



Operating System

Setting up a Certificate Authority

Beta 3 Technical Walkthrough

Abstract

This technical walkthrough describes the different types of public key Certificate Authorities (CAs) available for the Microsoft® Windows® 2000 operating system, and provides procedures for setting up a CA service in Windows 2000 Beta 3.

A CA service issues the certificates needed to run a public key infrastructure. The CA can be a commercial CA that services external customers, or it can be a CA run by your company that services internal needs. The certificates issued by the CA can be used for purposes such as smart card logon, sending encrypted e-mail, signing documents, and more. Because CAs are an important trust point in an organization, most organizations will have their own CA.

© 1999 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

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

Microsoft, Active Directory, Windows, the Windows logo, and Windows NT are registered trademarks of Microsoft Corporation.

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

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA
0699*

CONTENTS

INTRODUCTION	1
CERTIFICATE AUTHORITY REQUIREMENTS	2
Enterprise Root CA	2
Enterprise Subordinate CA	2
Standalone Root CA	2
Standalone Subordinate CA	2
CERTIFICATE AUTHORITY SETUP WALKTHROUGH	4
Certificate Authority Setup	4
Verify Certificate Server Installation	8
Certificate Server Uninstall	8
Installing a Subordinate CA Certificate from a File	8
KNOWN ISSUES	10
FOR MORE INFORMATION	11

INTRODUCTION

This technical walk through will help you set up a public-key Certificate Authority (CA) in a Microsoft® Windows® 2000 Server operating system.

A Certificate Authority is a service that issues the certificates needed to run a public key infrastructure. The CA could be an external commercial CA, or it could be a CA run by your company. The certificates enable a user to perform smart card logon, send encrypted e-mail, sign documents, and more. Since a CA is an important trust point in an organization, most organizations will have their own CA.

Microsoft Windows 2000 provides two types of CAs, determined by which policy modules are selected during installation—an *enterprise* CA or a *standalone* CA. Within these classes, there can be two types of CAs—a *root* or a *subordinate*. The policy modules define the actions that a CA can take when it receives a certificate request. Note that by changing the policy modules, it is possible to change the functionality of the system. A customer can write a policy module and customize the CA's behavior using the Windows 2000 Software Development Kit (SDK).

Typically, you should install an enterprise CA if you will be issuing certificates to users or computers inside an organization that is part of a Windows 2000 domain. You should install a standalone CA if you will be issuing certificates to users or computers outside of a Windows 2000 domain. An enterprise CA requires that all users requesting certificates have an entry in the Windows 2000 Active Directory™ directory services, and a standalone CA does not. Also, an enterprise CA can issue certificates that are used to log on to a Windows 2000 domain, and a standalone CA cannot.

CAs are organized into hierarchies with the fundamental trust point—or root CA—at the top. All other CAs in the hierarchy are subordinate CAs, and are trusted only because the root is trusted. The enterprise root CA is the trust point in the enterprise. There can be more than one enterprise root CA per Windows 2000 domain, and thus more than one hierarchy. It is also possible to mix and match standalone and enterprise CAs in a hierarchy to best suit your needs.

Enterprise CAs have a special policy module that enforces how certificates are processed and issued. The policy information used by these modules is stored centrally in a CA object in the Windows 2000 Active Directory. This means that to set up an Enterprise CA, you must have a working Windows 2000 Active Directory and DNS server.

In a standalone hierarchy, the standalone root CA is at the top. Each new standalone root CA starts a new hierarchy. Again, it is possible to mix and match standalone and enterprise CAs in a hierarchy to best suit your needs.

A standalone CA has a very simple policy module, and does not assume that a Windows 2000 Active Directory directory service is available. However, if an Active Directory is available, then the standalone CA will take advantage of it.

The next section of this paper describes the requirements for each type of CA in greater detail. You must meet all these requirements before installing the CA.

CERTIFICATE AUTHORITY REQUIREMENTS

This section describes the setup requirements for the various types of CAs.

Enterprise Root CA

An enterprise CA is the root of a Windows 2000-based corporate CA hierarchy. You should set up an enterprise CA if the CA will be issuing certificates to users and computers within your corporation. For security reasons, the enterprise CA is typically configured to issue certificates only to subordinate CAs.

The enterprise CA requires the following:

- Windows 2000 DNS Service installed (required by the Active Directory).
- Windows 2000 Directory Service installed. Enterprise policy places information into the Active Directory.
- Administrative privileges on the DNS, directory, and CA servers. This is especially important, because setup modifies information in numerous places, some of which require domain administrative privileges.

Enterprise Subordinate CA

An enterprise subordinate is a CA that issues certificates within a corporation, but is not the most trusted CA in that corporation. (It is subordinate to another CA in the hierarchy.)

The enterprise subordinate CA requires the following:

- A parent CA. This could be an external commercial CA or a standalone CA.
- Windows 2000 DNS Service installed (required by the Active Directory).
- Windows 2000 Directory Service installed. Enterprise policy places information into the Active Directory.
- Administrative privileges on the DNS, directory, and CA servers.

Standalone Root CA

A standalone CA is the root of a CA trust hierarchy. You should install a standalone root CA if you will be issuing certificates outside of a corporation's enterprise network. A root CA typically only issues certificates to subordinate CAs. For example, you want to issue certificates to your customers so they can access your Web site, and it is not feasible to give each one an account in your directory. Another example is if you intend to lock your root CA in a vault with no network access for security reasons, and want to allow only a few trusted people to access this server.

The standalone root CA requires administrative privileges on the local server.

Standalone Subordinate CA

A standalone subordinate CA is a CA that operates as a solitary certificate server, or exists in a CA trust hierarchy. You should set up a standalone subordinate CA when you will be issuing certificates to entities outside a corporation.

The standalone subordinate CA requires the following:

- An association with a CA that will process the subordinate CA's certificate requests. Again, this could be an external commercial CA.
- Administrative privileges on the local server.

CERTIFICATE AUTHORITY SETUP WALKTHROUGH

Certificate Authority Setup

Before you start

1. On the **Start** menu, point to **Programs**, then to **Administrative Tools** and click **Directory Management**.
2. Make sure that you can see and manage the Active Directory. Select the user folder to make sure your account is in the domain Administrators group. You must be an administrator to install the CA.
3. Ensure that the Internet Information Service (IIS) is installed (this is necessary if you want to install Certificate Services Web enrollment pages).

To set up the CA

1. On the **Start** menu, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**. The Add/Remove Programs dialog box appears.
3. Click **Add/Remove Windows Components** to start the **Windows Components Wizard**.
4. Click **Next** to begin configuring components.
5. Select **Certificate Server**, and then click **Next**. If you intend to use the Web components of the Certificate Services, then select the **IIS** check box.

The Certificate Server Web components allow you to do the following:

- Connect to the Web page to enroll for a certificate.
 - Download a CA certificate from the Web page.
 - Enroll for special purpose certificates, such as Internet Protocol Security (IPSec).
 - Save certificate request to file for processing by an external CA.
6. The wizard prompts you to specify the type of Certification Authority you want to set up. Setup attempts to guess which option is selected to make installation simpler.
 - If no Active Directory is detected, the two enterprise options will be disabled.
 - If an Active Directory is detected, the enterprise root CA will be selected if there are no CAs already registered in the Active Directory.
 - If there are CAs registered in the Active Directory, the enterprise subordinate CA will be selected.

If you will be issuing certificates to entities in your organization, or you need seamless integration with the Active Directory, or to enable smart card logon, then you should select an enterprise CA. Select one of the following:

- **Enterprise root CA**—If you do not have any CAs in your directory, or if you need a second enterprise root CA. The root CA will be registered in the

directory, and all computers in your enterprise using that directory will automatically trust the root CA. It is good security practice to limit the root CA to issuing certificates to subordinate CAs only, or to issuing only a few special purpose certificates. This means you want to install an enterprise subordinate after you finish installing the root. However, you can choose only the root CA.

- **Enterprise subordinate CA**—If you have already installed an Enterprise root CA. In general you will have multiple enterprise subordinate CAs. Each of these CAs will usually service either different communities of users, or provide different types of certificates. By having more than one subordinate, it is possible to revoke the subordinates certificate in case of disaster, and not have to reissue all certificates in the organization.

If you will be issuing certificates to entities outside your enterprise and do not want to use the Active Directory or other Windows 2000 Public Key Infrastructure (PKI) features, then you want astandalone CA. Select one of the following:

- **Standalone CA**—If you do not already have a standalone CA, or you need a second root for a purpose different than the first.
 - **Standalone subordinate CA**—If this CA will be a member of an existing CA hierarchy. The parent CA in the hierarchy can be a standalone CA, an enterprise CA, or an external commercial CA.
7. If you need to change the default cryptographic settings, click to select **Advanced options**. Select **Advanced options** only if you know how to change cryptographic settings.
 8. Click the **Next** button.
 9. If you selected **Advanced Options** the wizard will prompt you to specify the cryptographic service provider to use. (If you did not select **Advanced Options** proceed to step 10.)

This dialog box lets you change the cryptographic settings, such as Cryptographic Service Provider (CSP), hashing algorithm, and other advanced options. In general, you will not need to modify the default settings. Users who need to modify these settings must be very familiar with cryptography, Certificate Server, and the CAPI 2.0 architecture.

The list of CSPs will vary depending on the software and hardware that has been installed on the server. The **Key length** specifies the length of the public and private key pair. A value of **Default** in this box generates a key pair whose default length is determined by the selected provider. Microsoft recommends that you use a long key length, such as 1024 or 2048, for a root CA or an enterprise CA. (Note that a long key length is computationally more expensive, and may not be accepted by all hardware devices. For example, some smart cards may not accept certificates issued by a CA that has a 4096 bit key due to space limitations on the card.)

The **Use existing keys** option allows you to use keys that were generated previously or to reuse keys from a previously installed CA. When installing a CA you should almost never reuse keys. The exception to this is when you are restoring a CA after a catastrophic failure. You will then *import* a set of existing keys and install a new CA that uses those keys. In addition, if you are restoring a CA after a failure, you must check **Use the associated certificate**. This ensures that the new CA will have the identical certificate as the old CA. If you do not check this box, then a new certificate will be generated that makes the new CA different from the old CA.

Note The private key is always stored locally on the server except in the case where a cryptographic hardware device is used, in which case, the private key is stored in the device. The public key is placed in the certificate, and in the case of an Enterprise CA, the certificate is published in the Active Directory.

10. The wizard prompts you to supply identifying information appropriate for your site and organization

Note that the CA name (or common name) is critical because it is used to identify the CA object created in the Directory. The **Validity Duration** time can only be set for a root CA. Set the root CA Validity Duration to a reasonable value. The actual duration is a tradeoff between security and administrative overhead. Keep in mind that each time a root certificate expires, an administrator will have to update all trust relationships, and administrative steps will need to be taken to move the CA to a new certificate. A time period of two or more years is usually sufficient.

11. When you have completed the identifying information, click **Next**.

12. A dialog box defines the locations of the certificate database, configuration information, and the location where the Certificate Revocation List (CRL) is stored.

The Enterprise CA will always store its information, including the CRL, in the directory.

It is recommended that you select the **Shared folder** check box. This option specifies the location of a folder where configuration information for the CA will be stored. You should make this folder a UNC path and have all your CAs point to the same folder. Then the administration tools can use this folder for determining CA configuration if the Active Directory is not available. If you have an Active Directory, this folder is optional. If you do not have an Active Directory, this folder is required.

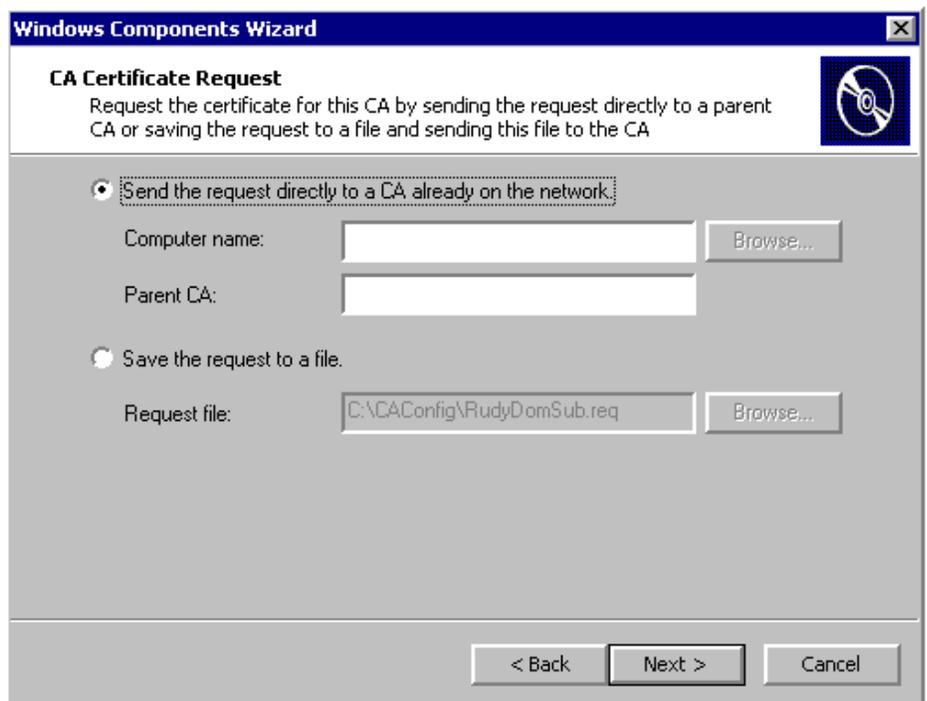
If you are installing a CA in the same location as a previously installed CA, then the Preserve existing certificate database option will be enabled. Check this option if you wish your new CA to use this Database, otherwise the database will be deleted.

13. When you have specified the storage locations for your information, click **Next**.

14. If IIS is running, the following message will appear, requesting that you stop the service. Click **OK** to stop IIS. You must stop IIS to install the Web components. If you do not have IIS installed, you will not see this message.

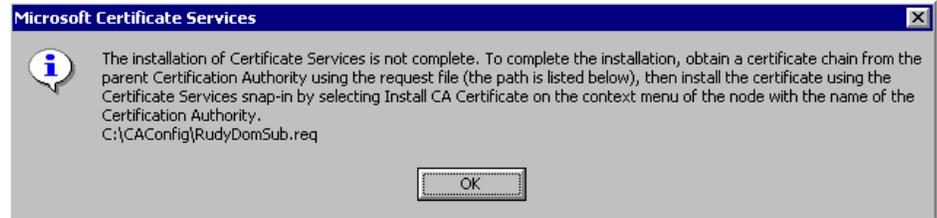


15. If you are installing a subordinate CA, the wizard next prompts you for information about how you will request the certificate.



Click **Browse** to locate an online CA, or select **Save the request to a file** if you will be making a request destined for a commercial CA or a CA that is not accessible from the network. (If you create a file, you must ~~take~~ **send** the file to a CA for processing. The CA provides you with a certificate, which you install using the MMC snap-in.) Then click **Next**.

16. If you created a certificate request to file, you will see the following message:



17. Press **OK** to finish the installation. Click **Finish** to close the wizard.

When the installation is finished, take the Certificate Request file you created to your CA, and have them process it. If you are using a Microsoft Certificate Service to process this file, you can refer to the Certificate Service Web Pages' walkthrough for details about how to process the request.

When you have your new certificate, use the Certificate Services MMC snap-in to install the certificate, and enable your CA.

Verify Certificate Server Installation

Whether you created an enterprise CA or a standalone CA, you can quickly check to see if your installation was successful:

The simplest way is to open a command window, and type **net start** to see if the Certificate Service is running.

- For an enterprise CA, open the Certificate Manager from the Start menu: Click **Start**, point to **Programs**, point to **Administrative Tools**, select **Certificate Manager**, and request a certificate.
- For a standalone CA, you can request a new certificate using Internet Explorer 5.0 by connecting to the URL `http://localhost/CertSrv`. Replace *localhost* with the name of the server. See the Certificate Service Web Pages' walkthrough for details.

Certificate Server Uninstall

To uninstall the CA

1. On the **Start** menu, point to **Settings**, and then click **Control Panel**.
2. Click **Add/Remove Programs**.
3. Click **Configure Windows**, and then click **Components**.
4. Clear the **Certificate Server** check box, and click **Next**.

Installing a Subordinate CA Certificate from a File

This section is to be used only by those people who created a certificate request file during installation of a subordinate CA.

Before you attempt this section, make sure you have taken the certificate request file you generated to your CA for processing. Your CA will provide you with a certificate for this file. If you are submitting this file to a Microsoft Certificate Service,

then you may want to refer to the 'Certificate Service Web Pages' walkthrough for detailed explanations on howto submit the request file.

This section uses the Certificate Service Manager snapin. Refer to the "Advanced Certificate Management" walkthrough for details.

1. Open the Certificate Service snapin.
2. Right-click the CA you want to install.
3. Click **Install CA Certificate**. The Install CA Certificate Wizard appears.
4. Follow the wizard, and select the file containing the certificate provided by your CA.
5. Click **Finish** to complete the setup.

Your CA is now installed and ready for verification.

KNOWN ISSUES

Standalone Policy Behavior Changed

Certificate Server standalone policy behavior has changed from Beta 2 and the version 1.0 product. In the past, the default policy module immediately processed requests and issued the certificate. The new standalone policy makes the request pending until an administrator manually approves the request. This new behavior affects only the standalone CAs. Enterprise policy still processes the request immediately. To change the policy behavior to immediately issue certificates, change the following registry key to a value of 1:

```
HKEY_LOCAL_MACHINE
  \System
    \CurrentControlSet
      \Services
        \CertSvc
          \Configuration
            \YourCAName
              \PolicyModules
                \CertificateAuthority_MicrosoftDefault.Policy
                  \RequestDisposition
```

A hex value of 101 will cause requests to be pended.

Installing Web Pages on a Remote Server

If the CA is an enterprise CA, the Certificate Services Web pages must be installed on the same computer as the CA. The CA needs to authenticate the client to ensure that it can request only the certificates they have permission to request. If the Web pages are on a different computer from the Web server, then the CA cannot authenticate the user.

Installing the CA and Web Server

The CA must be installed after the Web server to ensure that the Web pages are installed. If the CA is installed first, it will still to function, but you may not be able to access the Web pages. (You can enable the Web pages by running the command: `certutil -vroot`)

Upgrading Certificate Server 1.0

When you upgrade from Windows NT 4 to Windows 2000, the Certificate Services executable and dynamic-link library (DLL) files will need to be updated. Note that it is important to run the Dbcnvt.exe utility to convert the old version 1.0 database to the new format before the CA processes any new requests. Upgrades are not supported for any configuration that uses a version 1.0 database that has been modified.

FOR MORE INFORMATION

For the latest information on Windows 2000, visit our World Wide Web site at <http://www.microsoft.com/windows> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows2000 Beta 3, check out the World Wide Web site at <http://ntbeta.microsoft.com>

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported using the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce it and fix it. Refer to the Release Notes included on the Windows2000 Beta 3 distribution media for some of the known issues.