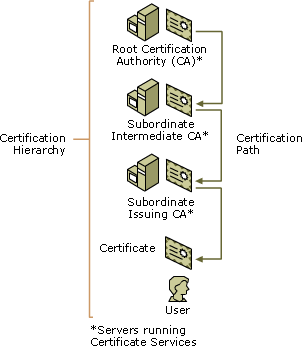
**Certificates and certification authorities**

When a certificate is presented to an entity as a means of identifying the certificate holder (the *subject* of the certificate), it is useful only if the entity receiving the certificate trusts the issuer, which is often referred to as the certification authority (CA).

When you *trust* a certification authority, that means you have confidence that the certification authority has the proper policies in place when evaluating certificate requests and will deny certificates to any entity that does not meet those policies. In addition, you trust that the certification authority will revoke certificates that should no longer be considered valid by publishing an up-to-date certificate revocation list. Certificate revocation lists are considered valid until they expire. So even if the CA publishes a new certificate revocation list with newly revoked certificates listed, all clients that have an old certificate revocation list will not look for, nor retrieve the new one until the old one expires or is deleted. Clients can use the CA Web pages to manually retrieve the most current certificate revocation list if necessary.

For Windows Server 2003 users, computers, and services, trust in a certification authority is established when you have a copy of the root certificate in the trusted root certification authorities store, as well as having a valid certification path, meaning that none of the certificates in the certification path has been revoked or has had its validity period expire. The certification path includes every certificate issued to each CA in the certification hierarchy from a subordinate CA to the root CA. For example, for a root CA, the certification path is one certificate, its own self-signed certificate. For a subordinate CA, just below the root CA in the hierarchy, its certification path is two certificates: its own certificate and the root CA certificate.



If your organization is using Active Directory, then trust in your organization's certification authorities will typically be established automatically, based on decisions and settings made by the system administrator.

A related concept with which you should be familiar is certificate store inheritance. If you place a root CA certificate into the computer's trusted root certification authorities store or enterprise trust store, then any user of the computer will see that certificate in their own user trusted root certification authorities store or enterprise trust store even though the root certificate is actually in the computer's store. Essentially, users will trust any CA that their computer trusts. Certificate store inheritance does not work the other way around: certificates in the user's trusted root certification authorities store and enterprise trust store are not inherited by the computer.

If your organization is using the version of Certificate Services installed with the Windows Server 2003 family to run its certification authority, the certification authority is one of two types: enterprise or stand-alone. The differences between the two standard types of Windows Server 2003 certification authorities for certificate users and requesters are summarized below.

**Enterprise certification authority**

An enterprise certification authority depends upon Active Directory being present.

You can use the Certificate Request Wizard (which is started from within the Certificates snap-in), as well as certification authority Web pages, to request certificates from an enterprise certification authority.

An enterprise certification authority offers different types of certificates to a requester based on the certificates it is configured to issue as well as the security permissions of the requester. An enterprise certification authority uses information available in Active Directory to help verify the requester's identity. An enterprise certification authority publishes its certificate revocation list to Active Directory as well as to a shared directory.

**Stand-alone certification authority**

A stand-alone certification authority is less automated for a user than an enterprise certification authority because it does not depend on the use of Active Directory.

By default, users can request certificates from a stand-alone certification authority only by using Web pages.

Stand-alone certification authorities that do not use Active Directory will generally have to request that the certificate requester provide more complete identifying information. A stand-alone certification authority makes its certificate revocation list available from a shared folder, or from Active Directory, if it is available.

**Generating encryption keys and certificate requests**

How you request and receive a certificate depends upon the policies and processes of the certification authority (CA) that issues the certificate. For example, some certification authorities have Web pages to which you can submit a reques or, if you are in an organization that has deployed Active Directory and Certificate Services, you can use the Certificates snap-in to request a certificate, if your computer is a member of a domain and you are authorized to request certificates.

In any case, when you generate a request for a new certificate, the information in that request is first passed from the requesting program to CryptoAPI. CryptoAPI will pass the proper data to a program known as a cryptographic service provider (CSP) that is installed on your computer or on a device that is accessible to your computer. If the CSP is software-based, it will generate a public key and a private key, often referred to as a key pair, on your computer. If the CSP is hardware-based, such as a smart card CSP, it will instruct a piece of hardware to generate the key pair.

After the keys are generated, a software CSP encrypts and then secures the private key. A smart card CSP stores the private key on a smart card and the smart card controls access to the key. The public key is sent to the certification authority, along with the certificate requester information. Once the CA verifies the certificate request according to its policies, it will use its own private key to create a digital signature in the certificate and then issue it to the requester. The certificate requester will then be presented with the certificate from the CA and the option to install it in the appropriate certificate store on the computer or hardware device.

## Certificate stores

Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition, store a certificate locally on the computer or device that requested it or, in the case of a user, on the computer or device that the user used to request it. The storage location is called the certificate store. A certificate store will often have numerous certificates, possibly issued from a number of a different certification authorities.

Using the Certificates snap-in, you can display the certificate store for a user, a computer, or a service according to the purpose for which the certificates were issued or by using their logical storage categories. When you display certificates according to their storage categories, you can also choose to display the physical stores, showing the certificate storage hierarchy. (This is recommended for advanced users only.)

If you have the user rights to do so, you can import or export certificates from any of the folders in the certificate store. Additionally, if the private key associated with a certificate is marked as available for export, you can export both into a PKCS #12 file.

Windows can also publish certificates to Active Directory. Publishing a certificate in Active Directory enables all users or computers with adequate permissions to retrieve the certificate as needed.

Certificates can be displayed by purpose or by logical stores, as shown in the following table. Displaying certificates by logical stores is the Certificates default. (Note that the list of certificate purpose stores does not include all the possible purpose stores.)

### 

|  |  |  |
| --- | --- | --- |
| **Display by** | **Folder name** | **Contents** |
| Logical Store | Personal | Certificates associated with private keys to which you have access. These are the certificates that have been issued to you, or to the computer or service for which you are managing certificates.  Note to administrators: Computers in a Windows Server 2003 Active Directory domain can have certificates automatically placed in this store through the use of Group Policy-based autoenrollment. For more information, see [Automatic certificate request settings](http://technet.microsoft.com/en-us/library/cc776310(WS.10).aspx). |
|  | Trusted Root Certification Authorities | Implicitly trusted certification authorities. Includes all of the certificates in the Third-Party Root Certification Authorities store plus root certificates from your organization and Microsoft.  If you are an administrator and want to add third-party certification authority certificates to this store for all computers in a Windows Server 2003 Active Directory domain, you can use Group Policy to distribute trusted root certificates to your organization. For more information, see [Trusted root certification authority policy](http://technet.microsoft.com/en-us/library/cc737408(WS.10).aspx). |
|  | Enterprise Trust | A container for certificate trust lists. A certificate trust list provides a mechanism for trusting self-signed root certificates from other organizations and limiting the purposes for which these certificates are trusted. For more information about Enterprise trust see [Enterprise trust policy](http://technet.microsoft.com/en-us/library/cc737306(WS.10).aspx). |
|  | Intermediate Certification Authorities | Certificates issued to subordinate certification authorities. |
|  | Trusted People | Certificates issued to people or end entities that are explicitly trusted. Most often these are self-signed certificates or certificates explicitly trusted in an application such as Microsoft Outlook. |
|  | Other People | Certificates issued to people or end entities that are implicitly trusted. These certificates must be part of a trusted certification hierarchy. Most often these are cached certificates for services like Encrypting File System, where certificates are used for creating authorization for decrypting an encrypted file. |
|  | Trusted Publishers | Certificates from certification authorities that are trusted by Software Restriction policies. |
|  | Disallowed Certificates | These are certificates that you have explicitly decided not to trust using either Software Restriction policy or by clicking "Do not trust this certificate" when the decision is presented to you in mail or a Web browser. |
|  | Third-Party Root Certification Authorities | Trusted root certificates from certification authorities other than Microsoft and your organization. |
|  | Certificate Enrollment Requests | Pending or rejected certificate requests. |
|  | Active Directory User Object | Certificates associated with your user object and published in Active Directory. |
| Purpose | Server Authentication | Certificates that server programs use to authenticate themselves to clients. |
|  | Client Authentication | Certificates that client programs use to authenticate themselves to servers. |
|  | Code Signing | Certificates associated with key pairs used to sign active content. |
|  | Secure Email | Certificates associated with key pairs used to sign e-mail messages. |
|  | Encrypting File System | Certificates associated with key pairs that encrypt and decrypt the symmetric key used for encrypting and decrypting data by Encrypting File System (EFS). |
|  | File Recovery | Certificates associated with key pairs that encrypt and decrypt the symmetric key used for recovering encrypted data by Encrypting File System (EFS). |

When you look at the contents of a certificate store in Logical Store mode, you will occasionally see what appears to be two copies of the same certificate in the store. This occurs because the same certificate is stored in separate physical stores under a logical store. When the contents of the physical certificates stores are combined into one logical store view, both instances of the same certificate are displayed.

You can verify this by setting the view option to show the physical certificate stores and then noting that the certificate is stored in separate physical stores under the same logical store. You can verify that it is the same certificate by comparing the serial numbers.

**Security with certificates**

Certificates can be used for:

* Authentication, which verifies the identity of someone or something.
* Privacy, which ensures that information is only available to the intended audience.
* Encryption, which disguises information so that unauthorized readers are unable to decipher it.
* Digital signatures, which provide nonrepudiation and message integrity.

**Authentication**

Authentication is crucial to secure communication. Users must be able to prove their identity to those with whom they communicate and must be able to verify the identity of others. Authentication of identity on a network is complex because the communicating parties do not physically meet as they communicate. This can allow an unethical person to intercept messages or to impersonate another person or entity.

The digital certificate is a common credential that provides a means to verify identity. Certificates use cryptographic techniques to address the problem of the lack of physical contact between those communicating. Using these techniques limits the possibility of an unethical person intercepting, altering, or counterfeiting messages. These cryptographic techniques make certificates difficult to modify. Thus, it is difficult for an entity to impersonate someone else.

The data in a certificate includes the public cryptographic key from the certificate subject's public and private key pair. A message signed with its sender's private key can be verified by the message's recipient as authentic by using the sender's public key. This key can be found on a copy of the sender's certificate. Verifying a signature with a public key from a certificate proves that the signature was produced using the certificate subject's private key. If the sender has been vigilant and has kept the private key secret, the receiver can be confident in the identity of the message sender.

A few of the ways certificates are used to provide authentication are:

* Authentication of a user to a secure Web site via the Transport Layer Security (TLS) or the Secure Sockets Layer (SSL) protocol.
* Authentication of a server to a user via TLS.
* Logging on to a Windows Server 2003 domain.

**Privacy**

Communications on a network, such as the Internet, are subject to possible monitoring by unknown and, perhaps, malicious users. Public networks are treacherous for unencrypted sensitive information because anyone can access the network and analyze the data being transmitted between two points. Even private local area networks (LANs) are vulnerable to determined efforts by intruders to acquire physical access to the network. Consequently, if sensitive information is transmitted between computing devices on any type of network, users will almost certainly want to use some sort of encryption to keep their data private.

Public key encryption is not used to encrypt large amounts of data. Instead, data is typically protected with secret key encryption and, in turn, that secret key is encrypted with the public key of the recipient of the data. The encrypted secret key will then be transmitted to the recipient along with encrypted data itself. The recipient will use the private key to decrypt the secret key. The secret key will then be used to decrypt the message itself.

Certificates enable privacy of transmitted data using a number of different methods. Some of the commonly used privacy-enabling protocols that use certificates are:

* Secure Multipurpose Internet Mail Extensions (S/MIME)
* Transport Layer Security (TLS)
* Internet Protocol security (IPSec). For more information, see [Introducing IPSec](http://technet.microsoft.com/en-us/library/cc757786(WS.10).aspx).

**Encryption**

Encryption can be thought of as locking something valuable into a strong box with a key. Conversely, decryption can be compared to opening the box and retrieving the valuable item. On computers, sensitive data in the form of e-mail messages, files on a disk, and files being transmitted across the network can be encrypted using a key. Encrypted data and the key used to encrypt data are both unintelligible.

Typically, public key encryption is not used to encrypt large amounts of data. However, public key cryptography does offer an efficient method to send someone the secret key that is used when a symmetric encryption operation is performed on a large amount of data.

As an example, suppose Bob wants to send Alice a large number of encrypted files. For performance reasons, he will use a symmetric encryption key algorithm, such as Data Encryption Standard (DES), to encrypt the data. To send the encrypted data and the DES secret key needed to decrypt the data securely, Bob will encrypt the secret key with Alice's public key obtained from her certificate. Because her public key was used to encrypt the secret key, Alice, using her private key, will be the only one able to decrypt the DES secret key and thus decrypt the DES-encrypted data.

**Digital signatures**

A digital signature is a way to ensure the integrity and origin of data. A digital signature provides strong evidence that the data has not been altered since it was signed and it confirms the identity of the person or entity who signed the data. This enables the important security features of *integrity* and *nonrepudiation*, which are essential for secure electronic commerce transactions.

Digital signatures are typically used when data is distributed in plaintext, or unencrypted form. In these cases, while the sensitivity of the message itself may not warrant encryption, there could be a compelling reason to ensure that the data is in its original form and has not been sent by an impostor because, in a distributed computing environment, plaintext can conceivably be read or altered by anyone on the network with the proper access, whether authorized or not.