Types of certification authorities

A certification authority (CA) accepts a certificate request, verifies the requester's information according to the policy of the CA, and then uses its private key to apply its digital signature to the certificate. The CA then issues the certificate to the subject of the certificate for use as a security credential within a public key infrastructure (PKI). A CA is also responsible for revoking certificates and publishing a certificate revocation list (CRL).

A CA can be an outside entity, such as VeriSign, or it can be a CA that you create for use by your organization by installing Microsoft Certificate Services. Each CA can have distinct proof-of-identity requirements for certificate requesters, such as a Windows Server 2003 family domain account, employee badge, driver's license, notarized request, or physical address. Identification checks such as this often warrant an onsite CA, so that organizations can validate their own employees or members.

Microsoft enterprise CAs use a person's user account credentials as proof of identity. In other words, if you are logged on to a Windows Server 2003 family domain and request a certificate from an enterprise CA, the CA knows that you are who the Active Directory directory service says you are.

Every CA also has a certificate to confirm its own identity, issued by another trusted CA or, in the case of root CAs, issued by itself. It is important to remember than anyone can create a CA. The real question revolves around whether you, as a user or an administrator, trust that CA and, by extension, the policies and procedures that CA has in place for confirming the identity of the entities issued certificates by that CA.

Root and subordinate certification authorities

A *root CA*, sometimes called a root authority, is meant to be the most trusted type of CA in an organization's PKI. Typically, both the physical security and the certificate issuance policy of a root CA are more rigorous than those for subordinate CAs; if the root CA is compromised or issues a certificate to an unauthorized entity, then any certificate-based security in your organization is suddenly vulnerable. While root CAs can be used to issue certificates to end users for such tasks as sending secure e-mail, in most organizations they will only be used to issue certificates to other CAs, called subordinate CAs.

A *subordinate CA* has been certified by another CA in your organization. Typically, a subordinate CA will issue certificates for specific uses, such as secure e-mail, Web-based authentication, or smart card authentication. Subordinate CAs can also issue certificates to other, more subordinate CAs. Together, a root CA, the subordinate CAs that have been certified by the root, and subordinate CAs that have been certified by other subordinate CAs form a certification hierarchy.

Enterprise certification authorities

The Enterprise Administrator can install Certificate Services to create an enterprise certification authority (CA). Enterprise CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions), authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), and logging on to a Windows Server 2003 family domain using a smart card.

An enterprise CA has the following features:

1. An enterprise CA requires the Active Directory directory service.
2. When you install an enterprise root CA, it uses Group Policy to propagate its certificate to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. You must be a Domain Administrator or be an administrator with write access to Active Directory to install an enterprise root CA.
3. Certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards.
4. The enterprise exit module publishes user certificates and the certificate revocation list (CRL) to Active Directory. In order to publish certificates to Active Directory, the server that the CA is installed on must be a member of the Certificate Publishers group. This is automatic for the domain the server is in, but the server must be delegated the proper security permissions to publish certificates in other domains. For more information about the exit module.

An enterprise CA uses certificate types, which are based on a certificate template. The following functionality is possible when you use certificate templates:

1. Enterprise CAs enforce credential checks on users during certificate enrollment. Each certificate template has a security permission set in Active Directory that determines whether the certificate requester is authorized to receive the type of certificate they have requested.
2. The certificate subject name can be generated automatically from the information in Active Directory or supplied explicitly by the requestor.
3. The policy module adds a predefined list of certificate extensions to the issued certificate. The extensions are defined

by the certificate template. This reduces the amount of information a certificate requester has to provide about the certificate and its intended use.

Certificate Authority Policy and Exit Modules

One powerful administrative feature of Certificate Services is the ability to control and customize the behavior of the certification authority (CA) through the use of policy and exit modules.

Policy modules can determine whether a certificate request should be automatically approved, denied, or marked as Pending. Exit modules provide an opportunity to perform post-processing after a certificate is issued.

Certificate Services comes with one exit module (Certxds.dll) and one policy module (Certpdef.dll). The policy module includes two separate policies: enterprise and stand-alone. As a CA administrator, you can replace these default modules with your own custom policy and exit modules or commercial policy and exit modules.

If you have upgraded to Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition Certificate Services from an earlier version of Certificate Services, you will have the option of using the policy module you have been using prior to upgrading. It will either be listed as a *legacy* policy module when you look at the properties of the CA or with its original name, depending on how it was created.

The policy module provided for the Microsoft CA determines the default action of a certification authority upon receiving a certificate request. Upon receiving a certificate request, a certification authority can either automatically issue a certificate or hold it as Pending until an administrator reviews the request. This is the policy module at work for the CA!

In the majority of instances, the administrator of a stand-alone CA will want to have all incoming certificate requests set to Pending. Because the stand-alone CA does not verify the identity of requesters via the Active Directory service, there is no way to verify the identity and validity of the certificate requester.

The CA can only have one policy module loaded at a time. The Windows 2000 CA policy module contained a great deal of functionality that has been integrated into the core certification authority functionality. This allows the policy module to be more easily replaced without losing functionality.

The exit module that is provided with the Microsoft CA performs the following functions:

1. Sends e-mail when a certification event occurs. If the CA is configured to send e-mail when specific events occur, the exit module will do so.
2. Allows certificate publication to the file system. If the certificate request specifies a location to publish the certificate in the file system, the exit module will do so.

These two options are not an exhaustive list of the functions of the exit module. Unlike the policy module, multiple exit modules can be used by a CA simultaneously.

Configuring the policy and exit modules

The administrator of a certification authority (CA) can configure settings in the default policy and exit modules provided with Certificate Services by using the Certification Authority snap-in.

As a CA Administrator, using the policy module, you can change the default action of the certification authority upon receiving a valid certificate request.

You can specify whether a stand-alone CA will hold incoming certificate requests as Pending or automatically issue the certificate. In most cases, for security reasons, it is recommended that all incoming certificate requests to a stand-alone CA be marked as Pending.

To set the default action upon receipt of a certificate request

1. Log on to the system as a Certification Authority Administrator.
2. Open Certification Authority.
3. In the console tree, click the name of the certification authority (CA).

Where do we do this?

4. Certification Authority (computer name/CA name)
5. On the Action menu, click Properties
6. On the Policy Module tab, click Properties
7. Click the option you want your CA to have.
   a. Normally Pending or Automatically issue the Certificate
8. Stop and Start the Certificate Services to effect this change.

A Security Word of Caution: Remember that Enterprise CA's use AD services for authentication, while stand-alone CA's cannot use AD services. Thus for stand-alone CA's, the the CA administrator is responsible for verifying the identity of the certificate requestor. Thus, since certificates provide trust relationships, for security reasons, it is strongly recommended that all incoming certificate requests to a stand-alone CA be marked as "pending."

You can configure the CA to send e-mail when a certification event occurs, such as the issuance of a certificate or when a certificate request is set to pending.

Steps To send e-mail when a certification event occurs

1. Open a command prompt, and type

   certutil -setreg exit\smtp\smtpserver *ServerName*

and then type certutil -setreg exit\smtp\eventfilter *+Event*

The following table shows parameters for these commands

Value	Description
certutil	Specifies the name of the command-line program.
-setreg	Modifies the registry.
exit\smtp\smtpserver	Indicates the registry value that contains the name of the Simple Mail Transfer Protocol (SMTP) server.
exit\smtp\eventfilter	Indicates the registry value that contains the list of events that the certification authority (CA) should monitor. When any of these events occur, the CA will send e-mail.
+	Indicates that, if there are current entries stored in this registry value, this entry should be appended to them.
Event	Specifies the event to add to the list of events for the CA to monitor. An event can be any value in the following table:

Once you have issued this command, the next items are for the events which the CA will monitor before it sends the appropriate emails. There are quite a few of these events, which are summarized in the next table.

Event value	Description
ExitEvent_CertIssued	Specifies the action of issuing a certificate.
ExitEvent_CertPending	Specifies the action of a certificate request being received by the CA and set to Pending.
ExitEvent_CertDenied	Specifies the action of a certificate request being received by the CA and that request being denied.
ExitEvent_CertRevoked	Specifies the action of a revocation of an existing certificate.
ExitEvent_CRLIssued	Specifies the action of a certificate revocation list being issued.
ExitEvent_Startup	Specifies the action of the certification authority starting.
ExitEvent_Shutdown	Specifies the action of the certification authority shutting down.

A word of caution here. Because these items edit the Windows registry, incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

Notes to consider when using these techniques.

1. To perform this procedure, you must be a member of the *Administrators group on the local computer*, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using *Run as* to perform this procedure.

2. To open a command prompt, click Start, point to All programs, point to Accessories, and then click Command prompt.
3. When the ExitEvent_CRLIssued, ExitEvent_Startup and ExitEvent_Shutdown events occur, the CA does not know where to send the e-mail, as there is no user associated with this event.
4. Therefore, an e-mail address must be configured when using these events. To configure the e-mail address to send e-mail to when these events occur, type the following certutil.exe commands at a command prompt:

   certutil -setreg exit\smtp\CRLIssued\To*E-mailString*

   certutil -setreg exit\smtp\Startup\To*E-mailString*

   certutil -setreg exit\smtp\Shutdown\To*E-mailString*

5. *E-mailString* specifies an e-mail address or a string of e-mail addresses that are separated by semicolons.
6. If the SMTP server is not set to accept anonymous connections, the CA must be configured to provide a user name and password when it connects.
7. To configure the CA to authenticate with the SMTP server, type the following certutil.exe commands at a command prompt:

   certutil -setreg exit\smtp\SMTPAuthenticate 1

   certutil –setsmtpinfo*UserName*

8. *UserName* specifies the user name of a valid account on the SMTP server. Certutil will prompt you to provide the password for this user name.
9. To view the complete syntax for this command, at a command prompt, type: ***certutil -setreg -?***

Stand-alone certification authorities

You can install Certificate Services to create a stand-alone certification authority (CA). Stand-alone CAs can issue certificates for purposes such as digital signatures, secure e-mail using S/MIME (Secure Multipurpose Internet Mail Extensions), and authentication to a secure Web server using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

A stand-alone CA has the following characteristics:

1. Unlike an enterprise CA, a stand-alone CA does not require the use of the Active Directory directory service. Stand-alone CAs are primarily intended to be used as Trusted Offline Root CAs in a CA hierarchy or when extranets and the Internet are involved.

2. If you want to use a custom policy module for a CA, you would first install a stand-alone CA and then replace the stand-alone policy module with your custom policy module.

3. When submitting a certificate request to a stand-alone CA, a certificate requester must explicitly supply all identifying information about themselves and the type of certificate that is wanted in the certificate request. (This does not need to be done when submitting a request to an enterprise CA, since the enterprise user's information is already in Active Directory and the certificate type is described by a certificate template). The authentication information for requests is obtained from the local computer's Security Accounts Manager database.

4. By default, all certificate requests sent to the stand-alone CA are set to Pending until the administrator of the stand-alone CA verifies the identity of the requester and approves the request.

This is done for security reasons, because the certificate requester's credentials are not verified by the stand-alone CA.

5. Certificate templates are not used.

6. No certificates can be issued for logging on to a Windows Server 2003 family domain using smart cards, but other types of certificates can be issued and stored on a smart card.

7. The administrator has to explicitly distribute the stand-alone CA's certificate to the domain user's trusted root store or users must perform that task themselves.

When a stand-alone CA uses Active Directory, it has these additional features:

1. If a member of the Domain Administrators group or an administrator with write access to Active Directory, installs a stand-alone root CA, it is automatically added to the Trusted Root Certification Authorities certificate store for all users and computers in the domain. For this reason, if you install a stand-alone root CA in an Active Directory domain, you should not change the default action of the CA upon receiving certificate requests (which marks requests as Pending). Otherwise, you will have a trusted root CA that automatically issues certificates without verifying the identity of the certificate requester.

2. If a stand-alone CA is installed by a member of the Domain Administrators group of the parent domain of a tree in the enterprise, or by an administrator with write access to Active Directory, then the stand-alone CA will publish its CA certificate and the certificate revocation list (CRL) to Active Directory.

Auditing and Backing Up a certification authority

To configure event auditing:

1. Log on to the system as a Certification Authority Administrator or as a CA Auditor.

2. Open the Certification Authority management console

3. In the console tree, click the name of the CA you want to configure auditing on.

4. On the Action menu, click Properties

5. On the Audit Tab, click on the events you want to audit.

Using the Certificate Authority MMC to backup the CA

The steps to backup the Microsoft CA are as follows:

1. Log on to the system as a Backup Operator or a Certification Authority Administrator.
2. Open Certification Authority
3. In the console tree, click the name of the certification authority (CA) you want to backup.
4. On the Action menu, point to All Tasks, and click Back Up CA.
5. Follow the instructions in the Certification Authority Backup Wizard.

Using the Command-Line Certutil utility to backup the CA

1, Open a command prompt

2. At the command prompt, type certutil -backup *BackupDirectory*

Using Certificates with users from other companies with Exchange

First off, there are two types of Certification Authorities, the Enterprise and the Stand-alone. They are quite different.

The Enterprise CA uses the active directory, and can issue certificates with just active directory authentication. Secondly, using Windows Server 2003's Enterprise version, the templates in the Enterprise CA can be modified to produce what you need in specialized certificates.

The stand-alone CA does not use the Active directory and issues certificates with OUIs. Given the proper OUI, a certificate can achieve desired results.

So if you are using an Active Directory and an Enterprise CA, you will be using AD accounts. People in another company will not normally have AD accounts, and thus not be able to get user certificates for Exchange use.

Thus, the easiest way to accomplish the task of allowing users in other companies to securely send email to your employees is to give users from the other company an AD account, and use the Enterprise CA to issue them a certificate. This is what we did in our class. Of course, we need to put these "other users" into a group and an OU and severely restrict that OU and the group.

If granting users from other companies AD accounts, however restricted, is not something your company wants to do, the next thing is to use the stand-alone CA. The problem here is that this CA can issue some certificates, but nowhere near what the Enterprise CA can issue.

Exchange users need to have certificates with the proper OIDs that Exchange requires. If you can get the stand-alone CA to do this, the

certificates it issues to employees outside your AD will work properly with Exchange. The necessary OID's for Exchange are in the class notes.

Then the question remains: *How do I build a certificate appropriate for Exchange users with the stand-alone CA?* Basically, you use the CA's output module to tailor the user and email certificates to have the right OIDs.

Here is an outline of what needs to be done.

1. The stand-alone CA does not use AD accounts; it is only interested in the right OIDs.

2. On the stand-alone CA, you can issue by default a user and a client certificate.

3. On the stand-alone CA, you use the output module and work with something similar to a Capolicy.inf file, and then figure out how to build the output module.

4. Using this technique, you are creating a custom template with the proper OIDs in it. The exact OIDs for Exchange are in the course.

5. If the certificate has the OIDs exchange wants, it will work ok with Exchange.