, when you allow CAs to issue certificates with truncated lifetimes, the certificates that are issued must be renewed more frequently as the end validity date of the CA's certificate is approached. Therefore, CAs are usually renewed before the certificates that are issued by the CA have truncated lifetimes. You also renew certificates with new keys before their maximum safe lifetime are exceeded. To reduce risks for private keys, you might also renew certificates with new keys each time the certificate is renewed if it is feasible to do so.

The deeper the certification hierarchy, the shorter the certificate lifetimes become. Plan your certificate life cycles to avoid excessively short certificate lifetimes and certificate renewal cycles.

General Considerations for Key Lifetimes

There is no simple formula for determining maximum private key lifetimes. The lifetimes you choose depend on various risk factors, such as the following:

- The length of private keys for certificates. In general, longer keys support longer key lifetimes.

- Security provided for private keys by the CSPs. In general, hardware-based CSPs provide more security and can support longer private key lifetimes than software-based CSPs.
- Security provided for CAs and their private keys. In general, the more secure the CA and its private key, the longer the safe CA lifetime. For example, you might improve the security for CAs by operating them offline and storing them in locked vaults or data centers.
- The strength of the cryptographic technology used for cryptographic operations. Some cryptographic technologies provide stronger security, as well as support for stronger cryptographic algorithms. For example, you might use smart cards for logging on by users or FORTEZZA Crypto Cards for secure mail and secure Web browsers. In general, stronger cryptographic technology supports longer key lifetimes.
- The risk of attack on the CA certification chain. These risks depend primarily on how secure your enterprise is, how valuable the network resources protected by your public key security applications are, and how much launching attacks would cost the attackers. In general, high risks of attack require longer CA private keys and shorter key lifetimes.

To further reduce the risk of a compromised private key, the private key and public key sets for certificates might be renewed each time the certificates are renewed, instead of waiting for the maximum key lifetime. However, for some hardware-based CSPs, renewing certificates with new key sets is not feasible either because of key storage limits or because key generation takes a long time.

When you install a Windows 2000 CA, you can select the **Advanced options** check box on the first page of the Windows Components wizard, with which you can specify the key length that is used with the CA's certificate. You can select CA key lengths from 384 bits to 16,384 bits. In general, the longer the key, the longer the safe key lifetime. The use of keys that are at least 1,024 bits long is recommended for CAs.

Consider using the largest keys that are practical to use for CAs to provide the maximum protection feasible without degrading CA performance. Keep in mind that very large keys can place a high load on computer processors and might require excessive amounts of time for signing operations. Test proposed CA key lengths in the lab and pilot programs before you deploy CAs to your production environment.

For more information about the risks associated with private keys, see "Cryptography for Network and Information Security" in this book.

When you renew certificates by using the Microsoft CSPs, you also can renew the certificate's private key and public key set. In general, the longer the key set is in use, the higher the risk that the key might become compromised. Establish maximum allowable key lifetimes, and renew certificates with new key sets before these limits are exceeded.

Certificate Enrollment and Renewal Methods

Windows 2000 Certificate Services supports the following certificate enrollment and renewal methods:

- Manual certificate requests that use the Certificate Request wizard (only for Windows 2000 users and computers).
- Automatic certificate requests, which use the Automatic Certificate Request Setup wizard (only for Windows 2000 computer certificates).
- Manual certificate requests that use the Web Enrollment Support pages (for Web browser users).
- Smart card enrollment, which uses the Smart Card Enrollment Station available in the Web Enrollment Support pages.
- Custom certificate enrollment and renewal applications.

The enrollment methods and types of certificates that are supported by third-party certificate services depend on the features and functions of each third-party product. For more information, contact the vendor for the certificate service.

Manual Certificate Requests for Windows 2000–based Clients

You can request or renew certificates for Windows 2000 users and computers by using the Certificate Request wizard that is available in the Certificates console. The Certificate Request wizard does not function unless an enterprise CA is online to process and issue certificate requests. The ACLs for the certificate templates determine which user accounts or computer accounts can enroll for the various types of certificates.

You can also use the Certificate Renewal wizard that is available in the Certificates console to renew certificates either before or after they expire. The Certificate Renewal wizard does not function unless an enterprise CA is online to process and issue certificate requests. You have the option of renewing certificates with the same private key and public key set. You must not renew certificates with the same private and public key sets if the maximum safe key lifetime would be exceeded.

Automatic Computer Certificate Enrollment and Renewal

You can use the Automatic Certificate Request Setup wizard (available from the Public Key section of the Group Policy console) to configure autoenrollment for computer certificates. Autoenrollment is not available for user certificates and does not function unless an enterprise CA is online to process certificate requests. You can configure autoenrollment for Computer, Domain Controller, and IPSec certificates.

When autoenrollment is configured, the specified certificate types are issued automatically to all computers that are within the scope of the Public Key Group Policy and to all computers that have Enroll permissions for that certificate type. Autoenrollment certificates are issued the next time the computer logs on to the network.

For example, if you configure autoenrollment for Computer certificates, the certificates are issued to all computers in the Domain Computers security group that are within the scope of the Public Key Group Policy. By default, all Windows 2000 computers are members of the Domain Computers security group, except for domain controllers, Routing and Remote Access servers, and Internet Authentication Services (IAS) servers. You can control which computers receive the Computer certificates by modifying the ACLs for the Computer certificate templates, for example, to grant Enroll permissions to a special security group composed of computers that you designate. Computers within the scope of the Public Key Group Policy that are members of the special security group are then issued Computer certificates the next time they log on to the network.

In addition, you also can use organizational units (OUs) and Public Key Group Policy for those OUs to restrict autoenrollment to certain groups of computers. For example, you might create an IPSec Authentication OU that contains the Windows 2000 clients that you designate for IPSec authentication with certificates. To limit the scope of autoenrollment for IPSec certificates, configure Public Key Group Policy and autoenrollment for the IPSec Authentication OU.

When autoenrollment is configured, the Computer certificates that are issued by autoenrollment also are automatically renewed from the enterprise issuing CA. You can also renew Computer certificates manually with the Certificate Renewal wizard or through the Certificate Services Web Enrollment Support pages.

Web Enrollment Support Pages

The Windows 2000 Certificate Services Web Enrollment Support pages are composed of Active Server Pages and ActiveX® controls that provide a Web-based user interface to a CA. By default, the Web Enrollment Support pages are automatically installed on the computer where the CA is installed, but you also have the option of installing the Web Enrollment Support pages on another Windows 2000 Server computer.

You can use the Web Enrollment Support pages to perform the following tasks:

- Request and obtain a basic user certificate.
- Request and obtain other types of certificates by using advanced options.
- Request a certificate by using a certificate request file.
- Renew certificates by using a certificate renewal request file.
- Save a certificate request to a file.
- Save the issued certificate to a file.
- Check on pending certificate requests.
- Retrieve the CA's certificate.
- Retrieve the latest certificate revocation list from the CA.
- Enroll for smart card certificates on behalf of other users (for use by trusted administrators).

The Web Enrollment Support pages that are installed for stand-alone CAs are similar to the pages that are installed for enterprise CAs, but they differ in the respect that stand-alone CAs do not use certificate templates. For stand-alone CAs, all information about the certificate, including information about the requestor, must be specified in the certificate request. The Web Enrollment Support pages for stand-alone CAs support a number of types of certificates that have much of the same functionality as certificate types that are based on templates. You can deploy stand-alone CAs and Web Enrollment Support pages to issue most of the types of certificates that enterprise CAs can issue. However, certificates for logging on by using smart cards logon and for autoenrollment require an enterprise CA to issue and renew the certificates.

The Web Enrollment Support pages work with Microsoft® Internet Explorer 4 and Microsoft® Internet Explorer 5. Use of the Microsoft Enhanced Cryptographic Provider requires Internet Explorer browsers with nonexportable cryptography. Internet Explorer browsers with exportable cryptography work only with the Microsoft Base Cryptographic Provider.

Netscape Navigator version 4.*x* and Netscape Communicator version 4.*x* work with most of the Web Enrollment Support pages. Netscape browsers do not work with the Advanced Certificate Requests form and the Smart Card Enrollment Station page because these pages use ActiveX controls. In addition, Netscape browsers use their own cryptographic security modules rather than CSPs and, therefore, might not support all of the features that are available for the Microsoft CSPs.

Custom Enrollment and Renewal Applications

The standard enrollment and renewal methods that are available in Windows 2000 can meet a wide range of needs. However, if you have special needs, you can develop custom certificate enrollment and renewal applications. The Windows 2000 Certificate Services Entry module supports industry-standard certificate requests by using remote procedure call (RPC) requests or HTTP requests. You can develop custom applications that make certificate requests to Certificate Services CAs. For more information about developing custom applications with Windows 2000 Certificate Services, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

Public Key Group Policy

Public Key settings are a subset of Group Policy. You can configure Public Key Group Policy to specify automatic enrollment for computer certificates, trusted root certificates, CTLs for computers and users, and EFS recovery agents and apply the Group Policy to sites, domains, or organizational units.

The Group Policy console is an MMC snap-in. You can use MMC to manage Public Key Group Policy for multiple sites, domains, and organizational units. You can configure Public Key Group Policy separately for users and for computers. You can use the Group Policy console to configure the following Public Key Group Policy settings for computers:

- Specify the certificates in Trusted Root Certification Authorities stores.
- Create CTLs to trust CAs and restrict the uses of certificates issued by the CAs.
- Specify automatic enrollment and renewal for computer certificates.
- Specify alternative Encrypted Data Recovery Agents for EFS.

Public Key Group Policy settings apply for computers within the scope of the Group Policy. For example, you can create an organizational unit and configure Public Key settings that apply only to the computers in that organizational unit.

You also can use the Group Policy console to configure CTLs that apply only to users within the scope of the Group Policy. For example, you can create an organizational unit and configure CTLs that apply only to the users in that organizational unit. For more information about Group Policy, see "Group Policy" in this book and Group Policy Reference.

Certificate Revocation Lists

Windows 2000 supports industry standard X.509 version 2 CRLs. Each CA maintains a CRL for the certificates it issues and publishes the CRL-to-CRL distribution points. CRL distribution points can include Web pages, network shares, or Active Directory. An X.509 version 3 certificate usually contains the CRL distribution point for its issuing CA.

By default, enterprise CAs publish CRLs weekly to Active Directory and stand-alone CAs publish CRLs weekly to the following folder on the CA server:

`<Drive:>\WINNT\System32\Certsrv\Certenroll`

where <*Drive:*> is the letter of the disk drive where the CA is installed.

You can use the Certification Authority console to modify the *CRL distribution points*. You also can use the Certification Authority console to manually publish a new CRL or to change the publication schedule.

Certificate revocation checking is supported by Internet Explorer 5, Internet Information Services, and Active Directory mapping services. When revocation checking is enabled, you have the option of caching CRLs on local computers to enhance revocation checking performance. If a certificate lists the CRL distribution point, the revocation checking process checks the local cache to determine whether the CRL is in the cache. If not, the revocation checking process then checks the network for the CRL. If a certificate does not list the CRL distribution point, revocation checking checks the issuing CA for a CRL, if one is available. You also can use the Web Enrollment Support pages to request the latest CRL from a CA.

When revoked certificates expire, they are removed from the next published CRL. For some large organizations with high certificate revocation rates, CRLs might become so large that it places a significant load on the network and computers during CRL publication. However, you can prevent large CRLs by deploying multiple issuing CAs to distribute the certificate load among your users and by issuing certificates with reasonably short lifetimes.

Preinstalled Trusted Root Certificates

The root CA certificates that are contained in the Trusted Root Certification Authorities store are trusted for all Windows applications that use public key certificates for security functions. Windows 2000–based computers include many preinstalled certificates in the Trusted Root Certification Authorities stores. The preinstalled trusted root certificates include root certificates from a variety of commercial CAs and Microsoft. Certificates that are issued by these trusted CAs are trusted on local computers for valid purposes. However, you might not want to trust the preinstalled root certificates, or you might want to add other certificates as trusted root certificates.

You can use the Certificates console to delete or add certificates manually for Trusted Root Certification Authorities stores on each local computer. You also can add trusted root certificates for groups of computers by using Public Key Group Policy.

In addition, you can use the Internet Explorer Administration Kit (IEAK) to create and deploy custom builds of Internet Explorer that have only the root certificates that you want for your enterprise. For example, you can create custom builds that include only a few trusted root certificates and then deploy those custom builds to groups of computers. The computers where the custom builds of Internet Explorer are installed have only the trusted root certificates that you specified. You can create different custom builds to meet the requirements of different groups in your organizations. For more information about using the IEAK, see the *Microsoft® Windows® 2000 Server Resource Kit Internet Explorer Resource Guide.*

Smart Card Support

Smart cards are credit card–sized and contain integrated circuit cards (ICCs). They can be used to store certificates and private keys and to perform public key cryptography operations, such as authentication, digital signing, and key exchange. Smart cards offer the following security enhancements and benefits:

- They provide tamper-resistant storage for protecting private keys and other forms of personal information.
- They isolate security-critical computations involving authentication, digital signatures, and key exchange from other parts of the system that do not have a specific purpose for this data.
- They enable the portability of credentials and other private information between work, home, and remote computers.

In addition, smart cards use Personal Identification Numbers (PINs) rather than passwords. The smart card is protected from misuse by the PIN, which is known only to the owner of the smart card. To use the smart card, a user inserts the card in a smart card reader that is attached to a computer and, when prompted, enters the PIN. The smart card can be used only by someone who possesses the smart card and knows the PIN.

PINs offer more protection than standard network passwords. Passwords (or derivations such as hashes) travel on the network and are subject to brute force or dictionary attacks. The strength of the password depends on its length, how well it is protected, and how difficult it is to guess. In contrast, PINs never travel on the network and cannot be sniffed. Furthermore, dictionary attacks or brute force (key search) attacks (where an attacker tries numerous PIN combinations in an attempt to "guess" the PIN) can be attempted only by someone in physical possession of the smart card. And, the smart card locks after only a few failed attempts to guess the PIN.

Windows 2000 supports industry standard Personal Computer/Smart Card (PC/SC)-compliant Plug and Play smart cards and smart card readers that conform to specifications that have been developed by the PC/SC Workgroup. To work under the Windows implementation of the PC/SC 1.0 Specification, a smart card must conform physically and electrically to the International Standards Organization (ISO) 7816-1, 7816-2, and 7816-3 standards.

Smart card readers attach to standard personal computer peripheral interfaces such as RS–232, PS/2, PCMCIA, and Universal Serial Bus (USB). Readers are considered standard Windows 2000 devices, and they carry a security descriptor and a Plug and Play identifier. Smart card readers are controlled through standard Windows device drivers and are installed and removed by using the Hardware wizard.

Windows 2000 includes drivers for various commercially available Plug and Play smart card readers that are certified to display the Windows-compatible logo. Some manufacturers might provide drivers for noncertified smart card readers that currently work with Windows 2000. Nevertheless, to ensure continuing support by Microsoft, it is recommended that you purchase only those smart card readers that display the Windows-compatible logo.

The Windows 2000 CSPs includes smart card CSPs from Gemplus SCA and Schlumberger Limited. These CSPs support smart cards from the respective vendors and work with all smart card readers that display the Windows-compatible logo. The smart card CSPs store the issued certificate and the private key on the smart card.

Each smart card vendor provides software that you must install and use to initialize and configure smart cards before they can be deployed. You can use the vendor's software to configure PINs and to configure the number of PIN attempts that are allowed to occur before the smart card locks. You also can use the vendor's software to return locked smart cards to service.

For more information about smart cards, see "Choosing Security Solutions That Use Public Key Technology" in this book.

Certificate Mapping

You can use certificate mapping to control access to network resources for domain user accounts. You also can use certificate mapping to control access to Web site resources for Internet Information Services.

Domain User Accounts

You can use the Active Directory Users and Computers console (an MMC snap-in) to map user certificates to individual network user accounts. The mapped certificates are used to authenticate users during the Kerberos authentication process. Authenticated users are granted the rights and permissions for user accounts on the basis of ownership of valid certificates. Smart card logon certificates are a special type of mapped certificate. During the smart card logon enrollment process, the system maps the smart card certificates to the users' corresponding Windows 2000 user accounts automatically.

Before you can map certificates, you must point to the **Active Directory Users and Computers** console, and then click **View** and **Advanced Features**. To map certificates, right-click a user account, and then click **Name Mappings**. When the **Security Identity Mapping** dialog box appears, click **Add** to import the certificates that you want to map to the user account. You can map multiple certificates to a user account. For example, you might issue EFS Recovery Agent certificates to smart cards for designated recovery agents and then map the smart card certificates to EFS recovery user accounts. The smart cards are then required to authenticate the EFS recovery agents when logging on to the network for the EFS recovery accounts, providing an additional level of security for them.

You can map certificates only to individual user accounts; not to security groups. If you map certificates that are not stored on smart cards, users can log on only to the mapped user account from the computer where the private key is located, unless smart cards or roaming profiles are being used.

Internet Information Services

For Internet Information Services, you can map certificates to user accounts that control access to Web resources. The mapped certificates are used either to deny access to Web resources or to grant rights and permissions for the mapped user account. You can map one certificate to one user account (one-to-one mapping) or you can map many certificates to one user account (many-to-one mapping). Many-to-one mapping uses rules to define the certificate criteria for mapping. If certificates match the rules, they are mapped to the appropriate account. For example, you can define rules that map certificates to different user accounts on the basis of the specific CA that issued the certificate. All clients with certificates that are issued by a qualifying CA are mapped to the appropriate

user account and granted the respective rights and permissions for that account.

For more information about certificate mapping with Internet Information Services, see "Choosing Security Solutions That Use Public Key Technology" in this book.

Roaming Profile Support

Windows 2000 supports roaming user profiles, which allow certificates to follow users no matter which computer they use to log on. When roaming profiles are enabled, user profiles, including issued certificates and private keys, are stored on the domain controller. The roaming profiles are downloaded to the computer during the logon process for the user. Smart cards also provide roaming capabilities because a user's logon credentials are stored on the smart card. For more information about roaming profiles, see "Introduction to Desktop Management" in this book and Windows 2000 Server Help.

Certificate Services Deployment

You can perform the following activities to deploy Windows 2000 Certificate Services:

- Install certification authorities.
- Configure certification authorities.
- Modify the default security permissions for certificate templates (optional).
- Install and configure support systems or applications.
- Configure Public Key Group Policy.
- Install Web Enrollment Support on another computer (optional).
- Configure security for Web Enrollment Support pages (optional).

For more information about how to install Windows 2000 Certificate Services, see Certificate Services Help. For more information about planning the deployment of the public key infrastructure, see "Planning Your Public Key Infrastructure" in the Deployment Planning Guide.

Install Certification Authorities

You must install the CA hierarchies necessary to provide the required certificate services for your organization. Certification hierarchies with Windows 2000 CAs can include a mixture of enterprise CAs and stand-alone CAs. You can install the root CA first and then each subordinate CA in the hierarchy. For example, to create a three-level certification hierarchy, you can install CAs on servers in the following order:

1. Root CA
2. Intermediate CAs
3. Issuing CAs

However, to install the CA software on computers, you are not required to install CAs in this order. Root CAs are certified by self-signed certificates, so they do not depend on another CA to complete the installation. However, the complete installation of child CAs requires the parent CA to process the certificate request and issue the subordinate CA certificate. You can install a subordinate CA at any time, save the certificate request to a file, and submit it to the parent CA later, after the parent CA is installed and running. After parent CAs are installed and running, you can submit the certificate request file by using the Advanced Certificate Request Web pages for the parent CA. After the certificate for the child CA is issued, you can install the certificate for the child CA by using the Certification Authority console. A CA must have a valid CA certificate to start.

Although you can install CAs on domain controllers, it is not a recommended practice. To distribute the network load and prevent excessive load conditions on computers, install CAs on Windows 2000 Server–based computers that are dedicated to providing CA services. Also consider installing the Web Enrollment Support pages on separate Windows 2000 Server–based computers.

For information about installing third-party CAs and using them with Windows certification hierarchies, see the documentation for the third-party CA product.

Upgrading from Certificate Server 1.0

If you upgrade a Windows NT 4.0–based server that is running Certificate Server 1.0 to Windows 2000 Server, Certificate Server 1.0 is upgraded automatically to the new version of Certificate Services. If the CA being upgraded is using a policy module other than the default policy module for Certificate Server 1.0, it continues to use its old policy module, which is referred to as the Legacy policy module. If the CA you are upgrading uses the default policy module that was provided with Certificate Server 1.0, the upgraded CA uses the Certificate Services stand-alone policy.

If you are not upgrading a Certificate Server 1.0 CA and, instead, are installing a separate Windows 2000 CA that is to replace the old CA, you might want to use the older policy module instead of the default policy module that is provided with Certificate Services. If you want to replace the policy module that is provided with Certificate Services with a custom policy module or a policy module developed for Certificate Server 1.0 and Windows NT 4.0, you must first register the policy module DLL file by using the **Regsrv32** command, and then select the policy module by using the Certification Authority console. For more information about using Regsv32 and selecting policy modules, see Windows 2000 Server Help and Certificate Services Help.

Creation of an Issuer Statement for the Certification Authority (Optional)

When you install a CA, you have the option of adding an issuer statement for the CA that appears when users click **Issuer Statement** in the **Certificate General** dialog box. The issuer statement is a policy statement that gives legal and other pertinent information about the CA and its issuing policies, limitations of liability, and so forth.

The issuer statement file must be installed on the server before you install Windows 2000 Certificate Services. This file, named Capolicy.inf, must be placed in the directory in which Windows 2000 Server is installed — the *systemroot* directory. (The default *systemroot* is C:\Winnt.) CAPolicy.inf can contain the text you want to be displayed as the policy statement, or it can contain a URL that points to the policy statement, for example, a Web page. For more information about how to create the Capolicy.inf file, see Certificate Services Help.

Installing Windows 2000 Certificate Services

Before you can install a CA, you must be logged on as either a member of the local Administrator security group for stand-alone computers or a member of the Domain Administrator security group for computers that are connected to the domain.

To install Windows 2000 Certificate Services

1. In Control Panel, click **Add/Remove Programs**.

   The **Add/Remove Programs** dialog box appears.

2. Click **Add/Remove Windows Components**.

   The Windows Component wizard appears.

3. In Windows Components, select the Certificate Services check box.

4. Click **Next**, and use the Windows Component wizard to install the CA.

Tables 16.5 through 16.9 describe the available CA configuration options for each page of the Windows Component wizard.

Note After the CA is installed, the computer cannot be renamed, joined to a domain, or removed from a domain. Installing an enterprise CA requires Active Directory, so the CA computer must already be joined to the Windows 2000 domain.

Table 16.5 Certification Authority Type Selection Page

Option	Description
Enterprise root CA	Select to install an enterprise root CA.
Enterprise subordinate CA	Select to install an enterprise subordinate CA.
Stand-alone root CA	Select to install a stand-alone root CA.
Stand-alone subordinate CA	Select to install a stand-alone subordinate CA.
Advanced options	Select to configure advanced options in the **Public and Private Key Selection** page of the wizard.

Table 16.6 Public and Private Key Selection Page

Option	Description
Cryptographic service provider	Select the CSP to be used to generate the public key and private key set for the CA certificate. This CSP also manages and stores the private key. The default CSP is the Microsoft Base Cryptographic Provider or the Microsoft Enhanced Cryptographic Provider, depending on whether the server that is running Windows 2000 contains exportable or nonexportable cryptography. If you want to use another CSP, such as a hardware-based CSP to manage and store the CA's private key, you must select the appropriate CA from the list of CSPs.
Hash algorithms	Select the message digest that is to be used for the digital signature of the CA certificates. The default is SHA-1, which provides the strongest cryptographic security.
Key length	Select a key length from the list, or type a key length for the private key and public key. The default key length is 512 bits for the Base Cryptographic Provider and 1,024 bits for the Enhanced Cryptographic Provider. The minimum key length you can specify is 384 bits, and the maximum is 16,384 bits. Use a key of at least 1,024 bits for CAs. In general, the longer the key, the longer the safe lifetime of the private key. Use the longest key that is feasible and that meets both CA performance requirements and CSP key storage limitations.
Use existing keys	Enables the selection of an existing private key from the list. The existing private key is used for the CA. You might need to use this option to restore a failed CA.
Use the associated certificate	Enables the selection of the certificate that is associated with the existing private key which is used for the CA. This option is not available unless you first select **Use the associated certificate**. You might need to use this option to restore a failed CA.
Import	Imports a private key that is not in the **Use existing keys** list. For example, you might import a private key from an archive for a failed CA.
View Certificate	Select this option to view the certificate associated with the private key in the **Use existing keys** list.

Table 16.7 CA Identifying Information Page

Option	Description
CA nameOrganizationOrganizational unitLocality State or province Country/region E-mail	Enter information that is to be used to uniquely identify the CA. This information is included in the CA certificate in the Subject field. The **CA name** that you enter here is used by Windows 2000 to identify the CA, so the **CA name** must be unique for each CA you install in your organization. However, all of the other information that is entered here can be the same if appropriate. Others can view the Subject field in the CA certificate to identify the CA or to find out how to contact the CA.
CA description	Enter a description for this CA (optional).
Validity duration	Enter the duration for the certificate lifetime for the root CA certificate, and select **Years**, **Months**, or **Weeks** from the list. The default certificate lifetime for root CAs is 2 years. You must choose a lifetime that supports your planned certificate life cycles. This option is not available for subordinate CAs because the certificate lifetime is determined by the parent CA.
Expires on	Lists the expiration date for the root CA certificate, which corresponds to the certificate lifetime in **Validity duration**.

Table 16.8 Data Storage Location Page

Option	Description
Certificate database Certificate log	By default, the certificate database and the log are installed at <*Drive*:>\WINNT\System32\CertLog, where <*Drive:*> is the letter of the disk drive where the CA is installed. You have the option of storing the database and the log on different drives to manage storage space. If this is something you want to do, type the new path and folder name in the **Certificate database** box or in the **Certificate log** box, or click **Browse** to select the new location.
Store configuration	Select to store configuration information in a shared folder, and then type the path and folder name

information in a shared folder	in the **Shared folder** box; or click **Browse** to select an existing folder. Members of the local Administrators security group are granted full control for the folder. Members of the Everyone security group are granted read permissions for the folder. The shared folder acts as a location where users can find information about certification authorities. This option is useful only if you are installing a stand-alone CA and do not have Active Directory.
Preserve existing certificate database	Select to preserve an existing certificate database. This option is available only when you are reusing a private key and the associated certificate from an existing CA configuration. You can use this option to restore a failed CA.

Table 16.9 CA Certificate Request Page (Subordinate CAs Only)

Option	Description
Send the request directly to a CA already on the network	Type the name of the parent CA, or click **Browse** to select the parent CA from a list of CAs. The certificate request is submitted to this CA, and the certificate is then processed and issued to the subordinate CA. If you make a request from a stand-alone CA, the CA is not certified automatically. An administrator must approve the certificate request before the CA can issue the certificate. You must later use the Certification Authority console to install the CA's certificate.
Save the request to a file	Select to save the request to a file, and then type the path and file name in the **Request file** box; or click **Browse** to select the file location. This option saves the certificate request to a request file that you can submit to an offline CA for processing. The CA is not certified automatically. You must later use the Certification Authority console to install the CA's certificate.

Configure Certification Authorities

You can use the Certification Authority console to configure CAs. This includes the following tasks:

- Installing the CA certificate when necessary.
- Configuring exit module settings.
- Configuring policy module settings.
- Scheduling certificate revocation list publication.
- Modifying security permissions and delegate control of CAs.
- Enabling optional Netscape-compatible Web-based revocation checking.

For more information about how to use the Certification Authority console to perform these tasks, see Certificate Services Help.

Installation of the Certification Authority Certificate

If you requested a certificate for a subordinate CA from an offline CA during the installation process, you must later obtain the CA certificate and install it to certify the CA. The CA does not run until the CA certificate is installed. You do not have to do this for root CAs or subordinate CAs that received the certificate from an enterprise CA during the installation process.

To obtain the CA certificate, use the **Submit a Saved Request** page of the Web Enrollment Support pages to submit the certificate request file that was created during the installation process. When the **Issued Certificate** page appears, click **Install this certification path** to install the certification path file for the CA. Then use the Certification Authority console to install the certification path file and certify the CA.

To use the Certification Authority console to install the CA certificate, right-click the CA node. Click **All Tasks,** and then click **Install CA Certificate**. The CA certificate is installed from the issuing parent CA, and then the CA service starts.

Configuration of Policy Module Settings

If the default policy module settings described in this section meet your needs, no further configuration is necessary. To configure the policy module setting by using the Certification Authority console, right-click the CA node and then click **Properties**. When the **CA Properties** dialog box appears, click **Policy Module** and then click **Configure**. When the **Properties** dialog box appears, modify the following settings as necessary.

Default Action (for Stand-alone Certification Authorities)

By default, the **Set the certificate request to pending** check box is selected and the request is held as pending until an administrator approves it for stand-alone CAs. Click **Automatically approve the certificate requests** to configure a stand-alone CA to issue each valid certificate request automatically. Note, however, that this is a major security risk and, thus, is not recommended. This option does not apply for enterprise CAs.

X.509 Extensions

You can click **Add** or **Remove** to modify the CRL distribution points that are listed in the **CRL Distribution Points** box. For example, to ensure that users have convenient access to CRLs, you can add a CRL distribution point for commonly used public folders and the URL for a page on your internal Web site. The CA writes these CRL distribution points into every certificate that it issues to support certificate revocation checking by applications such as Internet Explorer. You must also configure an exit module for the CA to publish its CRLs to any CRL distribution points you add. To disable a CRL distribution point that is listed in the **CRL Distribution Points** box, you can clear the check box next to it.

You can click **Add** or **Remove** to modify the certificate distribution points that are listed in **Authority Information Access**. For example, to ensure that users have convenient access to the certificate for a specified CA, you can add a certificate distribution point for frequently used public folders and the URL for a page on your internal Web site. The certificate for this CA is published to these certificate distribution points. In addition, the CA writes these certificate distribution points into every certificate that it issues. To disable a certificate distribution point that is listed in **Authority Information Access**, you can clear the check box next to a certificate distribution point. When you view the Certification Path dialog box for a certificate that is issued by this CA, and you select the CA's certificate in the path and click **View**, the system looks for the certificate in the order the certificate distribution points are listed in **Authority Information Access**.

Configuration of Exit Module Settings

If the default exit module settings described in this section meet your needs, no further configuration is necessary. To configure the active exit modules with the Certification Authority console, right-click the CA node, and then click **Properties**. When the **CA Properties** dialog box appears, click **Exit Module,** and then click **Add** or **Remove** to modify the active modules that are listed in **Active exit modules**. If you use custom exit modules that you have developed or exit modules provided by third-party vendors, you

must install the exit module as an active module.

Install additional exit modules if you want to publish certificates and CRLs to different locations than those that are supported by the default enterprise and default stand-alone exit modules. For example, you might install a custom exit module to publish certificates to a Web page or to a third-party directory service.

No matter what exit modules are installed, certificates are not published unless the publication location is specified in the certificate request. The exit modules enable certificates to be published to the locations specified in certificate requests.

To configure an exit module's settings with the Certification Authority console, right-click the CA node, and then click **Properties**. When the *CA name* **Properties** dialog box appears, click **Exit Modules**. Select the module you want to configure, and then click **Configure**. When the **Properties** dialog box appears, modify the options that are described in Table 16.10.

Table 16.10 Certificate Publication

Option	Description
Allow certificate publication to Active Directory	By default, this option is selected for the default enterprise exit module. If you do not want to publish certificates or CRLs to Active Directory, clear the check box associated with this option. This option is not available for the default stand-alone exit module.
Allow certificate publication to the file system	By default, this option is selected for the default stand-alone exit module. If you do not want to publish certificates or CRLs to the file system, clear the check box associated with this option. By default, the check box for this option is cleared for the default enterprise exit module. If you want to enable certificates to be published to the file system, select the check box associated with this option.

For enterprise CAs, certificates are published to Active Directory as long as the default exit module is active and configured to publish certificates to Active Directory (the default setting). For stand-alone CAs, certificates are published to the local file system as long as the default exit module is active and configured to allow certificates to be published to the local file system (the default setting).

Scheduling Certificate Revocation List Publication

If the default CRL publication schedule meets your needs (a new CRL is published every week), no further configuration is necessary. The following are some examples of how you might modify the default CRL publication:

- Schedule daily rather than weekly publication of CRLs because you expect a high rate of certificate revocations or because you want to ensure greater protection of valuable information that is being protected by public key security functions.
- Schedule biweekly or monthly publication of CRLs because you expect a low rate of certificate revocations.
- Turn off automatic CRL publication for offline CAs, such as stand-alone root CAs or stand-alone intermediate CAs, and instead publish CRLs manually.

To change the CRL publication schedule with the Certification Authority console, right-click the **Revoked Certificates** node of the CA, and then click **Properties**. When the **Revoked Certificate Properties** dialog box appears, configure the CRL publication options that are described in Table 16.11.

Table 16.11 CRL Publishing Parameters

Option	Description
Publish Interval	Type the interval and select **Hours**, **Days**, **Weeks**, **Months**, or **Years**. For example, to schedule biweekly CRL publication, type **2** and select **Weeks**.
Next Publish	Displays the time that the next CRL is scheduled to be published.
Disable Scheduled Publishing	Select to turn off automatic CRL publishing for this CA.
View Current CRL	Select to view the most current CRL for this CA.

Configuration of Certificates to Be Issued

When an enterprise CA is installed, the default issuing policy is configured to issue the following certificate types: Administrator, Domain Controller, Computer, Basic EFS, EFS Recovery Agent, User, Subordinate Certification Authority, and Web Server. You can configure each CA's issuing policy to meet the needs of your organization.

Before you can issue other certificate types besides the default, you must use the Certification Authority console to add the certificate type to the issuing policy. You can also use the Certification Authority console to delete certificate types from an enterprise CA's issuing policy. For example, you might modify the certificate issuing policy for a root or an intermediate CA to issue only Subordinate Certification Authority certificates. You might configure an issuing CA by adding the Trust List Signing certificate type to the default issuing policy and by deleting the Subordinate Certification Authority certificate type from the default issuing policy. You might want to configure a CA to issue only the Enrollment Agent certificate. You can also configure an issuing CA so that it issues only the Smart Card Logon and Smart Card User certificates to support the deployment of smart cards.

To add a certificate type to issuing policy with the Certification Authority console, right-click the **Policy Settings** node of the CA. Click **New**, and then click **Certificate to Issue**. When the **Select Certificate Template** dialog box appears, select one or more of the listed certificate templates, and then click **OK**. The selected certificate templates are added to the issuing policy.

When you select the **Policy Settings** node of a CA, the certificate types that the CA can issue are displayed in the details pane of the console. To delete a certificate template from the issuing policy, select the certificate template and press the DELETE key; or right-click the certificate template, and then click **Delete**.

Permission to enroll for each certificate type is controlled by the ACLs for each certificate template, as described in "Modify the Default Security Permissions for Certificate Templates (Optional)" later in this chapter. You also can use the Certification Authority console to modify security settings for a CA to prevent some users or members of some security groups from enrolling for certificates from that CA.

Modification of Security for a Certification Authority

By default, members of the local Administrators and Authenticated Users security groups and members of the global Domain Admins and Enterprise Admins security groups are granted Enroll permissions, so they can request certificates from the CA. This means that by default all users in the domain can request certificates from the CA for all certificate types that they are authorized to receive. In addition, members of the local Administrators security group and members of the global Domain Admins and Enterprise Admins security groups are granted Manage permissions for the CA. If the default security for the CA meets your needs, no further configuration is necessary.

To configure new security settings for a CA by using the Certification Authority console, right-click the CA node, and then click

Properties. When the **CA Properties** dialog box appears, click **Security,** and then modify the security settings as needed. Click **Add** or **Remove** to change the user accounts or security groups that are listed. When you select a security group or a user account from the list, the corresponding permissions appear in the **Permissions** box.

To change basic permissions, select a security group or a user account from the list, and then select or clear the appropriate check boxes next to the basic permissions in the **Permissions** box. You can select permissions check boxes in either the **Allow** or **Deny** columns. If you select a check box in the **Allow** column, the corresponding permissions are granted to the selected security group. If you select a check box in the **Deny** column, the corresponding permissions are denied to the selected security group.

To modify advanced permissions, click **Advanced**. When the **Permissions** dialog box appears, click **Add** or **Remove** to change the security groups or user accounts that are listed. Select a security group or a user account, and then click **View / Edit** to modify the advanced permissions.

Table 16.12 contains descriptions of the permissions you can configure for a CA. All of the permissions can be modified in the advanced **Permissions** dialog box.

Table 16.12 Permissions for Certificate Templates

Permission	Description
Manage (basic)	Determines which user accounts and security groups can manage the CA with the Certification Authority console or run command-line programs. By default, members of the local Administrators security group and members of the global Domain Admins and Enterprise Admins security groups are granted these permissions.
Enroll (basic)	Determines which user accounts and security groups can request certificates from the CA. By default, members of the local Administrators and Authenticated Users security groups and members of the global Domain Admins and Enterprise Admins security groups are granted these permissions.
Read (basic)	Determines which user accounts and security groups can read configuration information for the CA. By default, members of the local Administrators and Authenticated Users security groups and members of global Domain Admins and Enterprise Admins security groups are granted these permissions.
Write Configuration (advanced only)	Determines which user accounts and security groups can change configuration data for the CA. By default, these permissions are granted to all user accounts and security groups with Manage permissions.
Read Control (advanced only)	Determines which user accounts and security groups have read permission to view the security settings for the CA. By default, these permissions are granted to all user accounts and security groups with Read Configuration permissions.
Modify Permissions (advanced only)	Determines which user accounts and security groups can change permissions for CA security. By default, these permissions are granted to all user accounts and security groups with Manage permissions.
Modify Owner (advanced only)	Determines which user accounts and security groups can change the owner of the CA object. By default, these permissions are granted to all user accounts and security groups with Manage permissions.
Revoke Certificates (advanced only)	Determines which user accounts and security groups can revoke certificates. By default, these permissions are granted to all user accounts and security groups with Manage permissions.
Approve Certificates (advanced only)	Determines which user accounts and security groups can approve certificate requests for stand-alone CAs. By default, these permissions are granted to all user accounts and security groups with Manage permissions.
Read Database (advanced only)	Determines which user accounts and security groups can gain access to and read the information in the certificate database. By default, these permissions are granted to all user accounts and security groups with Manage permissions.

Enabling Netscape-compatible Web-based Revocation Checking

Netscape-compatible Web browsers support a proprietary online certificate revocation checking method that checks for revoked certificates at a location that is listed in an extension field of the certificate. To enable Netscape-compatible, Web-based revocation check extensions to be added to every certificate, run the following **Certutil** command from the command prompt on the CA server:

```
certutil -SetReg Policy\RevocationType +AspEnable
```

Then stop and start the Certification Authority service. Certificates that are issued by the certification authority after it is restarted contain the extension.

Modify the Default Security Permissions for Certificate Templates (Optional)

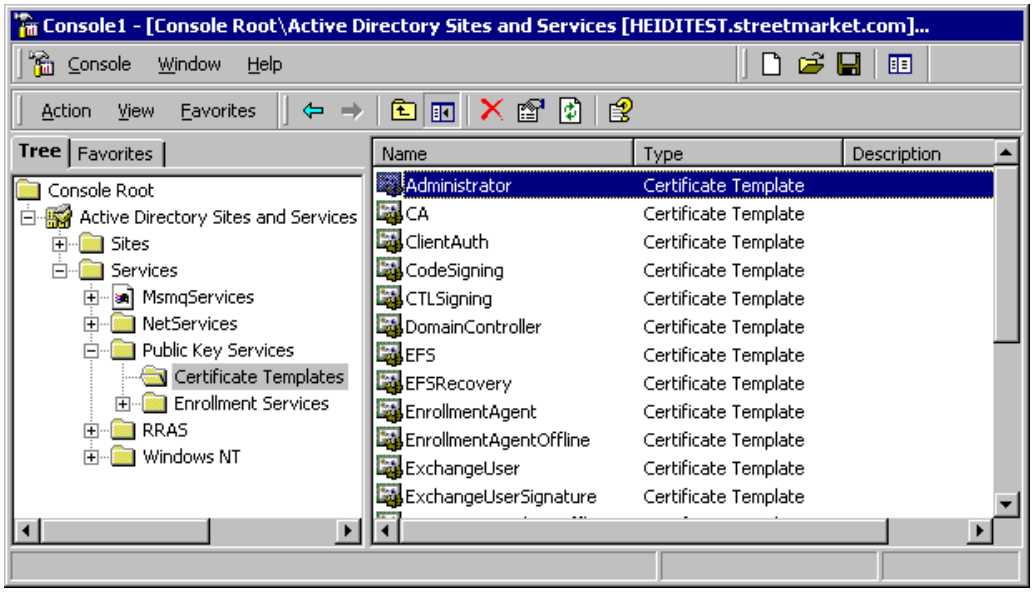
For enterprise CAs, Enroll permissions are controlled by ACLs for each certificate template. An enterprise CA grants certificate requests only for user accounts or computer accounts with Enroll permissions. The ACLs for certificate template are preconfigured to enable various security groups to enroll for certificate types.

By default, members of the Domain Admins security group for the domain where the CA is installed are granted Enroll permissions for all certificate types. Members of the Domain Users security group for the domain where the CA is installed are granted Enroll permissions for the following certificate types: Basic EFS, Authenticated Session, Exchange User, Exchange Signature Only, User, and User Signature Only. Members of the Enterprise Admins security group are granted Enroll permissions for all certificate types except for the Basic EFS, Authenticated Session, Exchange User, Exchange Signature Only, User, and User Signature Only.

If you want to enable other security groups to enroll for certificates, you must edit the ACLs for the certificate templates (for the domain where the CA is installed) to add the security group and assign Enroll permissions to them. In addition, if you want security groups in another domain to be able to enroll for certificates from an enterprise CA, you must add the other domain's security group to the ACLs of the certificate templates for the domain where the CA is installed.

You can use the Active Directory Sites and Services console (an MMC snap-in) to modify the ACLs for certificate templates. Before the Certificate Templates container appears, you must point to the Active Directory Sites and Services console and then click **View** and **Show Services Node**. For more information about how to use the Active Directory Sites and Services console, see Active Directory Help.

To show the Certificate Templates container, expand the Services container and the Public Key Services container, as shown in Figure 16.11.



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

Figure 16.11 Certificate Templates Container

To edit ACLs for a certificate template, click **Certificate Templates**. Then, right-click the certificate template in the details pane, and click **Properties**. When the **Certification Authorities Properties** dialog box appears, click **Security** and modify the security permissions as needed. For more information about how to edit ACLs for certificate templates, see Certificate Services Help.

For example, to ensure that only a few trusted individuals can obtain an Enrollment Agent certificate, you might modify the ACLs for the Enrollment Agent certificate template to delete the default security groups and add a special security group with Enroll permissions. You might also modify the ACLs for the Code Signing certificate template so that only certain developers who are members of a special code signers security group can enroll for code singing certificates.

Note When you change the ACLs for certificate templates, the changes might take a few minutes to replicate to other domain controllers.

Install and Configure Support Systems or Applications

You must install any systems or applications that are required to support the public key infrastructure. Supporting systems and applications can include the following:

- Smart card readers at local computers.
- Secure mail and key management systems.
- Custom certificate enrollment and renewal applications.
- Training and support Web sites to educate users about certificate services and to provide customer support for users.
- Third-party public key infrastructure and certificate services.

Configure Public Key Group Policy

You can use the Group Policy console to configure Public Key Group Policy for sites, domains, and organizational units or local computer policy. Most features of the public key infrastructure and certificate services work without your having to configure Public Key Group Policy settings. However, you must configure Public Key Group Policy if you want to do any of the following:

- Use automatic enrollment for computer certificates.
- Add trusted root certificates for groups of computers.
- Create CTLs for computers and users.
- Designate EFS recovery agent accounts.

To add a Group Policy console to MMC

1. Open MMC.
2. Click **Console**, and then click **Add/Remove Snap-in**, or press CTRL+M.

   The **Add/Remove Snap-in** dialog box appears.
3. Click **Add**.

   The **Add Standalone Snap-in** dialog box appears.
4. Select **Group Policy** from the list of snap-ins, and then click **Add**.

   The **Select Group Policy Object** dialog box appears, with Local Computer listed in the **Group Policy Object** box.
5. Click **Finish** to manage local computer policy.

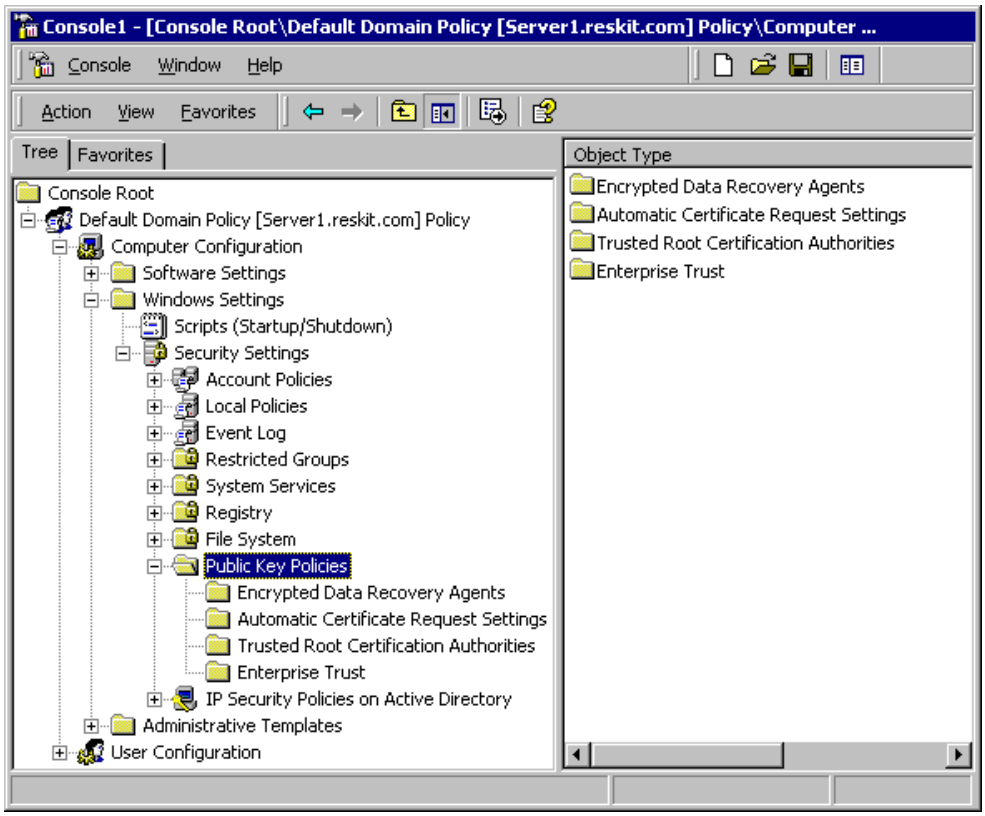
   – Or –

   Click **Browse** to select another Group Policy (or to create and select a new Group Policy), and then click **Finish** to manage the selected Group Policy.

   The **Add Standalone Snap-in** dialog box appears. Click **Add** again to add multiple Group Policy snap-ins.
6. When you are finished adding snap-ins, on the **Add Standalone Snap-in** dialog box, click **Close**.

   The **Add/Remove Snap-in** dialog box appears and displays the snap-ins that are to be installed in MMC.
7. In the **Add/Remove Snap-in** dialog box, click **Close**.

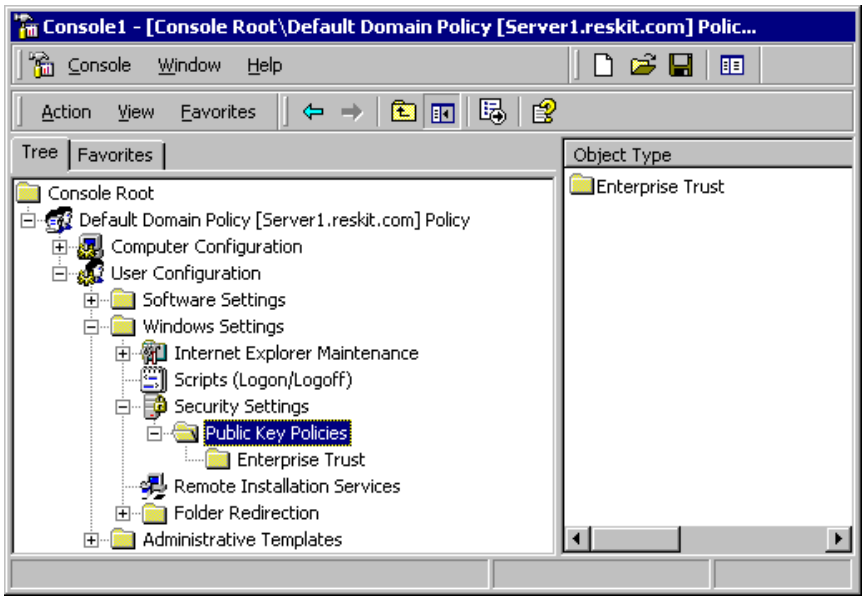
For Group Policy for sites, domains, and organizational units, there is a Public Key Policy container for both computers and users. Figure 16.12 shows an example of the Public Key Policies container for computers in the Default Domain Policy. To display the Public Key Policies containers for computers, expand the **Computer Configuration** node, expand the **Security Settings** node, and then click **Public Key Policies**.



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

Figure 16.12 Public Key Policies for Computers

Figure 16.13 shows the Public Key Policies container for users in the Default Domain Policy. To display the Public Key Policies containers for users, expand the **Computer Configuration** node, expand the **Security Settings** node, and then click **Public Key Policies**.



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

Figure 16.13 Public Key Policies for Users

The Public Key Policies containers are used for the following tasks:

- **Automatic Certificate Request Settings** for configuring autoenrollment for computer certificates.
- **Trusted Root Certification Authorities** for adding trusted root CA certificates to the Trusted Root Certification Authorities store.
- **Enterprise Trust** for configuring CTLs. (This is the only container that appears for users.)
- **Encrypted Data Recovery Agents** for configuring EFS recovery agents. (This is the only container that appears for Local Computer policy.)

For users, you can configure CTLs only. For Local Computer policy, you can configure EFS Recovery Agents Policy only. For more information about how to configure Public Key Group Policy, see Certificate Services Help and Group Policy Reference.

Note Changes to Group Policy do not take effect immediately. User and computer Group Policy is refreshed periodically (every 90 minutes, by default), when users log on, and when computers are started. You also can use the Secedit /refreshPolicy command-line option to refresh policy settings manually from the command prompt at each local computer.

Automatic Certificate Enrollment

You can specify automatic enrollment and renewal for computer certificates. When autoenrollment is configured, the specified certificate types are issued automatically to all computers within the scope of the Public Key Group Policy. Computer certificates that are issued by autoenrollment are renewed automatically from the issuing CA. Autoenrollment does not function unless at least one enterprise CA is online to process certificate requests.

To configure autoenrollment, in the **Public Key Policies** node, right-click the **Automatic Certificate Request Settings** node, and then click **New** and **Automatic Certificate Request**. When the Automatic Certificate Request wizard appears, configure autoenrollment by using the options that are described in Table 16.13.

Table 16.13 Automatic Certificate Request Wizard

Option	Description
Certificate Template page	Select a certificate template in the **Certificate templates** box, and then click **Next**. All computers that are within the scope of the autoenrollment policy with Enroll permissions for this certificate template are issued that certificate type the next time the computer restarts and logs on to the domain.
Certification Authority page	Select the check box next to one or more CAs that are listed in the **Certification authorities** box. If you select multiple CAs, certificate requests for autoenrollment are processed by the first CA that is available. After selecting the CAs, click **Next** and complete the wizard.

Root Certificate Trust

When you install an enterprise root CA or a stand-alone Root CA, the certificate of the CA is added automatically to the Trusted Root Certification Authorities Group Policy for the domain. You also can add certificates for other root CAs to Trusted Root Certification Authorities Group Policy. The root CA certificates that you add become trusted root CAs for computers within the scope of the Group Policy. For example, if you want to use a third-party CA as a root CA in a certification hierarchy, you must add the certificate for the third-party CA to the Trusted Root Certification Authorities Group Policy.

To add a certificate for the root CA to the Trusted Root Certification Authorities Group Policy, in the **Public Key Policies** node, right-click **Trusted Root Certification Authorities**, and then click **All Tasks** and **Import**. When the Certificate Import wizard appears, use the wizard to import a certificate file for the certificate of the root CA and add it to Group Policy. The certificate is added to the **Trusted Root Certification Authorities** store of all computers within the scope of Group Policy the next time it is refreshed on each computer.

Certificate Trust Lists

You can create CTLs to trust specific CAs and to restrict the uses of certificates issued by the CAs. For example, you might use a CTL to trust certificates that are issued by a commercial CA and restrict the permitted uses for those certificates. You might also use CTLs to control trust on an extranet for certificates that are issued by CAs that are managed by your business partners. You can configure CTLs for computers and for users.

Before administrators can create CTLs, they must have a valid trust list signing certificate, such as the Administrator certificate or the Trust List Signing certificate that are issued by enterprise CAs. The trust list signing private key for the administrator is used to sign the CTL for integrity. If the trust list signing certificate for an administrator is invalid, all CTLs that have been created and signed by that administrator also are invalid.

To create a CTL for computers or for users, in the **Public Key Policies** node (for the **Computer Configuration** node or for the **User Configuration** node), right-click the **Enterprise Trust** node, and then click **New** and **Certificate Trust List**. When the Certificate Trust wizard appears, configure the CTL by using the options that are described in Tables 16.14 through 16.18.

Table 16.14 Certificate Trust List Purpose Page

Option	Description
Type a prefix that identifies this CTL (optional)	Enter an option prefix for the CTL. This prefix is used to identify the CTL.
Valid duration (optional)	Specify an optional lifetime for the CTL. Enter the number of months in the **Months** box and the number of days in the **Valid duration (optional)** box. If you do not specify a lifetime, the CTL expires when the trust list signing certificate expires.
Designate Purposes	Select a check box next to one or more of the listed purposes in the **Designate purposes** box. The CTL establishes trust only for certificates that are valid for the selected purposes. A certificate might support all of the listed purposes, but you can restrict the purposes for which certificates are trusted.
Add Purpose	Click to add purposes to the **Designate purposes** box. When the **User Defined Purpose** dialog box appears, enter an object identifier for the new purpose in the **Object ID** text box.

Table 16.15 Certificates in the CTL Page

Option	Description
Current CTL Certificates	Displays the certificates of the root CAs that are to be trusted by this CTL. Certificates with certification paths to this root CA are trusted for all designated purposes specified by the CTL.
Add from Store	Adds a root certificate from the Trusted Root Certification Authorities store. When the **Select Certificate** dialog box appears, select all of the certificates that you want to add, and then click **OK**.
Add from File	Adds a root CA's certificate from a file.
Remove	Deletes the certificate that is selected in the **Current CTL Certificates** box.
View Certificate	Select this option to view the certificates that are selected in the **Current CTL Certificates** box.

Table 16.16 Signature Certificate Page

Option	Description
Use this certificate	Displays the trust list signing certificate for the private key that is to be used to sign the CTL.
Select from Store	Adds a trust list signing certificate from the Personal store for the administrator. When the **Select Certificate** dialog box appears, select the certificates you want to use, and then click **OK**.
Select from File	Adds the trust list signing certificate from a file.
View Certificate	Select this option to view the certificate listed in the **Use this certificate** box.

Table 16.17 Timestamping Page

Option	Description
Add a timestamp to the data	Adds a timestamp to the CTL. The timestamp is used to determine the valid lifetime of the CTL. If a timestamp is not used, the computer clock is used instead.
Timestamp service URL	Type the URL for a timestamp service that is to be used for the timestamp.

Table 16.18 Name and Description Page

Option	Description
Friendly Name	Type the optional name that is to appear in MMC when the CTL is displayed. To help you distinguish between CTLs, choose unique friendly names for all of the CTLs that you create.
Description	Type an optional description to describe this CTL. This description can let others know the purpose of the CTL.

EFS Recovery Agents

By default, the local Administrator users account for the first domain controller that is installed in the domain is the EFS recovery account for that domain. You can specify alternative recovery agents for EFS. Use the Group Policy console to designate alternative EFS recovery agents by adding the EFS Recovery Agent certificates into Public Key Group Policy, which means you must first issue EFS Recovery Agent certificates to designated recovery agent user accounts on local computers.

When you are configuring the EFS recovery settings, you have two choices: you can add recovery agent certificates that are published in Active Directory, or you can add recovery agent certificates from a file that is located on a disk or in a shared folder that is available from the computer where you are configuring Public Key settings. If you add recovery agent certificates from files, you must first export the appropriate certificates to the disk or shared folder that is to be used to add the files during the EFS recovery Group Policy configuration process.

To add an EFS recovery agent, in the **Public Key Policies** node, right-click **Encrypted Data Recovery Agents**, and then click **Add**. When the Add Recovery Agent wizard appears, add the appropriate recovery agent certificates by using the options described in Table 16.19.

Table 16.19 Add Recovery Agent Wizard

Option	Description
Recovery agents	Displays the certificates you choose for recovery agents.
Browse Directory	Browses Active Directory and adds a recovery agent certificate for a user account. Use this option when the certificate is published in Active Directory.
Browse Folders	Adds a recovery agent certificate from a file.

When you select **Encrypted Data Recovery Agents**, the EFS recovery agent certificates that are applied by Group Policy appear in the details pane of the console. These are the recovery agent certificates that are used by EFS within the scope of Group Policy. To delete an recovery agent certificate from the Group Policy settings, select the certificate. Next, either press DELETE, or right-click the certificate template, and then click **Delete**.

Install Web Enrollment Support on Another Computer (Optional)

You can install Windows 2000 Certificate Services with the Web Enrollment Support pages on the same server as the CA (the default configuration for the CA installation process). You also have the option of installing the Web Enrollment Support pages on another Windows 2000–based server. Installing the CA and the Web Enrollment Support package on different computers reduces the load that would otherwise be required for the CA computer. You might choose this option when the CA must support a high volume of certificate services traffic or when you are installing certificate services on less powerful computers.

The Web Enrollment Support pages are installed at the following location:

`<Drive:>\WINNT\System32\CertSrv`

where <*Drive*:>\ is the letter of the disk drive where the Web Enrollment Support pages are installed.

Folder CertSrv contains Web files (Active Server Page files, graphics files, and so forth) and two folders (CertEnroll and CertControl) that contain additional support files and ActiveX controls for the Web pages.

Trusting the Computer for Delegation

For enterprise CAs, the Web Enrollment Support pages work from a computer other than the CA computer only if the computer (where the Web Enrollment Support pages are installed) is trusted for delegation. You do not need to trust the other computer for delegation for the Web Enrollment Support pages to work with stand-alone CAs.

You can trust a computer for delegation by using the Active Directory Users and Computers console. Before you can install the Web Enrollment Support pages, you must be logged on to the computer as a member of the Domain Admins security group.

To trust a computer for delegation

1. Expand the Active Directory Users and Computers node for the domain.
2. Select the container with the computer that you want to trust.

   The computers in the container appear in the details pane of the console.
3. Double-click the computer that you want to trust.

   The **Properties** dialog box for that computer appears.
4. In the **General** dialog box, click **Trust computer for delegation** to select the check box, and then click either **OK** or **Apply**.
5. Restart the computer so that the new delegation setting can take effect.

   The Web Enrollment Support pages will not work until after the computer has been restarted.

For more information about the Active Directory Users and Computers console, see Active Directory Help.

Installing the Web Enrollment Support Pages

You can use the Windows Components wizard to install the Web Enrollment Support pages on another computer other than where the CA is installed. Before you can install the Web Enrollment Support pages, you must be logged on to the computer as a member of the Domain Admins security group. You can install the Web Enrollment Support pages only on a Windows 2000–based server on which Internet Information Services is installed.

To install Web Enrollment Support pages on a computer other than where the CA is installed

1. In Control Panel, click **Add/Remove Programs**.

   The **Add/Remove Programs** dialog box appears.
2. Click **Add/Remove Windows Components**.

   The Windows Components wizard appears.
3. In the **Windows Components** page, select the **Certificate Services** check box.
4. Click **Details**, and then clear the **Certificate Services** check box. Verify that the **Certificate Services Web Enrollment Support** check box is selected, and then click **OK**.
5. Click **Next**.

   The **Certificate Services Client Configuration** page appears.
6. Type the domain name of the server computer with the CA in the **Computer Name** box.

   – Or –

   Click **Browse** to locate and select the computer.

   The **CA Name** box displays the name of the CA that is running on the server you have selected. The Web Enrollment Support pages are installed to work with this CA.
7. Click **Next**, and complete the Windows Component wizard.

After the Web Enrollment Support pages are installed, test the Web pages to be sure that they work properly with the CA. For example, use the Web Enrollment Support pages to request a certificate or a CRL from the CA. You might also want to change the default security settings for the Web Enrollment Support pages.

Configure Security for Web Enrollment Support Pages (Optional)

The folders CertSrv, CertEnroll, and CertControl are added as virtual directories to the Default Web Site for Internet Information Services. For enterprise CAs, CertSrv and CertControl are configured for authenticated access with basic authentication and integrated Windows authentication enabled. Authenticated access authenticates users and grants access to Web resources on the basis of the users' Windows 2000 user accounts. Authenticated access is required because enterprise CAs must process certificate requests according to the information that is contained in the requestor's Windows 2000 user account. For stand-alone CAs, CertSrv and CertControl are configured for anonymous access to provide all users with access to the Enrollment Support pages. For enterprise CAs, anonymous authentication is turned off by default; otherwise the Web Enrollment Support pages do not work for enterprise CAs.

Integrated Windows authentication grants access to Web pages on the basis of the logon credentials of the users of Internet Explorer. Users are granted access to the Web pages when their logon credentials match a valid Windows 2000 user account. Integrated Windows authentication is not a part of the HTTP standard and is supported only by Microsoft® Internet Explorer version 2.0 or later and Internet Explorer 5. Integrated Windows authentication does not work across proxy servers or other firewall applications.

If integrated Windows authentication fails because of a firewall or another problem, the browser prompts the user to enter his or her user name and password for basic authentication. Users of third-party browsers also are prompted to enter their user names and passwords for basic authentication.

Basic authentication is a part of the HTTP version 1.0 standard, so most browsers support this authentication method. It grants access to Web pages after users have transmitted their Windows 2000 user names and passwords. However, a user must enter the correct user name and password before access is granted. User passwords are transmitted in plaintext, so they can be intercepted easily by someone who "sniffs" communications between the Web browser and the Web server. For enterprise Web Enrollment Support pages, basic authentication is enabled to ensure that all browsers have access to the Web pages. Because sending passwords as plaintext presents a security risk, you might want to turn off basic authentication or turn on digest authentication.

If you need to support only Internet Explorer, you can use the Internet Information Services console (an MMC snap-in) to configure security for CertSrv and CertControl, which turn basic authentication off and prevent passwords from being transmitted as plaintext. If you need to support other browsers, you can configure security for CertSrv and CertControl to require secure channels with the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. With secure channels, passwords that are sent for basic authentication are encrypted. However, the performance of the Web Enrollment Support pages might be reduced because of the extra load of encryption that is required for secure channels.

Internet Information Services also supports digest authentication, which is a new feature of HTTP version 1.1. With digest authentication, passwords are sent in a secure manner as message digests (hashes) that can be deciphered only by the Windows 2000 Key Distribution Center (KDC) service for Kerberos authentication. If browsers support HTTP version 1.1 (recent version of browsers usually support HTTP version 1.1), you can use the Internet Information Services console (an MMC snap-in) to configure security for CertSrv and CertControl to turn off basic authentication and to turn on digest authentication. If you turn on both basic authentication and digest authentication, digest authentication is used if it is supported by the browser; otherwise basic authentication is used.

If you turn on integrated Windows authentication, basic authentication, and digest authentication, authentication is done in the following order of priority:

1. Integrated Windows authentication

2. Digest authentication
3. Basic authentication

The highest-ranked authentication method that is supported by browsers is used to authenticate users. If anonymous access is turned on, authenticated access is used only when NTFS file protection security has been configured to control access for Web site resources.

To ensure that the Web Enrollment Support pages work correctly with new security configurations, test the Web pages with all versions of the browsers that you intend to support.

For more information about security for Internet Information Services Web sites, see "Choosing Security Solutions That Use Public Key Technology" in this book. For information about how to use the Internet Information Services console to configure security and authenticated access for Web site resources, see Internet Information Services Help.

Integrate with Third-Party Certificate Services (Optional)

The Windows 2000 public key infrastructure is interoperable with various third-party certificate services that comply with the standards recommended by the Public Key Infrastructure X.509 (PKIX) working group of the Internet Engineering Task Force (IETF). However, interoperability between commercially available PKIX-compliant products is not guaranteed because the technology is still in an early stage of development. For more information about interoperability, see "Choosing Security Solutions That Use Public Key Technology" in this book.

In general, Windows 2000 Certificate Services provides many benefits that third-party CAs do not because Certificate Services are fully integrated with the Windows 2000 public key infrastructure and Active Directory. However, you can use third-party certificate services with Windows 2000 to deploy CAs and issue certificates for your organizations.

To work properly with Windows 2000 public key infrastructure, third-party CAs must support industry standard X.509 version 3 certificates and X.509 version 2 certificate revocation lists. X.509-compliant certificates from third-party CAs can be used for most public key–based Windows 2000 security solutions. However, third-party CAs can't be used for features that require enterprise CA integration with Active Directory. For example, third-party CAs can't be used to issue Smart Card Logon certificates or Smart Card User certificates for Windows 2000 domains or to autoenroll certificates for computers.

You can use compliant third-party CAs to form all or part of your certification trust chains. Third-party root CAs are not added automatically to Trusted Root Certification Authorities stores. You can configure Public Key Group Policies to add third-party root CAs to Trusted Root Certification Authorities stores and to create CTLs that trust third-party CAs.

To ensure that third-party certificate services work as intended with the Windows 2000 public key infrastructure, test third-party solutions thoroughly in labs and pilot programs. For more information about the capabilities of specific third-party solutions, contact the appropriate third-party vendors.

Ongoing Certificate Services Tasks

Ongoing tasks for Windows 2000 Certificate Services include the following activities:

- Using the Web Enrollment Support pages.
- Requesting certificates by using the Certificate Request wizard.
- Viewing information about certificates.
- Exporting certificates and private keys.
- Backing up and restoring certification authorities.
- Approving or denying certificate requests.
- Revoking certificates.
- Publishing certificate revocation lists.
- Renewing certification authorities.
- Recovering encrypted data.
- Using the Certificate Services command-line programs.

For more information about how to perform Certificate Services tasks, see Certificate Services Help.

Using the Web Enrollment Support Pages

To use the Web Enrollment Support pages, open the following URL with your Web browser:

http://<*servername*>/certsrv

where <*Servername*> is the name of the server computer where the Web Enrollment Support pages are installed.

When the **Welcome** page appears in your browser window, choose one of the options described in Table 16.20.

Table 16.20 Welcome Page Options

Option	Description
Retrieve the CA certificate or certificate revocation list	Retrieves the CA's certificate or the most current CRL. When you click **Next**, the **Retrieve The CA Certificate or Certificate Revocation List** page appears. You can also use this page to establish trust for the CA on the local computer by installing the certification path for the CA's certificate in the certificate store of the local computer.
Request a certificate	Requests a basic certificate or to submit a certificate request by using advanced options, as described later in this chapter. When you click **Next**, the **Choose Request Type** page appears.
Check on a pending certificate	Checks the status of a pending certificate request and installs the certificate after the request has been approved. When you click **Next**, the **Check On a Pending Certificate Request** page appears. Use this option for certificate requests that are sent to stand-alone CAs. If you don't check the status of pending certificates within 10 days, the pending certificates are not issued and you must request the certificate again.

After you have selected an option, click **Next**. Different Web pages appear for each option.

Choosing the Type of Certificate to Request

You can use the **Choose Certificate Type** page to request user certificates or to submit a certificate request by using the advanced options that are described in Table 16.21.

Table 16.21 Choose Certificate Type Page

Option	Description
User certificate request	Select one of the certificate types listed. For enterprise CAs, you can select **User Certificate**. For stand-alone CAs, you can select either **E-Mail Protection Certificate** or **Web Browser Certificate**. The Web Browser and E-Mail Protection certificates for stand-alone CAs together provide most of the functionality of the User certificate type for enterprise CAs (except for EFS functionality). When you click **Next**, the **User Certificate - Identifying Information** page appears.
Advanced request	Makes a certificate request by using advanced options. When you click **Next**, the **Advanced Certificate Requests** page appears.

After you select an option, click **Next**, and then complete the certificate request process by using the Web pages that appear.

When you request a certificate from an enterprise CA, the CA uses the certificate template and user account information in Active Directory to verify your user account and determine whether to approve or deny the certificate request. However, by default, stand-alone CAs store certificate requests as "pending" until a CA administrator approves or denies the request. Use the stand-alone Web pages to submit a request for a certificate from the stand-alone CA, and then return later to the Web pages to check the status of the pending request. When the request has been approved, you are prompted to install the issued certificate. You can configure stand-alone CAs to grant certificate requests immediately, but this is a significant security risk and is not recommended.

Submitting User Certificate Requests

You can use the **User Certificate - Identifying Information** page to request user certificates by using the options that are described in Table 16.22.

Table 16.22 User Certificate - Identifying Information Page

Option	Description
Identifying Information (stand-alone CAs only)	Enter identification information that is to appear in the certificate including Name, E-Mail, Company, Department, City, State, and Country/region. Enterprise CAs obtain this information from Active Directory. This information is included in the Subject field of the certificate when it is issued.
More options	Displays advanced options for choosing the CSP or for choosing strong private key protection.
Enable strong private key protection	Provides strong private key protection. When this option is selected, the system prompts the user for permission before it performs cryptographic operations with the user's private key.
CSP	The default CSP is the Microsoft Base Cryptographic Provider or the Microsoft Enhanced Cryptographic Provider, depending on whether the Windows 2000–based client that requests the certificate is exportable or not. You have the option of choosing a CSP from the selection list, which is used for the private key. The CSP you choose must support the type of certificate to be issued. For example, a smart card CSP cannot support a Basic EFS certificate.

After you configure options in the **User Certificate - Identifying Information** page, click **Next**. For enterprise CAs, requests are submitted to the CA and approved immediately. For a stand-alone CA, certificate requests are held as "pending" until an administrator approves the certificate request. You must return to the **Welcome** page within 10 days and select the **Check on a pending certificate** option to determine whether a pending certificate request has been approved. When the certificate is issued, the **Issued Certificate** page appears so that you can install the certificate.

Submitting Advanced Certificate Requests

You can use the **Advanced Certificate Requests** page to request certificates by using advanced options that are described in Table 16.23.

Table 16.23 Advanced Certificate Requests Form

Option	Description
Submit advanced requests to this CA using a form.	Submits an advanced certificate request by using a Web form. When you click **Next**, the **Advanced Certificate Request** form appears.
Submit a certificate request using a base 64 encoded PKCS #10 file or a renewal request using a base 64 encoded PKCS #7 file	Submits a certificate request by using a certificate request or a certificate renewal file. When you click **Next**, the **Submit a Saved Request** page appears.
Request a certificate for a smart card on behalf of another user by using the Smart Card Enrollment Station	Requests smart card certificates for other users. When you click **Next**, the **Smart Card Enrollment Station** page appears.

After you select an option, click **Next**, and then use the Web pages that appear to submit the advanced request.

Advanced Certificate Request Form

You can use the **Advanced Certificate Request** form to submit certificate requests by using the options that are described in Table 16.24.

Table 16.24 Advanced Certificate Request Page

Option	Description
Identifying Information(stand-alone CAs only)	Type identification information that is to appear in the certificate, including Name, E-mail, Company, Department, City, State, and Country/region. Enterprise CAs obtain this information from Active Directory. This information is included in the Subject field of the certificate when it is issued.
Intended Purpose(stand-alone CAs only)	Choose the intended purpose of the certificate that is to be requested from the selection.
Certificate Template(enterprise CAs only)	Choose the certificate template from the selection list that is to be used by the

	enterprise CA to process the certificate request and issue the certificate.
CSP	The default CSP is the Microsoft Base Cryptographic Provider or the Microsoft Enhanced Cryptographic Provider, depending on whether the Windows 2000 client that requests the certificate is exportable or not. You have the option of choosing a CSP from the selection list, which is to be used for the private key. The CSP you choose must support the type of certificate that is to be issued. For example, a smart card CSP cannot support a Basic EFS certificate.
Key Usage	Select the basic purpose of the certificate that is to be issued. The options are **Exchange**, **Signature**, or **Both**. If you click **Exchange**, the key can be used for symmetric key exchange only. If you click **Signature**, the key can be used for digital signing only. The default is **Both**, so the key can be used for both purposes.
Key Size	For a Key Usage of Exchange or Both, you can enter a key length from 384 bits to 1,024 bits. The minimum recommended key length is 512 bits. For a Key Usage of Signature, you can enter a key length from 384 bits to 16,384 bits. Key generation for very large signing keys can take a considerable amount of time.
Create new key set	This is selected by default, so a new private key and public key set are created for the issued certificate. Click **Select the container name** to enter a container name for the private key in the **Container name** box.
Use existing key set	Uses an existing private key and public key set. You also can enter the name of the key container in the **Container name** box. You must not reuse private keys if the maximum safe lifetime of the key might be exceeded.
Enable strong private key protection	Provides strong private key protection. When this option is selected, the system prompts the user for permission before it performs cryptographic operations with the user's private key.
Mark keys as exportable	Enables the private key to be exported. Private keys that are used for digital signing (signatures) cannot be enabled for export.
Use local machine store	Stores a certificate that is to be issued in the HKEY_LOCAL_MACHINE subtree of the system registry for the local computer. You must be an administrator to use this option. The default certificate storage location for user certificates is the Personal certificate store for the user. Select this option to request and install computer certificates for the local computer.
Hash Algorithm	Select the message digest (hash) algorithm that is used to sign the certificate request and ensure its integrity. The default algorithm is SHA-1. You can choose another algorithm from the selection list, which is used to sign the certificate request.
Save request to a PKCS #10 file	Saves the certificate request to a file rather than submitting the request to the CA. You must also type a file name in the **File name** box. You can submit the request file to a CA later.
Attributes	Enter additional attributes for the requested certificate in the **Attributes** box. For more information about certificate attributes and the syntax to use, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

For enterprise CAs, the Advanced Certificate Requests form enables you to request all certificate types that are supported by the enterprise CA's certificate issuing policy. Enterprise CAs use certificate templates and information in the logged-on user's user account to process and issue the requested certificates. For offline certificate templates, you must type identifying information in the following fields of the Web form:

- Name
- E-mail
- Company
- Department
- City
- State
- Country/region

This information is included in the Subject field of the certificate when it is issued. For online certificate templates, this information is obtained from the Windows 2000 user account of the logged on user.

For stand-alone CAs, you also can choose the following types of certificates in **Intended Purpose**:

- Secure mail
- Client authentication
- Server authentication
- Code signing
- IP security authentication
- Timestamp signing
- Other

Certificate uses are based on the object identifier contained in the Extended Key Usage field of X.509 version 3 certificates. You can optionally choose Other types of certificates from the selection list and enter the object identifier in the **Usage OID** box. Some object identifiers for certificate types that are not included in the **Intended Purpose** selection list include the following:

- EFS local file encryption (1.3.6.1.4.1.311.10.3.4)
- EFS recovery agent (1.3.6.1.4.1.311.10.3.4.1)
- Certificate Trust List Signing (1.3.6.1.4.1.311.10.3.1)
- Enrollment Agent (1.3.6.1.4.1.311.20.2.1)

For more information about the available types of certificates and their object identifiers, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

After you have configured the options in the **Advanced Certificate Request** page, click **Next**. For enterprise CAs, requests are submitted to the CA and approved immediately. For a stand-alone CA, certificate requests are held as "pending" until an administrator approves the certificate request. You must return to the **Welcome** page within 10 days and select the **Check on a pending certificate** option to determine whether a request has been approved. When the certificate is issued, the **Issued Certificate** page appears so that you can install the certificate.

Submit a Saved Request Page

You can use the **Submit a Saved Request** page to submit a request file to the CA by using the options that are described in Table 16.25.

Table 16.25 Submit a Saved Request Page

Option	Description
Saved Request	Paste the certificate request into the **Saved Request** box, or click **Browse** to locate and select a request file that is to be inserted in **Saved Request**. Requests can be either base 64 encoded PKCS #10 certificate requests or PKCS #7 renewal requests.
Certificate Template(enterprise CAs only)	Choose the certificate template from the selection list that is to be used by enterprise CAs to process the certificate request and issue the certificate.
Attributes	Enter additional attributes for the requested certificate in the **Attributes** box. For more information about certificate attributes and the syntax you must use, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .

After you have configured the options in the **Submit a Saved Request** page, click **Next**. For enterprise CAs, requests are submitted to the CA and approved immediately. For a stand-alone CA, certificate requests are held as "pending" until an administrator approves the certificate request. You must return to the **Welcome** page within 10 days and select the **Check on a pending certificate** option to determine whether a pending certificate request has been approved. When the certificate is issued, the **Issued Certificate** page appears so that you can install the certificate.

Smart Card Enrollment Station Page

To enable central and secure administration of your smart card program, the Web Enrollment Support pages include the **Smart Card Enrollment Station** page so that trusted administrators or security personnel can enroll for smart card certificates on the behalf of other users. Things to keep in mind for using this station include the following:

- Only administrators with Enrollment Agent certificates can use the Smart Card Enrollment Station page. Requests for smart card certificates must be signed with the administrator's Enrollment Agent certificate.
- By default, only members of the Domain Admins and Enterprise Admins security groups can request and obtain Enrollment Agent certificates.
- By default, only members of the Domain Admins and Enterprise Admins security groups can request and obtain Smart Card Logon and Smart Card User certificates.
- Issued certificates are stored on the user's smart card, which is inserted into the smart card reader at the smart card administrator's workstation.
- Certificates for logging on with a smart card must be mapped to the user's network account by an enterprise CA. Therefore, you cannot use stand-alone CAs to enroll users for certificates that are used for the smart card logon process. However, you can use stand-alone CAs to enroll users for client authentication and secure mail certificates, which are stored on smart cards.
- You can issue any type of certificate to a smart card to provide extra security for private keys or to enable users to easily transport certificates. However, not all applications or services support smart cards. For example, you can store a Basic EFS certificate on a smart card, but EFS does not support smart cards.

You can modify the Enroll permissions for the Enrollment Agent, Smart Card Logon, and Smart Card User certificate templates to allow other users and security groups to enroll for these certificates. For example, you can modify the ACLs for the smart card certificate templates to grant the Domain Users security group (all user accounts in the domain) Enroll permissions so that they can request or renew their own smart card certificates. However, this weakens the overall security provided by smart cards and is not recommended.

In addition, when someone has an Enrollment Agent certificate, they can enroll for a certificate and generate a smart card certificate on behalf of anyone in the organization. The resulting smart card might then be used to log on to the network and impersonate the real user. The unauthorized impersonator can have all the rights and permissions that are granted to the authorized user. For this reason, it is strongly recommended that your organization maintain strict security policies over who can be issued this certificate type.

For example, to minimize the risk of Enrollment Agent certificate misuse, you can configure one dedicated subordinate CA with restrictive administrative controls to issue Enrollment Agent certificates for your organization. After the initial Enrollment Agent certificates have been issued, the administrator of the CA can disable the issuance of Enrollment Agent certificates until they are needed again. By restricting which administrators can operate the CA service on the subordinate CA, the service can be kept online for the generation and distribution of CRLs, if necessary. Other CAs in the hierarchy can conceivably still issue Enrollment Agent certificates if their issuing policy settings are changed, but you can determine whether inappropriate Enrollment Agent certificates are issued by regularly checking the Issued Certificates log for each CA.

You also can change the ACLs on the Enrollment Agent, Smart Card Logon, and Smart Card User certificate templates to grant Enroll permissions to a small group of trusted administrators only. For example, you might allow only members of a smart card security officers security group to have Enroll permissions for the Enrollment Agent, Smart Card Logon, and Smart Card User certificate templates.

Tip In Windows 2000, only one certificate and one private key can be stored on a smart card. Windows 2000 Certificate Services includes the Smart Card User certificate template, which supports network logon authentication, client authentication for Web communications, and secure mail. To provide maximum functionality for smart cards, you can issue this certificate to smart card users rather than the Smart Card Logon certificate, which is valid only for network logon authentication.

You can use the **Smart Card Enrollment Station** page to enroll users for smart card certificates by using the options described in Table 16.26.

Table 16.26 Smart Card Enrollment Station Options

Option	Description
Identifying Information(stand-alone CAs only)	Type identification information that is to appear in the certificate, including Name,

	E-mail, Company, Department, City, State, and Country/region. Enterprise CAs obtain this information from Active Directory.
Intended Purpose(stand-alone CAs only)	From the selection list, choose the intended purpose of the certificate that is to be requested.
Certificate Template(enterprise CAs only)	From the selection list, choose the certificate template that is to be used by the enterprise CA to process the certificate request and issue the certificate. For example, choose either Smart Card Logon or Smart Card User.
Cryptographic Service Provider	Choose the smart card CSP that is appropriate for the user's smart card. For example, choose the Gemplus GemSAFE Card CSP for Gemplus smart cards or the Schlumberger Cryptographic Service Provider for Schlumberger smart cards.
Administrator Signing Certificate	From the selection list, click **Select Certificate** to choose your Enrollment Agent certificate. You cannot use an Enrollment Agent certificate that belongs to someone else.
User to Enroll	Click **Select User** to select a user account from Active Directory for which you are enrolling the smart card certificate.

After you have configured all of the options, insert the user's smart card in the smart card reader. Then click **Enroll** to request the smart card certificate. The PIN confirmation process and dialog boxes that appear differ depending on the specific smart card CSP that is used.

For the Schlumberger Cryptographic Service Provider, the **Smart Card PIN Confirmation** dialog box appears. For the Gemplus GemSAFE Card CSP, an untitled dialog box appears. Use the dialog box to confirm the PIN for the smart card. You also have the option of changing the PIN. Table 16.27 describes the options for the Schlumberger CSP dialog box. Table 16.28 describes the Gemplus CSP dialog box.

Table 16.27 Smart Card PIN Confirmation Dialog Box (Schlumberger CSP)

Option	Description
Please enter your PIN	Type the correct PIN for the smart card that is inserted in the smart card reader. Click **OK** to submit the PIN for confirmation by the CSP.
Change PIN after Confirmation	Select this check box to change the PIN. When you click **OK**, the CSP confirms the PIN you typed in the **Please enter your PIN** box, and then displays the **Change PIN on Smartcard** dialog box. Type the new PIN in the **New PIN** box; type it again in the **Confirm New PIN** box. Click **OK** to change the PIN.

Table 16.28 Untitled Dialog Box (Gemplus CSP)

Option	Description
Unlabeled box	Type the correct PIN for the smart card that is inserted in the smart card reader. Click **Change** to change the PIN, or click **OK** to submit the PIN for confirmation by the CSP.
Change	Changes the PIN. The CSP confirms the PIN you typed in the unlabeled box and displays the **Please Enter New PIN Code** dialog box. Type the new PIN in the top (unlabeled) box, and then type it again in the bottom (unlabeled) box. Click **OK** to change the PIN.

It is recommended that you assign a unique PIN for each smart card that is issued. Your policies for PINs can be much less restrictive than your policies for network passwords. In general, network passwords require long and complex composition, and it is recommended that users change them often. Users are more likely to write down their complex passwords because they are hard to remember. However, PINs can be changed infrequently and can be relatively short and easy to remember so that users are less likely to write them down. PINs are managed by the smart card CSP and can be changed only when smart card certificates are issued or renewed.

After the smart card PIN is confirmed or successfully changed, the smart card CSP generates the public key and private key set, and then stores the private key and the certificate on the user's smart card. When the smart card certificate is issued, the **Status** section of the **Smart Card Enrollment Station** page appears with a message that explains that the smart card is ready. Click **View Certificate** to display the certificate and verify that the user account information and the certificate type are correct. Click **New User** to submit another certificate request by using the Smart Card Enrollment Station page.

Installing the Certificate After It Is Issued

For enterprise CAs, the certificate is approved and issued after a short time unless the request is denied. For stand-alone CAs, certificate requests are held as "pending" until an administrator approves the request and the CA issues the certificate.

When certificates (except smart card certificates) are issued by CAs, the **Issued Certificate** page appears. Click **Install this certificate** to install the certificate in the Personal certificate store for the logged-on user. If you are requesting a certificate for a computer, you must select the **Use local machine store** option on the **Advanced Certificate Request Form** page to install the certificate in the Personal store for the computer rather than in the Personal store for the logged-on user.

For subordinate CA certificates, click **Install this certification path** to install the certification path file for the CA. You then can use the Certification Authority console to install the certification path file and certify the CA.

Requesting Certificates with the Certificate Request Wizard

You can request certificates for Windows 2000–based computers by using the Certificates console. When you right-click the Personal store for a user or for a computer and then click **All Tasks** and **Request New Certificate**, the Certificate Request wizard appears. You can use the Certificate Request wizard to request a certificate from an active enterprise CA. The Certificate Request wizard lists all certificate types that the user or computer is eligible to obtain. You can select a certificate type and submit it to any active CA that is configured to issue that type. If no CA is available to process certificate requests or the user or computer is not eligible for any certificate types, the Certificate Request wizard does not appear.

You have the option of selecting the **Advanced** check box on the first page of the Certificate Request wizard to choose advanced options. The advanced options enable you to select the CSP that is used with the certificate (as long as the CSP supports the cryptographic operations required for that certificate type). For user certificates only, users can also select strong private key protection as an advanced option. You also have the option of selecting the **Enable strong private key** check box, which means that the system prompts the user for permission before conducting cryptographic operations with the user's private key. Strong private key protection is available only for user certificates, not for computer certificates.

When you are choosing strong private key security, you can select either **Medium security** or **High security**. For **Medium security**, the system prompts the user for permission before using the private key, but it does not require a password. For **High security**, the user also must specify a password, which is used to protect the private key.

When you are requesting EFS user certificates, you can choose **Enable strong private key**; but EFS does not support a user interface, so users are never prompted for EFS user operations. However, strong private key protection works for recovery agent certificates. When you are requesting recovery agent certificates, consider choosing **Enable strong private key** and **High security** to provide an additional level of security for EFS recovery operations. Likewise, consider choosing **High security** to password protect the private keys for smart card enrollment agent certificates, code signing certificates, and trust list signing certificates, which might be misused to cause significant damage to your network resources.

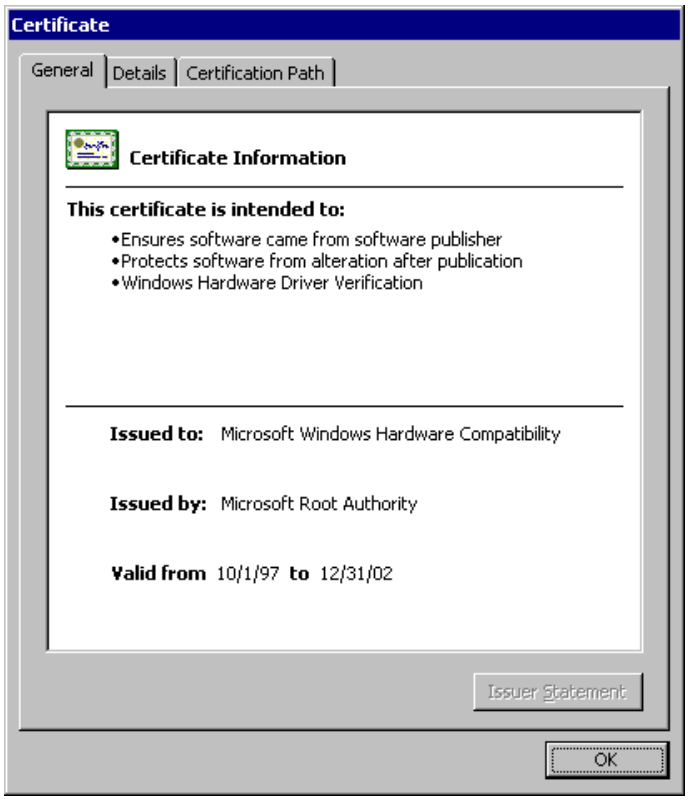
When the CA issues the requested certificate, you can choose to view the certificate or install the certificate in the Personal store for the selected user or computer. Users also can request certificates from CAs with the Web Enrollment Support pages.

Viewing Information About Certificates

When you double-click a certificate, or right-click the certificate, and then click **Open**, the **Certificate** dialog box appears, in which you can view the following:

- General information
- Details information
- Certification path information

Figure 16.14 is an example of the **General** dialog box.

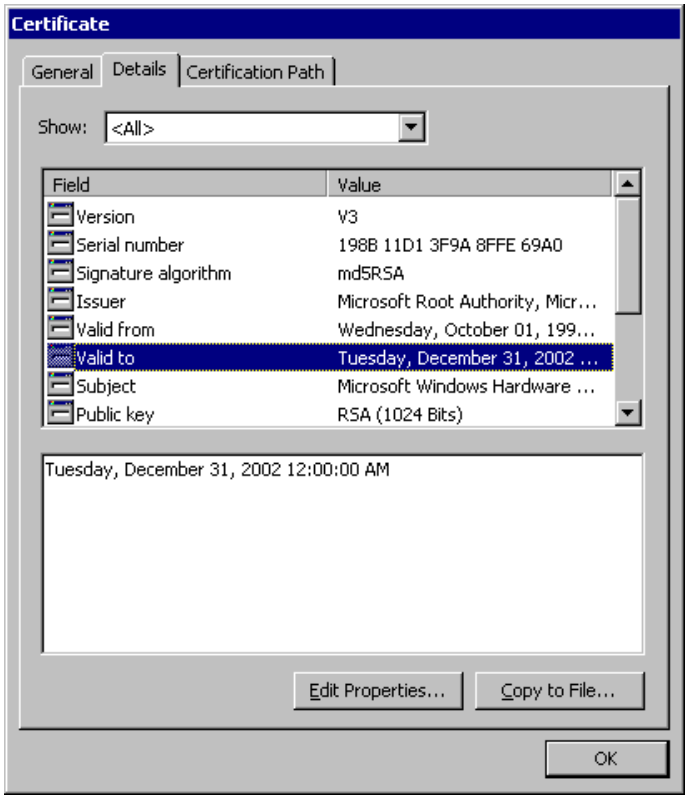


If your browser does not support inline frames, click here to view on a separate page.

Figure 16.14 Certificate General Dialog Box

The **Certificate General** dialog box lists general information about the certificate, including the intended purposes of the certificate, the issuing CA, and the validity dates. If there is a problem with the certificate, a warning message with additional information appears in the dialog box. **Issuer Statement** is grayed out because the issuing CA does not provide a statement. However, if the issuing CA provides a statement, you can click **Issuer Statement** to obtain additional information about the certificate from the issuing CAs Web site.

Figure 16.15 is an example of a **Certificate Details** dialog box.



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

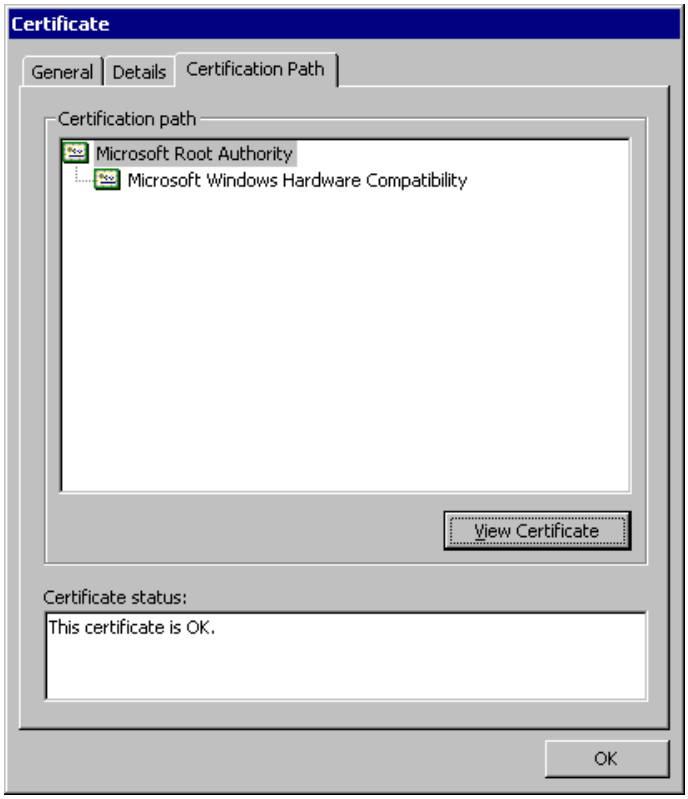
Figure 16.15 Certificate Details Dialog Box

The **Certificate Details** dialog box shows the information that is contained in the certificate, such as **Version**, **Valid to**, and **Friendly Name** (not shown). When you select an item in the **Field** column, the contents of the **Value** column for that item appear in the display box at the bottom of the dialog box. For example, in Figure 16.15, **Valid to** is selected and "Tuesday, December 31, 2002 12:00:00 AM" appears in the display box.

You can click **Edit Properties** to edit the **Friendly Name** and **Description** for the certificate, which appear in the Certificates console. You can also click **Edit Properties** to restrict the purposes for which the certificate can be used. By default, all of the purposes that are listed in the certificate are enabled. However, you can choose to disable all purposes (thus making the certificate invalid), or you can choose to trust the certificate for specific purposes only. For example, if a certificate is valid for code signing, secure mail, and secure Web communications, you can choose to trust it for secure mail only.

You can click **Copy to File** to export the certificate. If key export is enabled for the certificate, you also have the option of exporting the private key.

Figure 16.16 shows an example of a **Certification Path** dialog box.



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

Figure 16.16 Certificate Certification Path Dialog Box

The **Certificate Certification Path** dialog box provides a graphic representation of the certification path and lists the trust status of the certificate. The **Certificate status** box describes the status of the certificate. If there is a problem with the certificate or the path, a warning appears in the **Certificate Certification Path** dialog box with information that explains the problem. Common problems include the parent certificate not being in the Trusted Root Certification Authorities store or a certificate in the **Certification path** box that does not validate properly. You can select a certificate in the **Certification path** box and click **View Certificate** to view information about the selected certificate.

Exporting Certificates and Private Keys

When you right-click a certificate and then click **All Tasks** and **Import**, or when you click **Copy to File** in the **Certificate Details** dialog box, the Certificate Export wizard appears. You can use the Certificate Export wizard to export the selected certificate to a file and to optionally export the private key if enabled to do so. If the private key is exported, the key is stored in a password protected encrypted file format. You must specify a password that is then used to lock and unlock the exported key. You cannot access the exported private key again without the password.

Of course, because password protection provides relatively weak protection, someone who has access to an exported private key can launch a brute force or dictionary attack and decode the encryption scheme in a relatively short period of time. Therefore, to avoid the compromise of private keys, you must carefully control the export of private keys and provide adequate security for any medium that contains exported private keys.

Important Private keys that are used for digital signing must never be exported or stored in a file or an archive. Someone other than the legitimate key owner might be able to gain access to the duplicate and impersonate the owner. If a copy of a signing key exists, the authentication, integrity, or nonrepudiation provided by the key is compromised. Therefore, Windows 2000 does not permit the export of private keys that are used for signing.

For standard Windows 2000 Certificate Services certificates, private key export is enabled only for EFS user certificates and recovery agent certificates. Key export is enabled for EFS certificates, so that you can maintain a key recovery archive. The export of private keys is enabled by an attribute that is included in the certificate when it is created. When you use the Advanced Certificate Request Web pages, you have the option of enabling private key export for custom certificates that you issue for key exchange purposes only. You cannot use the Advanced Certificate Request Web pages to enable private key export for custom certificates that are used for the purpose of both key exchange and signatures.

You must enable the export of private keys only for keys that are used to store long-term (persistent) data, such as encrypted files on your hard disk. For example, if you issue secure mail certificates that have the purpose of confidential mail only (not signing mail), you might want to enable key export so that you can archive the keys securely for recovery purposes. If so, you also need to issue secure mail certificates that are used for signing mail only and that have private key export disabled.

Backing Up and Restoring Certification Authorities

It is recommended that CAs be backed up regularly so that the CA can be restored if there is a server disaster such as a hard disk failure. If a hard disk fails, you can lose data that has changed since the last back up, such as the following information:

- Changes to the configuration of Certificate Services
- Record of certificates issued
- Record of certificate requests
- Certificate request queue
- Record of certificates revoked

To minimize the effect of a server disaster, you can use Windows 2000 Backup to back up and restore the CA as part of your server backup and restore program. You also can back up and restore the Certificate Services configuration data, the private key, the certificate, and the certificate database for the CA by using the Certification Authority console.

Windows 2000 Backup and Restore

You can use Windows 2000 Backup to schedule and perform periodic backups for the server where the CA is installed. If the server fails (for example, as a result of a hard disk failure), you can use Windows 2000 Backup to restore the server and its services by using the most current backup set.

In Windows 2000 Backup, schedule and perform the following types of backups:

- Normal (full) backups. Backs up the entire server file system and the system state.
- Differential backups. Backs up all changes to the server file system and the system state since the last normal backup.
- Incremental backups. Backs up all changes to the server file system and the system state since the last back up.

Although you have the option of backing up the file system without the system state, back up files with the system state to ensure full recovery of the server. Because Certificate Services depends on the Web Enrollment Support pages, you must also make sure to backup Internet Information Services at the same time.

Windows 2000 Backup supports a wide range of storage devices, such as hard disks, tape drives, removable disks, recordable CDs, or an entire library of disks or tapes organized into a media pool and controlled by a robotic changer. For more information about how to use Windows 2000 Backup, see Windows 2000 Server Help.

Certification Authority Console Backup and Restore

You can use the Certification Authority Backup wizard and the Certification Authority Restore wizard (available from the Certification Authority console) to back up and restore the following types of CA data:

- Private key and certificate
- Certificate database

You can back up all data or only selected data for the CA. For example, you can backup only the private key and certificate, or you can back up only the certificate database. You also can choose to perform a normal (full) backup or an incremental back up. You can back up CA data to an empty folder on any NTFS, FAT, or FAT32 storage device that is supported by Windows 2000.

If a server disaster occurs, you can restore the CA from the most current backup set. You must first restore the last normal backup, and then restore each incremental backup in the order in which they were backed up.

When you back up the CA's private key, you must provide a password. The private key is stored in a password-protected, encrypted format for protection and confidentiality of the key. You must supply the original password before you are permitted to restore the private key. For more information about how to use the Certification Authority console to backup and restore CAs, see Certificate Services Help.

Backup Strategies

It is recommended that you schedule and perform frequent backups to ensure that the CA can be restored with the minimum disruption to Certificate Services. Typical backup strategies usually include the following combinations of periodic normal (full), differential, and incremental backups.

Daily Normal Backups Normal backups are the most complete and easiest to restore. However, normal backups take the most time, consume the most storage space, and place the greatest load on servers and the network.

Weekly Normal and Daily Differential Backups Daily differential backups take less time, consume less storage space, and place less load on servers and the network than daily normal backups do. However, restoring the data takes longer because you must restore the last normal backup and then the last differential backup.

Weekly Normal and Daily Incremental Backups Daily incremental backups take less time, consume less storage space, and place less load on servers and the network than daily differential backups do. However, restoring the data takes longer because you must restore the last normal backup and each incremental backup in order since the last normal backup.

In addition, you can alternate normal backups with differential or incremental backups at any interval that meets your needs. For example, you might want to perform normal backups every three days and perform daily differential backups in between the normal backups.

Choose backup strategies that meet the backup storage capacity and load restrictions of your networks. Back up Certificate Services at least daily so that no more than one day's worth of certificate transactions is lost if the hard disk that contains the certificate database fails.

In addition to routine backups, you can use the Certification Authority Backup wizard to create an archive that contains the CA's private key, certificate, and configuration data. The archive is then updated only when the CA's data changes. The archive can be used to restore CAs to service even if something happens to the routine backup sets.

Restore Considerations

When the restore of a CA is complete, it is important that you make a new full backup of the certificate server database. This is necessary to truncate the restored log files and to establish a base backup set for future restores. Backups that are performed after a restore cannot be mixed with backups (either full or incremental) that are taken before the restore — that is, after a Certificate Services database is restored and has progressed to a subsequent state, you cannot use the prerestoration backups to restore the database to that subsequent state.

When you are restoring a failed CA with Windows 2000 Backup, you must restore Internet Information Services as well as Certificate Services, or else Internet Information Services fails to start when the system is restarted. Certificate Services requires that the Internet Information Services be running to support the Web Enrollment Support pages.

When you are restoring Certificate Services, if the database logs are not manually deleted, Certificate Services is brought up-to-date. If the logs are manually deleted, Certificate Services is restored to the point in time that the backup was performed. By default, the certificate database and the request log are installed at the following location:

`<Drive:>WINNT\System32\CertLog`

where <*Drive:*> is the letter of the drive where the CA is installed.

Revoking Certificates

The Windows 2000 Certificate Services certificate database records information for each certificate the CA issues. You can use the Certification Authority console to revoke issued certificates. For example, you might revoke the certificates issued for employees who are terminated or who have transferred to another unit. You also might revoke certificates when you suspect or discover that private keys have been compromised or misused. Until they expire, revoked certificates are published in the certificate revocation list.

When a certificate has been revoked, it is invalid and cannot be made valid again. If you revoke a certificate by mistake, you can re-issue a new valid certificate to take the place of the revoked certificate.

To use the Certification Authority console to revoke a certificate, select the Issued Certificates container for the CA and click the certificate in the details pane of the console. Then click **Action**, **All Tasks**, and **Revoke Certificate**. When the **Certificate Revocation** dialog box appears, select a reason code from the list in the **Select a reason code** box, and then click **Yes** to revoke the certificate. Reason codes include: Unspecified, Key Compromise, CA Compromise, Change of Affiliation, Superceded, Cease of Operation, and Certificate Hold. Revoked certificates are moved to the Revoked Certificates container of the CA.

Publishing Certificate Revocation Lists

Windows 2000 Certificate Services publishes periodic certificate revocation lists (CRLs). However, you can also use the Certification Authority console to manually publish a new CRL at any time. For example, you might want to publish a new CRL immediately after revoking certificates.

To publish CRLs manually, right-click the Revoked Certificates container for the CA. Then click **All Tasks** and **Publish**. When the **Certificate Revocation List** dialog box appears, click **Yes** to replace the old CRL.

Approving or Denying Certificate Requests

Windows 2000 Certificate Services stores pending requests in the Pending Request queue. For enterprise CAs, requests are processed automatically and the request is either approved or denied. By default, for stand-alone CAs, certificate requests are stored in the Pending Request queue for review by a CA administrator. You can use the Certification Authority console to review pending requests and either approve or deny the request. Approved requests are issued by the CA.

To use the Certification Authority console to approve a certificate request

1. Click the **Pending Requests** container for the appropriate CA.

   The pending certificate requests appear in the details pane of the console.
2. Right-click the appropriate certificate request, and then click **All Tasks** and **Issue.**

   The CA issues the certificate.

To use the Certification Authority console to deny a certificate request

1. Click the **Pending Requests** container for the appropriate CA.

   The pending certificate requests appear in the details pane of the console.
2. Right-click the appropriate certificate request, and then click **All Tasks** and **Deny.**

   The **Deny Certificate Requests** dialog box appears.
3. Click **Yes** to deny the certificate request.

   The certificate request is moved to the Failed Requests container.

Renewing Certification Authorities

If a CA's certificate expires, the CA can no longer provide certificate services. Before the CA certificate expires, you can use the Certification Authority console to renew the CA to provide uninterrupted certificate services. The interval that is required for CA renewal depends on the certificate life cycle that you designed for the public key infrastructure.

After you renew a CA, the CA continues to issue certificates by using the new CA certificate, and the cycle starts over. The prerenewal CA certificate remains trusted, so nonexpired certificates that were issued by the prerenewal CA continue to be trusted until they expire or are revoked.

You have the option of renewing the CA certificate by using the existing key set of the prerenewal CA certificate. However, the longer a key set is in use, the greater the risk the key set might be compromised. The risks of longer key lifetimes involves many complex factors, including key length and protection from attacks. For more information about risk factors for cryptographic keys, see "Cryptography for Network and Information Security" in this book.

To use the Certification Authority console to renew a CA certificate

1. Select the CA node, and then click **Action**. Then click **All Tasks** and **Stop Service** to stop the CA. If you skip this step, you are later prompted to stop the CA.
2. Click **Action**, and then click **All Tasks** and **Renew CA Certificate**.

   The **Renew CA Certificate** dialog box appears.
3. Click **Yes** to generate a new key set, or click **No** to reuse the old key set. Then click **OK**.

   For root CAs, the certificate is renewed and no further action is required. For subordinate CAs, the **Complete this CA Installation** dialog box appears.
4. Type the domain name of the server for the parent CA in the **Computer Name** box, or click **Browse** to select the server.

   The **Parent CA** box displays the name of the CA that is running on the server computer that you have selected.
5. Click **OK**.

   The renewal request is sent to the parent CA to process. When the parent CA issues the new certificate, the CA certificate of the child CA is renewed.

Root CA certificates are renewed with the same lifetime as the original certificate. Subordinate CA certificates are renewed with the lifetime that is determined by the parent CA.

Recovering Encrypted Data

Windows 2000 supports the encryption of persistent data by EFS and secure mail systems. Encrypted data is usually readable only to the user who possesses the required private key to unlock the data. However, if the user's private key is lost or damaged, the encrypted data becomes unusable unless there is a means to restore the plaintext or the private key to the user. Furthermore, if a user who has encrypted information leaves the organization or is terminated, organizations can lose access to valuable encrypted information unless there is a means for someone else besides the user to recover the encrypted information.

When you deploy EFS or secure mail, implement a recovery program and policies to ensure that users' encrypted data can be recovered. EFS provides for recovery agents (trusted administrators) who can recover encrypted files. Many secure mail systems, such

as Microsoft® Exchange Server, provide a key recovery database so that trusted administrators can restore users' private keys when necessary for users to read their encrypted mail (for example, when a user's private key is corrupted).

Recovery for Encrypting File System

EFS provides for data recovery agents. By default the domain Administrator user account (the local Administrator account for the first domain controller installed in the domain) is issued an EFS recovery certificate. You can use this account to recover files encrypted by EFS users in the domain. The private key for EFS recovery is stored on the local computer where the EFS recovery account is located. You must perform EFS recovery operations on the computer where the private key that is used for recovery resides.

You can configure Encrypted Data Recovery Agents policy to designate alternative recovery agents. For example, to distribute the administrative workload in your organization, you can designate alternative EFS recovery accounts for categories of computers grouped by organizational units. You can use Encrypted Data Recovery Agent policy to designate recovery accounts on computers to be used for EFS recovery operations.

You must deploy a CA to issue EFS Recovery Agent certificates to the EFS recovery accounts you want to designate by means of Encrypted Data Recovery Agents policy. You can issue certificates for EFS recovery with an enterprise CA or a stand-alone CA.

For enterprise CAs, by default, members of the Domain Admins and Enterprise Admins security groups are granted permissions to enroll for EFS Recovery Agent certificates. To change the default certificate enrollment settings, modify the ACLs for the EFS Recovery Agent certificate template. You can request an EFS Recovery Agent certificate by using the Certificate Request wizard or by using the Advanced Certificate Request page for an enterprise CA.

For stand-alone CAs, you can use the Advanced Certificate Requests form to request a recovery agent certificate by entering **1.3.6.1.4.1.311.10.3.4.1** as the object identifier in the **Usage OID** box.

The **cipher** command-line program is used to recover EFS files. The recovery operation decrypts the encrypted file to plaintext, which is readable by others. Therefore, administrators must take precautions when they are transferring the plaintext back to the user to ensure that the confidentiality of the information is preserved. For more information about **cipher,** see Windows 2000 Server Help.

For EFS encrypted files, the recovery agent information is refreshed every time the file system performs an operation on the file (for example, when the file is opened, moved, or copied). However, if an encrypted file is dormant for a long time, the recovery agents can expire. To ensure that dormant encrypted files can be recovered, maintain archives of the recovery agent certificates and private keys. To create an archive, export the certificate and its private key to a secure medium and store it in a safe location. When you export private keys, you must provide a secret password for authorizing access to the exported key. The secret key is stored in an encrypted format to protect its confidentiality.

To recover dormant files with expired recovery agent information, import the appropriate expired recovery agent certificate and private key from the archive to a recovery account on a local computer and then perform the recovery. To view recovery agent information for an encrypted file, use the **efsinfo** tool. For more information about **efsinfo,** see Windows 2000 Tools Help.

For more information about EFS and EFS recovery, see "Encrypting File System" in this book.

Recovery for Secure Mail

The Windows 2000 public key infrastructure does not provide a key recovery system for secure mail. However, to provide key recovery services, you can deploy secure mail systems, such as Exchange Server.

Exchange Server maintains users' private keys in a central protected store. Security administrators can use the Key Management server (KM server) to recover keys and restore the keys to users as necessary. For more information about KM Server, see Exchange Server Help and the *Microsoft® BackOffice® Resource Kit.*

Anyone who can obtain a user's private key can impersonate that user in e-mail transactions or read confidential mail that is intended for that user. Therefore, it is recommended that administrators take precautions when transferring keys back to users to ensure that the confidentiality of the keys is preserved.

Using the Certificate Services Command-Line Programs

Windows 2000 Server provides the following three command-line programs for Certificate Services:

- CertUtil.exe
- CertReq.exe
- CertSvr.exe

These command-line programs provide extended functionality and control of certificate services. The use of the command line is primarily intended for developers and knowledgeable certification authority administrators.

For more information about the command-line programs, see Certificate Services Help.

CertUtil.exe

You can use CertUtil.exe to perform the following tasks:

- Dump certificate services configuration information, certificate requests, certificates, or certificate revocation lists to files.
- Get the certification authority (CA) configuration string.
- Retrieve the CA signing certificate.
- Revoke certificates.
- Publish or retrieve a certificate revocation list.
- Determine if a certificate is valid or if the encoding length is incompatible with old enrollment controls.
- Verify one or all levels of a certificate chain.
- Resubmit or deny pending requests.
- Set attributes or an integer or string value extension for a pending request.
- Verify a public/private key set.
- Decode files that are based on hexadecimal or base 64.
- Encode files to base 64.
- Shut down the Certificate Services server.
- Display the database schema.
- Convert a Certificate Server version 1.0 database to a Windows 2000 Certificate Services version 2.0 database.
- Back up and restore the CA keys and database.
- Display certificates in a certificate store.

- Display error message text for a specified error code.
- Import issued certificates that are missing from the database.
- Set and display certification authority registry settings.
- Create or remove Certificate Services Web virtual roots and file shares.

CertReq.exe

You can use CertReq.exe to request certificates from a certification authority. CertReq submits certificate requests by using PKCS 10 certificate request files and PKCS 7 certificate renewal files. You also can use the advanced options on the Web Enrollment Support pages to submit certificate requests by using PKCS 10 and PKCS 7 files.

CertSrv.exe

CertSrv.exe is the server engine program that is run when the Certification Authority service starts. For troubleshooting purposes only, you can run CertSrv as a stand-alone application in a command prompt window. When CertSrv is running in the diagnostics mode, it displays a log of its actions in the console window. You can start CertSrv as a service through **Services** in Control Panel.

Disaster Recovery Practices

Disasters, such as hard disk failure or a compromised CA certificate, can disrupt certificate services. You can take various steps to minimize the impact of such disasters and to ensure timely recovery from server or network disasters. The following practices can reduce the risk of failed or compromised CAs:

- Using preventive practices for servers.
- Providing security for certification authority servers.
- Protecting private keys for certification authority servers.
- Developing recovery plans.

Using Preventive Practices for Servers

The server where a CA is installed can fail, resulting in a disruption of certificate services. You can use the following preventive practices to reduce the risk of CA failures and to minimize the disruption of CA services:

- Provide duplicate CA services so that if one server is offline, another server can still issue the appropriate certificates.
- Back up CAs frequently so that they can be restored with a minimal loss of data.
- Install certificate services on hard disks by using disk arrays and redundant array of independent disks (RAID) Level 5 protection.
- Prepare recovery plans and train administrative staff on recovery plans.
- Maintain records of all server and CA configuration information so that exact configurations can be easily restored.
- Maintain replacement servers in standby or in ready stores for immediate recovery.

Providing Security for Certification Authority Servers

Computers that run CA services can be priority targets for attack by intruders who maliciously want to disrupt network services or compromise the security of network and information systems. If intruders can gain unauthorized access to a CA server or exploit weaknesses in the security of the server, they can gain access to valuable network resources and compromise the security of the affected portion of the certification trust chain. Therefore, you should provide higher security for CA servers than for regular servers.

The risk of attacks on your CAs depends on many factors, including how secure your networks are, the value to be gained by a successful attack, and the costs of attempting the attack. If the CA is inside your firewall and used on the intranet for routine business purposes, the risk of attack might be low. However, if the CA is outside your firewall and used for an extranet, the risk of attack might be high.

If a CA is compromised, there can be considerable damage and cost to your organization. The damages and costs of a compromised CA include the following:

- Stolen proprietary information.
- Efforts spent investigating and stopping the intruder's attacks on the network.
- Failed or disrupted network services.
- Destroyed or corrupted network resources.
- Efforts to recover from the CA compromise and redeploy new CAs and certificates.

A compromised root CA is far more costly than a compromised intermediate CA or issuing CA. You can deploy multiple CA hierarchies to reduce the impact of a single compromised CA on your organization.

To determine what security measures are appropriate for CAs, weigh the estimated cost of providing security measures against the estimated cost of compromised CAs. Security measures for CA servers can include the following:

- Maintaining servers in secure data centers and controlling physical access to trusted administrators.
- Using hardware CA devices or hardware-based CSPs to provide maximum security for the CAs' private keys.
- Configuring server security settings for high security levels, such as those security levels provided by the High Security template.
- Using the Windows 2000 system key (SysKey) to provide additional encryption protection of CA servers' protected stores.
- Performing security auditing to monitor for potential attacks on CA servers.
- Restricting user rights assignments to limit user rights to the appropriate administrator group. (No other users or groups have rights or permissions to view or perform any tasks on the local CA computer.)
- Disabling unnecessary services so they cannot run on CA servers; running unnecessary services provides a mechanism that intruders can exploit.
- Implementing security policies and procedures to control the deployment of CAs in the enterprise.

Choosing security measures for a CA involves weighing the costs of implementing and maintaining those security measures against the risks of potential attack on the CA and the potential costs of a CA compromise. Higher risks of attacks on the CA and higher costs of a CA compromise generally justify higher costs for security measures to protect the CA. Provide the most protection for root CAs, and provide more protection for intermediate CAs than for issuing CAs.

For example, your organization decides to protect a large amount of highly valuable and confidential information by using public key security solutions. You also decide to acquire expensive hardware CA devices for root CAs and store the root CAs in maximum security vaults that are located at your headquarters for safekeeping. You authorize access to the root CAs for trusted administrators so that

they can certify intermediate CAs for each of your business units. The intermediate CAs are offline Windows 2000 CAs, which are disconnected from the network and maintained in locked data centers by the administrator for each business unit. The intermediate CAs are used to certify issuing Windows 2000 CAs as necessary to meet the certificate needs of each business unit. Issuing CAs are Windows 2000 enterprise CAs or stand-alone CAs that are maintained in secure data centers by each business unit. Your organization's security policy includes strict procedures and controls for requesting, authorizing, and implementing root CAs, intermediate CAs, and issuing CAs in the enterprise.

However, if your organization uses public key security solutions to protect information with relatively low value, you might decide to deploy offline Windows 2000 root CAs that are locked in data centers, rather than expensive hardware-based CAs locked in vaults. You might allow business units to maintain intermediate CAs and issuing CAs outside data centers. You also might place fewer restrictions on requesting, authorizing, and implementing CAs.

You can deploy Windows 2000 Certificate Services by using the Microsoft Base CSPs to provide CA security that meets a wide range of needs. However, when you need to provide the highest security for CAs, consider using hardware-based CAs. For more information about hardware-based cryptography solutions that work with Windows 2000 Server and Certificate Services, contact the appropriate hardware vendors.

Protecting Private Keys for Certification Authority Servers

If intruders can access a CA computer either physically or through the network, they might decode the private key and then impersonate the CA to gain access to valuable network resources. Intruders who impersonate a CA can cause widespread damage by stealing information, disrupting network services, or destroying network resources. A compromised CA key undermines and invalidates all security protection provided by that CA and any CA hierarchy deployed below it. To reduce the risks of intruder attacks on CA keys, consider using the following practices.

Provide Security for Certification Authority Servers Provide security for CA servers as discussed earlier in this chapter. Providing physical security minimizes the risk that intruders can gain access to the CA server or the protected store (whether hardware-based or software-based) where the CA key resides. Providing network and server (software) security minimizes the risk that intruders can gain access to the CA server or exploit applications and services that are running on the server to compromise the CA key.

Provide Enhanced Security for Certification Authority Keys Use hardware-based CSPs when you want to provide maximum security for private keys because keys are stored on tamper-resistant hardware devices and keys are never exposed to the operating system. Use SysKey to provide extra protection for CAs' private keys that are stored by Microsoft CSPs.

Use Large Keys for Certification Authorities Large CA keys reduce the risks of key attacks, but large keys also require more storage space as well as more computer processing power to sign certificates. Consider using the largest key lengths that are feasible depending on key storage requirements and CA performance requirements.

For example, a 4,096-bit CA key generally provides a great deal of key protection, but signing certificates with such a long key takes a long time, even if you are using crypto-accelerator boards. A 4,096-bit CA key might perform acceptably for root CAs or intermediate CAs that are used infrequently only to certify subordinate CAs. Although, some CAs with hardware-based CSPs might not support the storage of a 4,096-bit key.

However, a 4,096-bit CA key would likely cause unacceptably slow performance for most issuing CAs. For issuing CAs, use key lengths that are as long as feasible and that enable adequate CA performance to support your long-term certificate services goals. You can often use crypto-accelerator boards to improve performance and enable longer keys for issuing CAs. Test the performance CAs in labs and in pilot programs by using the proposed CA key lengths before you deploy CAs in the production environment.

Use Appropriate Lifetimes for CA Keys The longer CA keys are valid, the greater the risk of key compromise because attackers have more time to attempt cracking the key. There is no simple formula to determine maximum key lifetimes. However, the adequacy of longer key lifetimes depends largely on how well protected the key is and how long the key is. In general, longer keys can have longer key lifetimes. Likewise, keys with more secure storage can have longer lifetimes. For example, keys stored in tamper-resistant hardware crypto-devices are safer than keys stored on local computer hard disks. Therefore, for the same-sized keys, keys stored in hardware crypto-devices usually can have longer safe key lifetimes than keys stored by software CSPs on hard disks.

For more information about the major risk factors for cryptographic keys, see "Cryptography for Network and Information Security" in this book.

Developing Recovery Plans

You can develop recovery plans to help restore CAs if certificate services fail or CAs are compromised. It is recommended that you test recovery plans to ensure that they work as intended. Hold training sessions for your staff to ensure that they know how to use the recovery plans.

Recovery plans can include the following:

- Recovery procedures and checklists for administrators to follow
- Recovery toolkits or pointers to the toolkits
- Contingency plans

Failed Certification Authority

A CA can fail for a variety of reasons, such as a server hard disk crash, a failed network card, or a server motherboard failure. Some failures can be corrected quickly by locating and correcting the problem within the CA server. For example, you can replace a failed network card or a failed motherboard and restart the computer to restore certificate services.

If a hard disk has failed, you can replace the hard disk and restore the server and the CA from the most recent backup set. If the CA is damaged or corrupted, you can restore the CA from the server's most recent backup set. If you must replace the server, configure the new server with the same network name and IP address as the failed CA server. Then install the CA with the original configuration information and the original private key and certificate for the CA.

Select the Windows Component wizard **Advanced options** when you are installing the CA to enable you to reuse the key and the associated certificate. In the **Public and Private Key Selection** page, you must click **Use existing keys**, select the key from the list, and then click **Use the associated certificate**. You can also click **Import** to import a private key from archives. The CA information that is contained in the certificate is automatically used for the **CA Identifying Information** page. The CA is installed as the original CA.

If **Use the associated certificate** is grayed out, you cannot use the subject information contained in the certificate. If so, you must configure the **CA Identifying Information** page exactly as the original, or else the process cannot work. Furthermore, on the **CA Certificate Request** page, you must click **Save the request to a file** instead of requesting a certificate from an online CA (otherwise, the parent CA issues a new certificate for the CA). After the CA is installed, you can use the Certification Authority console to install the original certificate to certify the CA.

You must click **Preserve existing certificate database** on the **Data Storage Location** page to preserve an existing CA database. Otherwise, you might overwrite the existing database and destroy the information that is contained in the database.

It is important to keep in mind that only the associated certificate works with the private key because the certificate contains the

complementary public key. It is also important to remember that the identifying information for the CA must match the Subject information in the certificate Subject field *verbatim* or else the CA does not work. The following information that is entered on the **CA Identifying Information** page during installation of the CA is used for the certificate Subject field:

- CA name
- Organization
- Organizational unit
- Locality
- State or province
- Country/region
- E-mail

The information in the Subject field is case sensitive, so review the information on the **CA Identifying Information** page carefully before you complete the installation process. You can view a certificate's Subject information with the **Certificate Details** dialog box by selecting **Subject**.

After a replacement CA is installed and running, you can use Windows 2000 Backup or the Certification Authorities Restore wizard to restore the CA configuration data from the most recent backup set.

Compromised Certification Authority

When a CA is found to be compromised, the only solution is to revoke the CA's certificate. Revoking a CA's certificate invalidates the CA and its subordinate CAs, as well as invalidating all certificates issued by the CA and its subordinate CAs. If you discover a compromised CA, it is recommended that you perform the following activities as soon as possible:

- Revoke the compromised CA's certificate.
- Publish a new CRL containing the revoked CA certificate.
- Remove compromised CA certificates from Trusted Root Certification Authorities stores and CTLs.
- Notify all affected users and administrators of the compromise and inform them that certificates issued by the affected CAs are being revoked.
- Repair security holes that led to the compromise.

To restore the CA hierarchy, you must redeploy new CAs to replace the compromised hierarchy. You must then reissue the appropriate certificates to users, computers, and services.

Additional Resources

- For more information about how to develop custom applications by using Windows 2000 Certificate Services and how to use the services of Microsoft CryptoAPI and CSPs, see the Microsoft Platform SDK link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For more information about Internet Engineering Task Force (IETF) drafts and recommendations, see the Internet Engineering Task Force (IETF) link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For more information about Public Key Cryptography Standards (PKCS), see the RSA Data Security link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For more information about the FIPS 140-1 standard, see the National Institute of Standards and Technology (NIST) link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources . Search for "Security Requirements for Cryptographic Modules."
- For more information about FIPS 140-1 as a de facto international standard for cryptographic modules, see the International Organization for Standardization link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources . Search for "International Standard 15408: Evaluation Criteria for Information Technology Security."
- For more information about the "Certified for Microsoft Windows" program and a list of currently compatible smart card products, see the Microsoft Windows Hardware Compatibility List link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
- For more information about the security technologies in Microsoft products, including cryptography export restrictions and licensing requirements, see the Microsoft Security Advisor link on the Web Resources page at http://windows.microsoft.com/windows2000/reskit/webresources .
