Windows 2000 Server and Key Management Server Interoperability

Topics on this Page

- Introduction
- Certification Authority Setup
- Scenarios
- Installing Trusted Root Certification Authorities
- KM Server Configuration
- Troubleshooting
- KM Server Forklift Upgrade Process
- Exchange 2000 Server
- Additional References

Operating System

Microsoft Product Support Services White Paper – Version 2.1

Written by David B. Cross, Windows Security; Gene Ferioli, Microsoft Consulting Services; Carsten B. Kinder, Microsoft Consulting Services

Published on March 14, 2000

Abstract

Microsoft® Exchange Server version 5.5 Service Pack 1 with Key Management server (KM server) introduced the capability to use X.509 V3 certificates with Exchange Server advanced security. With the robust public key infrastructure that is built into the Microsoft® Windows® 2000 Server operating system, you can combine KM server with a number of different certification authority configurations to achieve 128-bit advanced security with the Microsoft Outlook e-mail client. This white paper describes a variety of scenarios that integrate Windows 2000 Server certification authorities with Exchange Server 5.5 advanced security.

Introduction

Public key technology enables organizations to extend their businesses to the Internet, where strong distributed authentication and secure communication are critical to business-to-business and business-to-consumer interaction. The standards-based public key infrastructure (PKI) is interoperable with other PKI products in the Microsoft® Windows® 2000 Server operating system. Customers can deploy an integrated PKI as part of their server and desktop deployment, and manage that integrated PKI the same way that they manage other Windows 2000 Server security features.

Scope

This white paper describes Windows 2000 Server PKI interoperability with the Key Management server (KM server) component of Microsoft Exchange Server version 5.5, and Windows 2000 Server interoperability with other root certification authority (CA) providers. This white paper does not address Microsoft® Windows NT® Server version 4.0 setup or its interoperability with Exchange Server 5.5. This white paper also does not address third-party PKI products or solutions other than the use of a third-party CA as the root of a server hierarchy.

Operating System Requirements

For Exchange Server 5.5 KM server to use a Windows 2000 Server CA, both the

KM server and the CA *must* be running the Windows 2000 Server operating system; if Exchange Server is deployed on Windows NT Server 4.0, Exchange Server cannot communicate with a Windows 2000 Server CA. The Windows 2000 Server CA can be installed on the same computer that KM server is installed on, or on a separate physical server. To facilitate this change in an existing deployment, you can upgrade a computer running a Windows NT Server 4.0 KM server and Microsoft® Certificate Server version 1.0 to Windows 2000 Server, and set up Certificate Services.

If an organization does not want to upgrade the Exchange Server 5.5 KM server to Windows 2000 Server, that organization can only use a Windows NT Server 4.0 Certificate Server. The policy module that is installed for Exchange Server 5.5 KM server is an exclusive policy that ensures that the certificates the Certificate Server issues are marked for e-mail [or Secure/Multipurpose Internet Mail Extensions (S/MIME)] use only. After this module is installed on any CA, that authority cannot service other types of certificate requests. Therefore, to support the KM server functions, a Windows 2000 Server CA must be a stand-alone CA; it cannot be used as an enterprise CA.

Windows 2000 Server CA Basics

Windows 2000 Server provides two classes of CAs: an enterprise CA or a stand-alone CA. The CA class is determined by the policy module that you select during installation. In each CA class, there are 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. A stand-alone CA has a very simple policy module and does not assume that Windows 2000 Active Directory™ is available. Note that if you change the policy modules, you can change the way the system functions.

CAs are organized into hierarchies that have the fundamental trust point, or root CA, at the top. All of the other CAs in the hierarchy are subordinate CAs, and are trusted only because the root is trusted. There may be more than one root CA for each Windows 2000 Server domain, and thus more than one hierarchy. A stand-alone subordinate CA has the following requirements:

- It must be associated with a CA that will process the subordinate CAs certificate requests. Again, this could be an external commercial CA.
- Administrative privileges on the local server.

X.509 V1 and X.509 V3 Certificate Differences

X.509 V1 certificates include fields for the version number, serial number, signature algorithm ID, issuer name, validity period, user name, and public key information for the user, and also include signatures on each of these fields. X.509 V3 certificates add fields for issuer-unique identifier; subject-unique identifier; and extensions, such as subject and issuer attributes, certification policy information, and key usage restrictions. You can use either version to digitally sign items (to verify the sender's identity and that the contents of the item have not changed) or to encrypt items. However, you can use only X.509 V3 certificates in S/MIME-specific encryption and decryption operations.

KM Server Basics

Exchange Server 5.5 has a Cryptography Service Provider (CSP) that isolates all of the KM server cryptography functions into one dynamic-link library (DLL). Versions of Exchange Server earlier than version 5.5 Service Pack 1 allow only one KM server for each organization. Multiple-site architectures must be configured so that individual sites point to one KM server. Exchange Server 5.5 Service Pack 1 KM server supports certificate trust lists, which allow cross-certification between organizations and up to one KM server for each Exchange

Server site. Certificate trust lists contain certificates from other trusted CAs (even those outside the Exchange Server architecture), are signed by the root CA for the Exchange Server organization, and are stored in the Exchange Server directory. Certificate trust lists allow inter-organization and intra-organization webs of trust, which clients can use to validate certificates that are attached to or associated with received items. Administrators can easily revoke trust for certificates in the certificate trust lists, if necessary.

With the release of Exchange Server 5.5 Service Pack 1, computers running Microsoft Certificate Server can also become CAs for Exchange Server 5.5 Service Pack 1 KM servers. An organization can install multiple KM servers— up to one KM server for each Exchange Server site. However, if you choose to have multiple KM servers in your organization, be aware that user histories (old encryption keys) may be lost. If a site is modified to point to a new KM server, user key histories are lost. To minimize such loss, create new KM servers only when you create new Exchange Server sites. For Exchange Server 5.5 KM server to run properly on Windows 2000 Server, Exchange Server 5.5 Service Pack 3 must be installed.

Key Recovery

Exchange Server 5.5 KM server provides key recovery for users who lose keys or forget passwords. KM server can recover an encryption key pair so that an end user can access previously encrypted items. To prevent administrators from impersonating users, digital signatures are treated differently and are never stored or recovered. In Exchange Server 5.5, when the client generates a new key pair, the new public key is placed in the directory, in addition to the previous public key. (Certificate fields in the Exchange Server directory are multivalued.) If the client requests a certificate directly from a Microsoft CA, and not in conjunction with the Exchange Server 5.5 KM server, key escrow or key recovery capability is not provided.

Supported Clients

Exchange Server 5.5 KM server supports X.509 V3 certificates for Microsoft® Outlook® 98 and Microsoft Outlook 2000; these are the only clients that currently support S/MIME. Although Microsoft Outlook Express version 5.0 does support S/MIME capabilities, it is a POP/SMTP client only, and does not operate with the Exchange 5.5 KM server system.

Third-Party Root CAs

Most third-party CAs operate properly with a Windows 2000 Server subordinate CA. This white paper does not provide detailed information about third-party configuration, but to ensure compatibility, make sure that the following conditions are true:

- The root CA conforms to Request for Comments (RFC) 2459.
- The subject and issuer names on the root CA are identical.
- The root CA signs subordinate CA requests with an expiration date that is later than two years after the date the subordinate CA requests are signed.
- The root CA publishes a Certification Revocation List (CRL) distribution point in its certificates, in accordance with RFC 2459.

Certification Authority Setup

Certification Authority Setup

Exchange Server 5.5 requires a Windows 2000 Server certification authority (CA) for S/MIME 128-bit encryption. The following are general steps to install

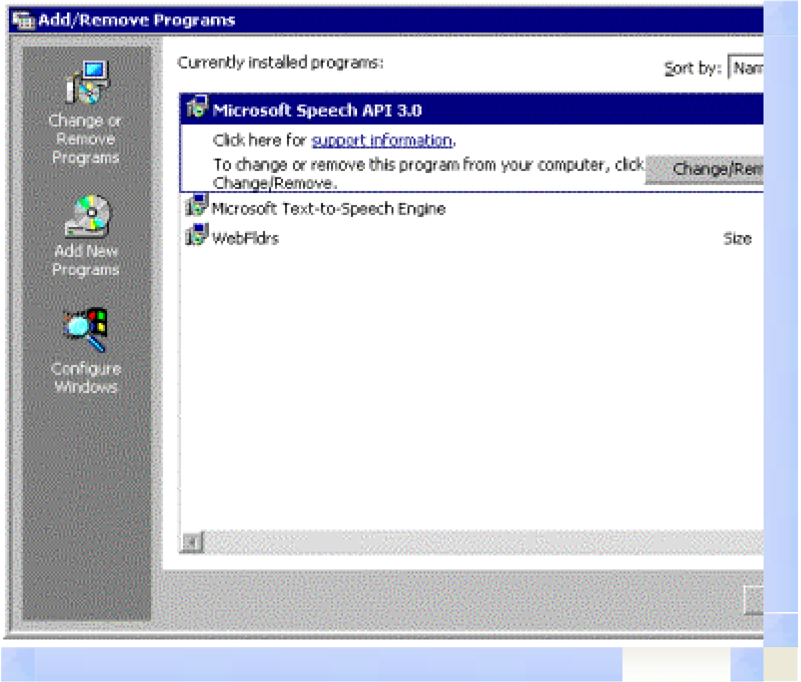
Windows 2000 Server Certificate Services for either a stand-alone root CA or a subordinate CA in a hierarchy.

Before you start:

- Make sure that your account is in the Domain Administrators group. This group is in the Users folder. You must be an administrator to install the CA.
- To install the Certificate Services Web enrollment pages, you need to ensure that Microsoft Internet Information Services (IIS) are already installed. Ensure that the computer running Microsoft Certificate Services does not have a name that contains more than 15 characters. Exchange Server 5.5 KM server does not support CAs that have names that contain more than 15 characters. To avoid future issues, do not use extended ASCII characters either.

To set up the CA:

1. Click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**. When an **Add/Remove Programs** dialog box similar to the following is displayed, click **Configure Windows**.

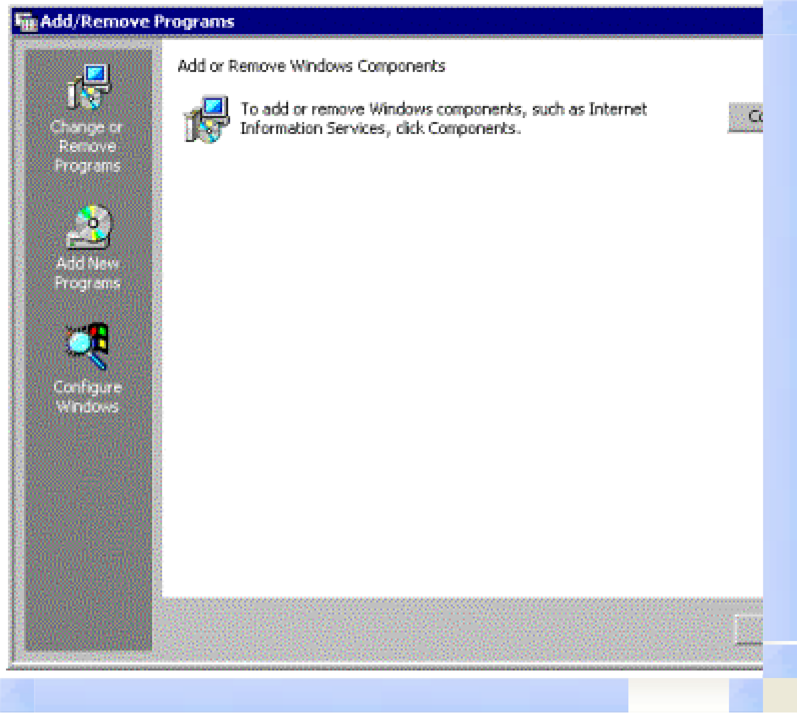


Click here for support information.

To change or remove this program from your computer, click Change/Remove.

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

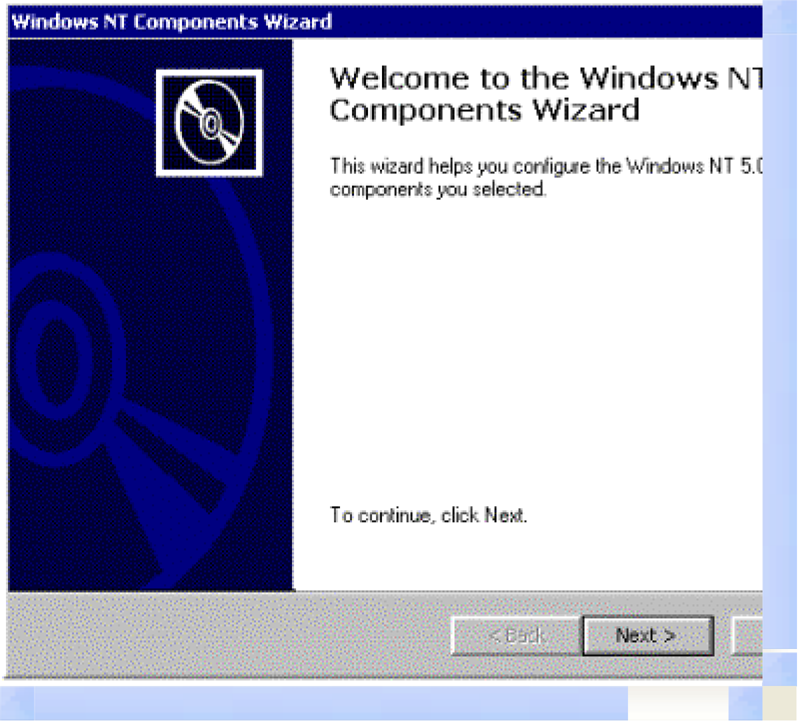
3. Click **Components**.



Add/Remove Programs
Change or Remove Programs
Add New Programs
Configure Windows
Add or Remove Windows Components
To add or remove Windows components, such as Internet Information Services, click Components.

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

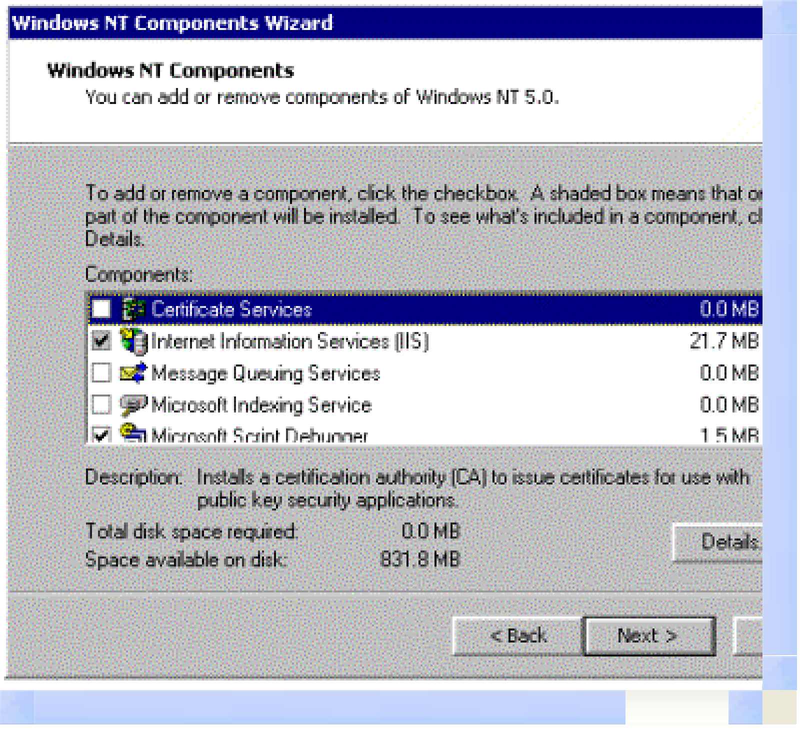
4. When a dialog box similar to the following is displayed, click **Next**.



Windows NT Components Wizard
Welcome to the Windows NT Components Wizard
This wizard helps you configure the Windows NT 5.0 components you selected.
To continue, click Next.
< Back
Next >

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

5. Click to select the **Certificate Services** check box, and then click **Next**.



Windows NT Components Wizard

Windows NT Components

You can add or remove components of Windows NT 5.0.

To add or remove a component, click the checkbox. A shaded box means that o part of the component will be installed. To see what's included in a component, cl Details.

Components:

□ Certificate Services	0.0 MB
☑ Internet Information Services (IIS)	21.7 MB
□ Message Queuing Services	0.0 MB
□ Microsoft Indexing Service	0.0 MB
☑ Microsoft Script Debugger	1.5 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security applications.

Total disk space required: 0.0 MB

Space available on disk: 831.8 MB

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

Note If you want to use the Web components of the Certificate Services, click to select the **Internet Information Services (IIS)** check box. When a warning message is displayed, click **OK**. The Certificate Services Web components allow you to:

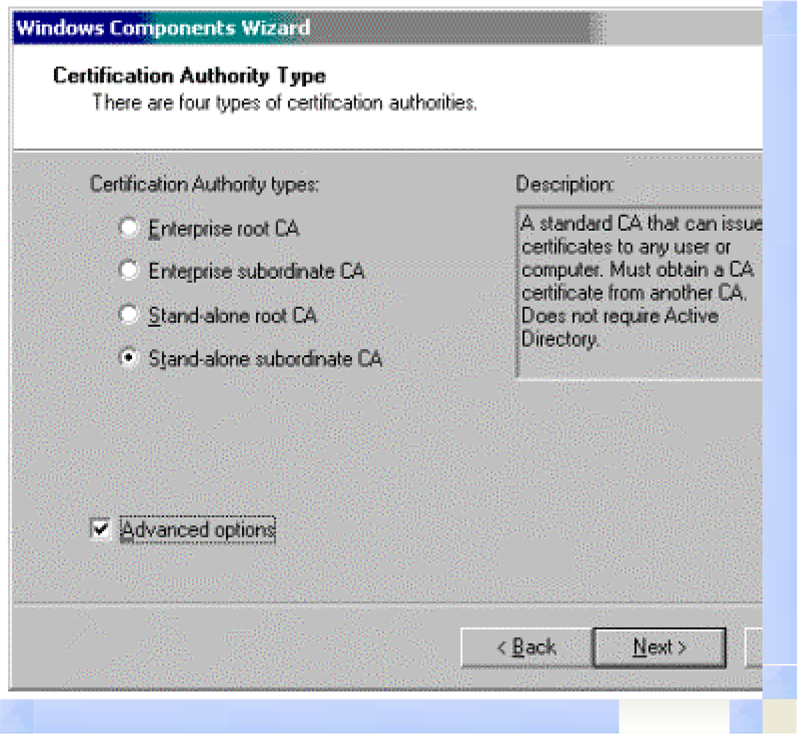
- Connect to the Web page to enroll for a certificate.
- Download a CA certificate from the Web page.
- Save the certificate request to a file so that it can be processed by an external CA.

When the **Certification Authority Type** dialog box is displayed, click one of the following CA types, as applicable:

- **Stand-alone root CA**. You need a stand-alone root CA if you do not already have a stand-alone CA, or if you need a second root to use for another purpose.
- **Stand-alone subordinate CA**. You need a stand-alone subordinate CA if this CA will be a member of an existing CA hierarchy. The parent CA in the hierarchy can be a stand-alone CA, a Windows 2000 Server enterprise CA, or an external commercial CA.

Caution An enterprise root or subordinate CA cannot be used with Exchange Server 5.5 KM server. However, Enterprise CAs will be supported by Microsoft Exchange 2000 Server KM server.

6. Click to select the **Advanced options** check box to change the default cryptographic settings, and then click **Next**.



Windows Components Wizard

Certification Authority Type

There are four types of certification authorities.

Certification Authority types:

- ○ Enterprise root CA
- ○ Enterprise subordinate CA
- ○ Stand-alone root CA
- ● Stand-alone subordinate CA

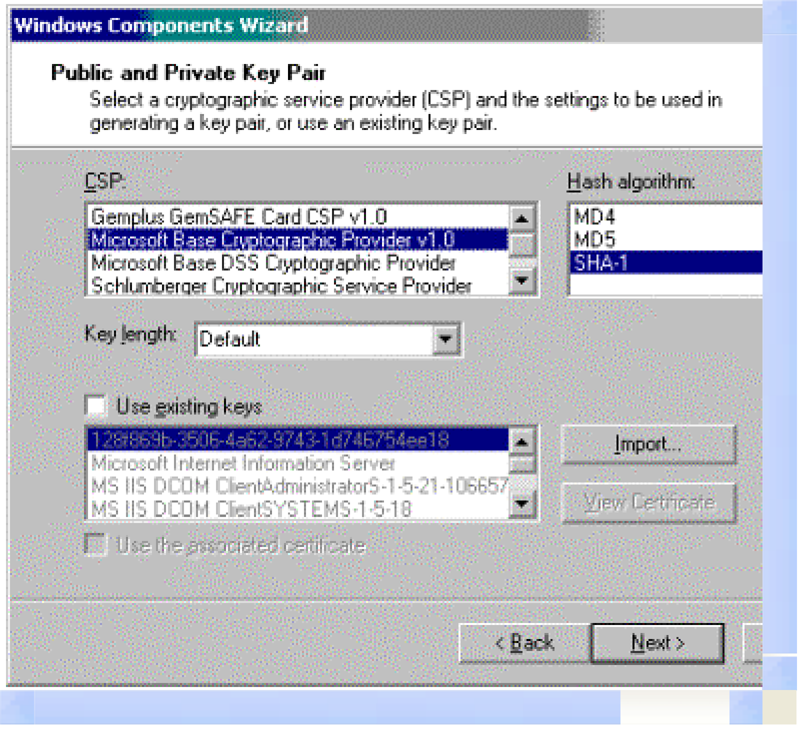
Description:

A standard CA that can issue certificates to any user or computer. Must obtain a CA certificate from another CA. Does not require Active Directory.

☑ Advanced options

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

7. Because you selected the **Advanced Options** check box, the **Public and Private Key Pair** dialog box is displayed, in which you can change the cryptographic settings, such as the cryptographic service provider (CSP), the hashing algorithm, and other advanced options.



Windows Components Wizard

Public and Private Key Pair

Select a cryptographic service provider (CSP) and the settings to be used in generating a key pair, or use an existing key pair.

CSP:

- Gemplus GemSAFE Card CSP v1.0
- Microsoft Base Cryptographic Provider v1.0
- Microsoft Base DSS Cryptographic Provider
- Schlumberger Cryptographic Service Provider

Hash algorithm:

- MD4
- MD5
- SHA-1

Key length: Default

□ Use existing keys

- 128f869b-3506-4a62-9743-1d746754ee18
- Microsoft Internet Information Server
- MS IIS DCOM ClientAdministratorS-1-5-21-106657
- MS IIS DCOM ClientSYSTEMS-1-5-18

□ Use the associated certificate

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

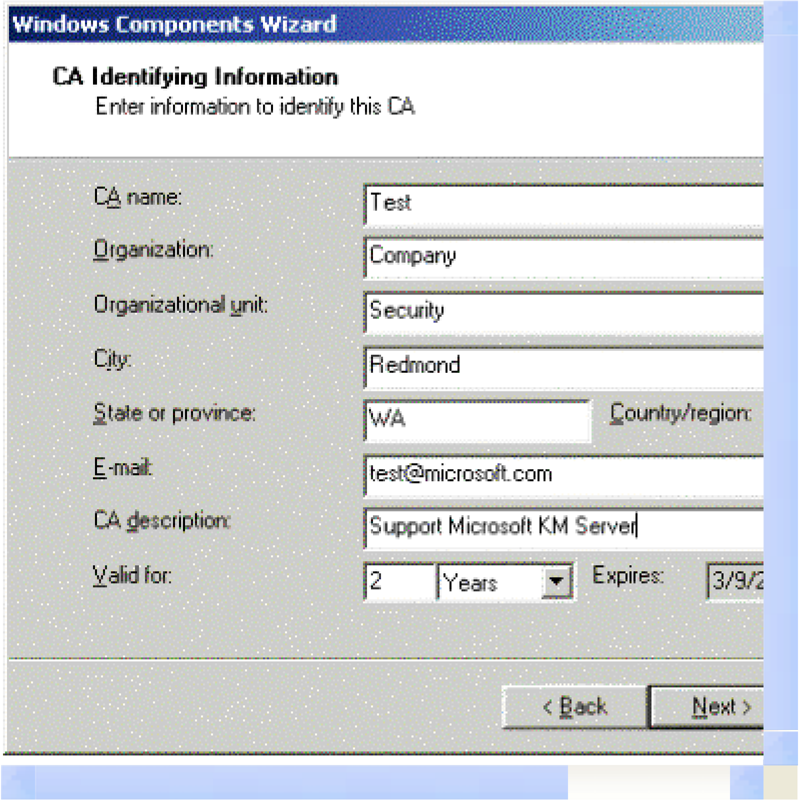
To support KM server, in the **CSP** list, click **Microsoft Base Cryptographic Provider v1.0**, and in the **Hash algorithm** list, click **SHA-1**. Make sure that the **Use existing keys** check box is cleared, and that in the **Key length** list, **Default** is selected.

8. The **CA Identifying Information** dialog box is displayed. Type the identifying information that is 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.

   You can only set the validity duration for a root CA. In the **Valid for** box, type a reasonable value to set the root CA validity duration. If you have subordinate Windows 2000 Server CA servers, make sure that the value is at least 3 (years). The KM server requires a certificate that is valid for at least two years; therefore, a subordinate CA or root must be able to issue certificates at least as long as the KM server can issue certificates.

   Root certificates that are valid for a short duration require additional management, because you must reissue root certificates to all of the client computers. The choice of a duration value is a trade-off between security and administrative overhead. Remember that each time a root certificate expires, an administrator must update all of the trust relationships and "roll" the CA to a new certificate. For information about how to modify the expiration date, please see the "Changing the Certificate Expiration Date" section of this white paper.

   After you type the identifying information, click **Next**.


Windows Components Wizard
CA Identifying Information
Enter information to identify this CA
< Back
Next >

CA name: Test
Organization: Company
Organizational unit: Security
City: Redmond
State or province: WA
Country/region:
E-mail: test@microsoft.com
CA description: Support Microsoft KM Server
Valid for: 2 Years
Expires: 3/9/2

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

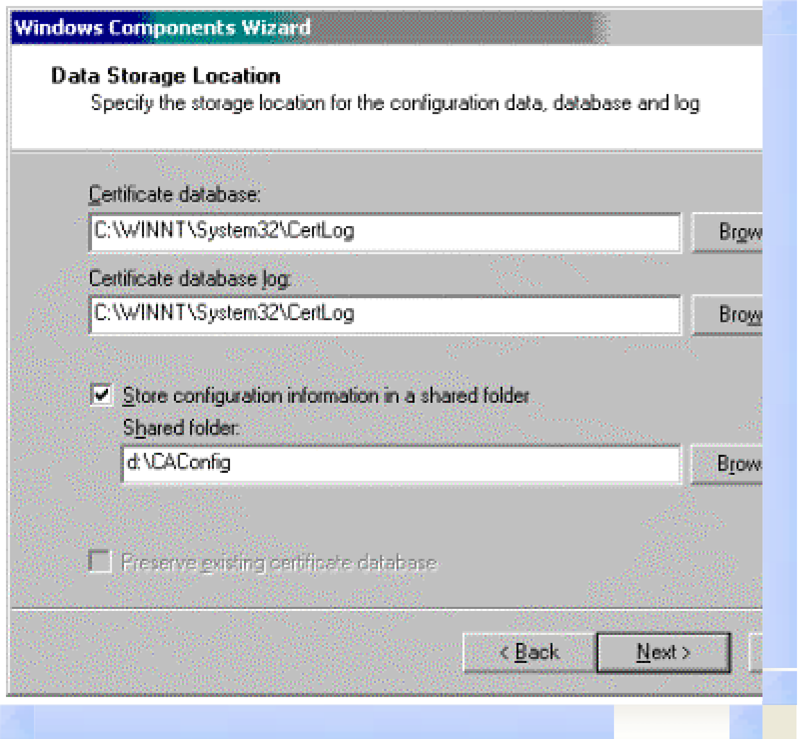
   Note The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

9. The **Data Storage Location** dialog box is displayed, in which you can define the location of the certificate database, the location of configuration information, and the location of the Certificate Revocation List (CRL). Click to select the **Store configuration information in a shared folder** check box to specify the location of the folder where configuration information for the CA is stored. In the **Shared folder** box, type a Universal Naming Convention (UNC) path for this folder, and make sure that all of your CAs point to the same folder. The CA Web client and KM server use this folder to

determine CA configuration.

If you are installing a CA in the same location as a previously installed CA, the **Preserve existing certificate database** check box is selected by default. Click **Next**.

Important Do not select the **Preserve existing certificate database** check box if you want to perform a new installation of the CA.



Windows Components Wizard

Data Storage Location
Specify the storage location for the configuration data, database and log

Certificate database:
C:\WINNT\System32\CertLog

Certificate database log:
C:\WINNT\System32\CertLog

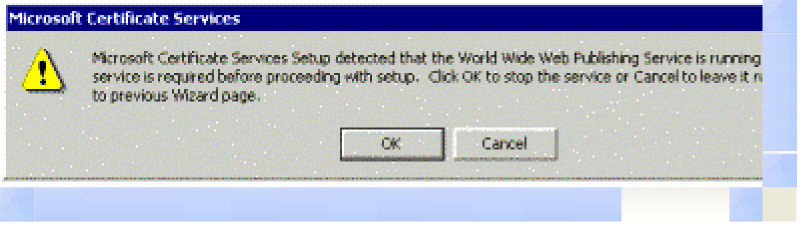
☑ Store configuration information in a shared folder

Shared folder:
d:\CAConfig

□ Preserve existing certificate database

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

10. If Microsoft Internet Information Service (IIS) is running, the following message is displayed. Click **OK** to stop IIS.



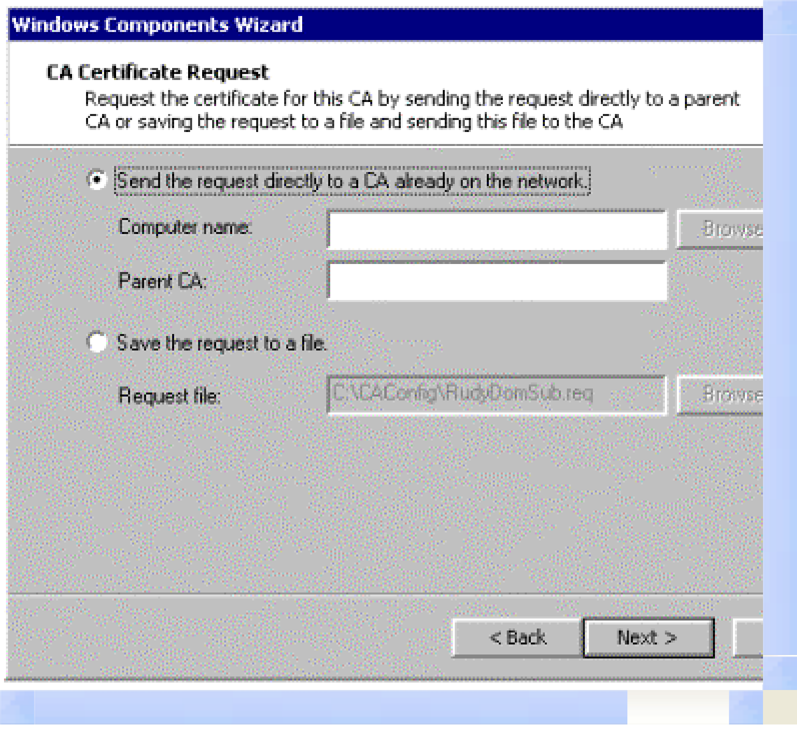
Microsoft Certificate Services

Microsoft Certificate Services Setup detected that the World Wide Web Publishing Service is running service is required before proceeding with setup. Click OK to stop the service or Cancel to leave it r to previous Wizard page.

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

You must stop IIS to install the Web components. If IIS is not installed, this dialog box is not displayed.

11. If you are installing a subordinate CA, the **CA Certificate Request** dialog box is displayed. To locate an online CA, click **Send the request directly to a CA already on the network**, and then click **Browse**, or if you are making a request for a commercial CA or a CA that is not accessible on the network (such as an offline root CA), click **Save the request to a file**. If you create a file, you need to take the file to an external or root CA to be processed. The CA provides you with a certificate. To enable your CA, use Microsoft Management Console (MMC) to install this certificate. For more information about this procedure, see the "Installing a Subordinate CA Certificate from a Request File" section of this white paper.



Windows Components Wizard

CA Certificate Request

Request the certificate for this CA by sending the request directly to a parent CA or saving the request to a file and sending this file to the CA

● Send the request directly to a CA already on the network.

Computer name:

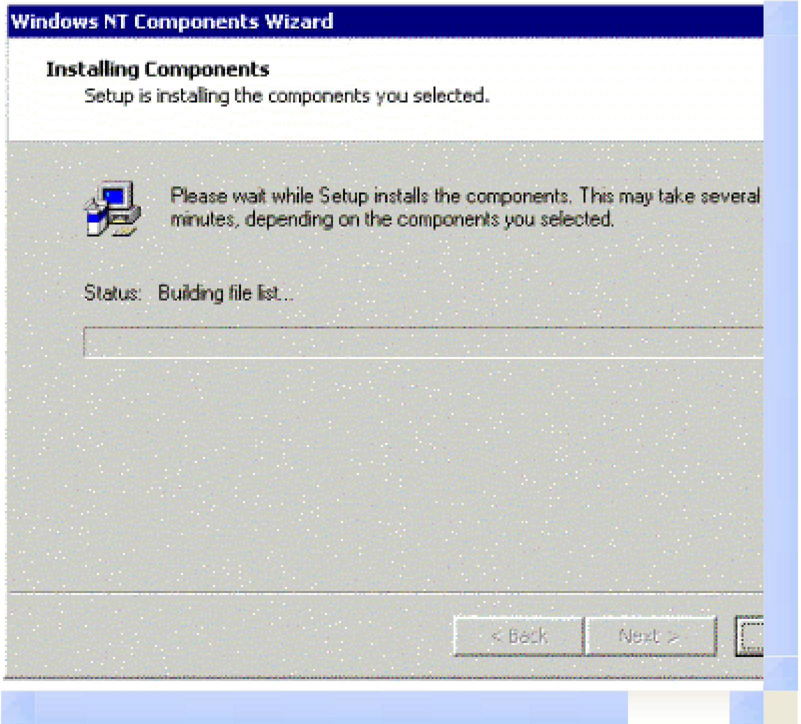
Parent CA:

○ Save the request to a file.

Request file: C:\CAConfig\RudyDomSub.req

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

12. The **Installing Components** dialog box is displayed. Wait until the installation finishes.



Windows NT Components Wizard

Installing Components

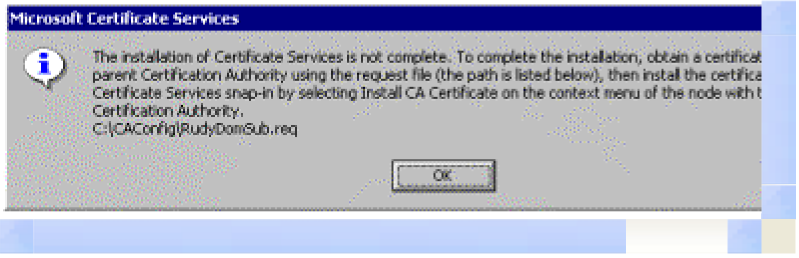
Setup is installing the components you selected.

Please wait while Setup installs the components. This may take several minutes, depending on the components you selected.

Status: Building file list...

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

13. If you are creating a certificate request to a file, the following message is displayed. Click **OK**.

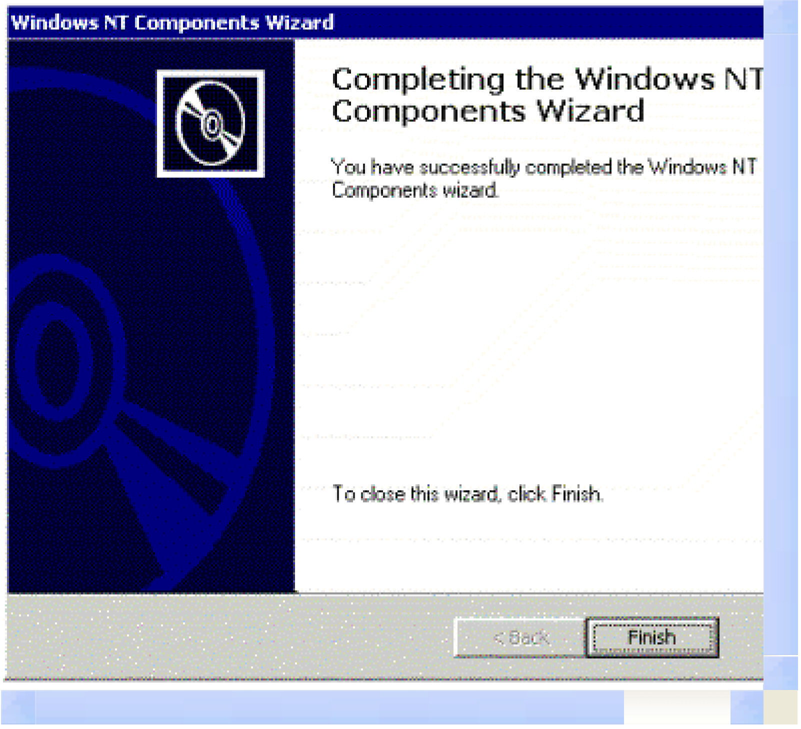


Microsoft Certificate Services

The installation of Certificate Services is not complete. To complete the installation, obtain a certificat parent Certification Authority using the request file (the path is listed below), then install the certifica Certificate Services snap-in by selecting Install CA Certificate on the context menu of the node with t Certification Authority.
C:\CAConfig\RudyDomSub.req

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

14. Click **Finish**.



Windows NT Components Wizard

Completing the Windows NT Components Wizard

You have successfully completed the Windows NT Components wizard.

To close this wizard, click Finish.

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

After you finish the installation, take the certificate request file that you created to the root or signing CA and have the request processed. Either a Microsoft Windows 2000 Server root CA or a third-party root CA can sign the request.

After you have your new certificate, use the Certificate Services MMC to install the certificate and enable your CA. For more information about this procedure, see the "Installing a Subordinate CA Certificate from a Request File" section of this white paper.

Note The root CA administrator needs to return both the signed request certificate and its own root CA certificate. If you do not already have the root CA certificate in the subordinate CA root store, you are prompted for it when you install the signed certificate request.

To Verify Certificate Services Installation

Perform one of the following steps to verify that the Certificate Services installation was successful:

- At a command prompt, type **net start**, and then make sure the Certificate Services are running. This is the simplest way to verify Certificate Services installation.

- For an enterprise CA, click the **Start** button, point to **Programs**, click **Administrative Tools**, click **Certificate Manager** to start Certificate Manager, and then request a certificate.
- For a stand-alone CA, request a new certificate by using Microsoft Internet Explorer version 5.0 to connect to the following URL:

  http://*local_host*/certsrv

  where *local_host* is the name of the server.

Installing a Subordinate CA Certificate from a Request File

Use the procedure outlined in this section only when a subordinate CA has been installed by using a certificate request file.

Before you perform the following steps, make sure that you take the certificate request file that you generated to your root CA for processing. Your root CA administrator provides you with a certificate for this file. If you submit this file to a Microsoft Certificate Service, you may want to refer to the Windows 2000 Server help files for detailed steps on this process.

Note The following steps use the Certification Authority MMC.

1. Start the Certification Authority MMC.
2. Right-click the CA that you want to install with a signed certificate from a root CA.
3. Click **Install CA Certificate**.
4. Follow the steps in the wizard and select the file that contains the certificate that your root CA signed and provided.
5. Finish the setup.

Changing the Certificate Expiration Date

Certificates issued to the KM server for S/MIME users must be valid for at least two years. If the certificates have an expiration date that is less than two years from the date the certificate is issued, they do not function properly. To change the certificate expiration date, modify the registry values in the following registry location on the Windows 2000 Server CA that issues certificates to the KM server:

> **HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \CertSvc \Configuration*your_CA_name***

Where *your_CA_name* is the name of the Windows 2000 Server CA. The default settings are:

> **ValidityPeriod** REG_SZ = Years
>
> **ValidityPeriodUnits** REG_DWORD = 1

Change the **ValidityPeriodUnits** value to 2 or more on the CA that the legacy policy module is installed on, stop and restart the computer running Certificate Server, and then try to enable X.509 V3 certificates again on the KM server. This procedure is also documented in Microsoft Knowledge Base article Q242276.

Installing the Legacy Policy Module

The Expolicyw2k.dll File

You must register the Exchange Server policy module (the Expolicyw2k.dll file) with the Certificate Server to configure Exchange Server advanced security to use a Certificate Server. This process is also documented in Knowledge Base article Q192044.

Important After you register this policy module and restart the Certificate Services, that Certificate Server will only be able to issue and verify certificates for Exchange Server. If you need a Certificate Server that can issue and verify certificates other than Exchange Server certificates, you need to install another Certificate Server to perform that function.

Note You will not need the legacy policy module for Exchange 2000 Server KM server, because Exchange 2000 Server KM server will enable a single Certificate Server to serve multiple PKI services.

The Exchange Server policy module (Expolicy.dll) that is included with Exchange Server 5.5 does not support configurable (CDP) (Certificate Revocation List [CRL] Distribution Point) extensions in the KM server issued S/MIME certificates. For an updated Exchange Server KM server policy module for Windows 2000 Certificate Server that supports configurable CDP extensions, please contact Microsoft Product Support Services (PSS) and refer to Knowledge Base article Q264862.

1. The Expolicy.dll file is located on the Exchange Server 5.5 Service Pack 3 installation disk in the following folder:

   Server\Support\Kms\Expolicy\CPU_type

   Where *CPU_type* is the type of processor that the computer uses. To register this file:

   a. Copy the file to the following location on the CA:

      %systemroot%\System32

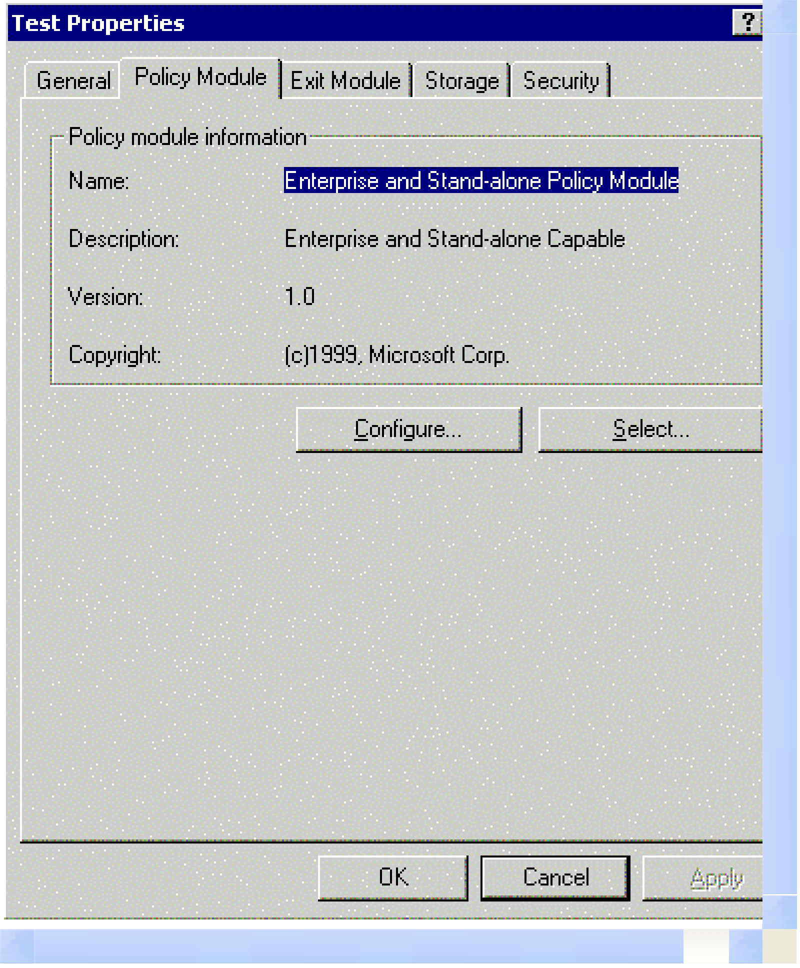
      For example, C:\Winnt\System32.

   b. At an MS-DOS command prompt on the Certificate Server, change to the %systemroot% folder, and then type the following:

      regsvr32 expolicy.dll

   Note You cannot register the policy module from CD-ROM or a mapped drive. Use only the Expolicy.dll file that is located on the Exchange Server 5.5 Service Pack 3 installation disk. The Expolicy.dll file that is located on the Exchange Server 5.5 Service Pack 1 installation disk is not the most recent version. For a newer version of the Exchange KM policy module that supports CDP extensions, please refer to Knowledge Base article Q264862.

2. Select the legacy policy module on the Windows 2000 Server CA. On the Windows 2000 Server CA, in Control Panel, double-click **Administrative Tools**, and then start the Certification Authority snap-in. Right-click the server to open its properties, and then click the **Policy Module** tab. When the following page is displayed, click **Select**.



Test Properties

Name: Enterprise and Stand-alone Policy Module

Description: Enterprise and Stand-alone Capable

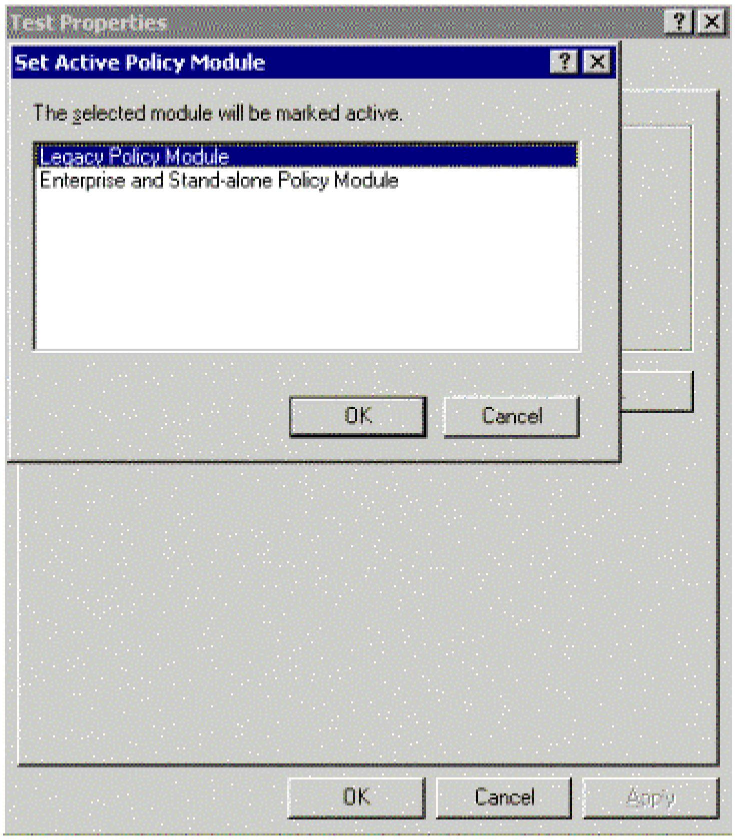
Version: 1.0

Copyright: (c)1999, Microsoft Corp.

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

3. When the **Set Active Policy Module** dialog box is displayed, click **Legacy Policy Module**, and then click **OK**.

   Note If the newer policy module that is described in Knowledge Base article Q264862 is installed, click **Exchange 5.5 Windows 2000 policy module** instead of **Legacy Policy Module**. If you click **Exchange 5.5 Windows 2000 policy module**, the administrator can configure CDP extensions for issued certificates, in a similar manner to the Enterprise and Stand-alone policy module.

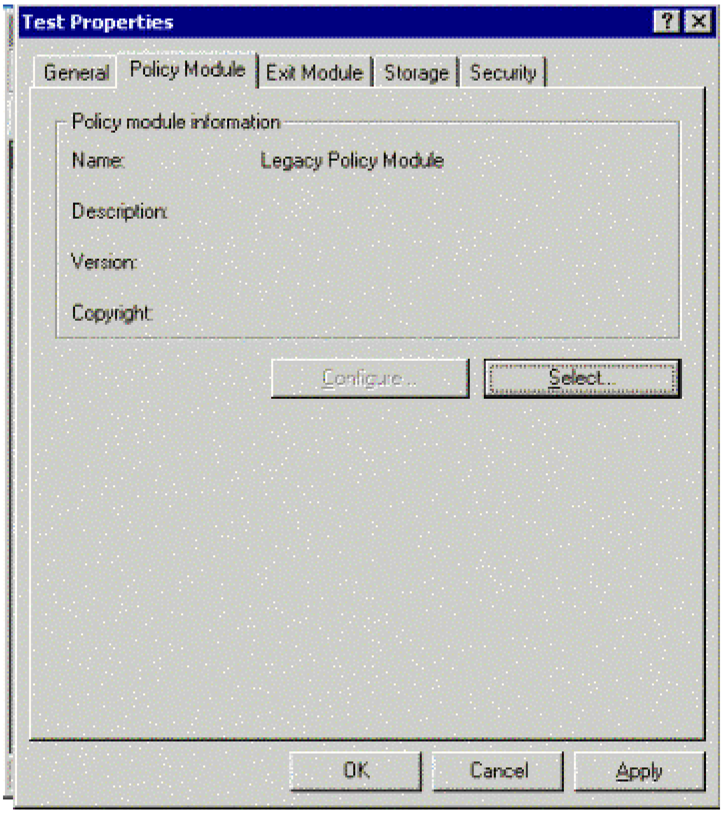


The selected module will be marked active.

Legacy Policy Module
Enterprise and Stand-alone Policy Module

4. Click either **OK** or **Apply**. The Certificate Services automatically restart and begin to use the legacy policy module.

   If you are installing Certificate Services on a remote server, you must install Certificate Services Web Enrollment Support on the Exchange Server 5.5 KM server. For more information, see the "KM Server Installation" section of this white paper.



Policy module information

Name: Legacy Policy Module

Description:

Version:

Copyright:

Scenarios

The Key Management server (KM server) that is included with Exchange Server 5.5 requires a Microsoft certification authority (CA) to issue X.509 V3 certificates. However, third-party root CAs can sign a Microsoft subordinate CA and exist in a public key infrastructure (PKI) hierarchy. This section describes some common scenarios and the key installation steps for each scenario.

Warning After a KM server is attached to a Microsoft Certificate Server, it cannot be attached to a new or different CA. If it is attached to a new or different CA, the root of trust is invalidated, and all mail encrypted with certificates issued from this root will be inaccessible.

Note The new policy module for Exchange Server 5.5 and Windows 2000 is Expolicyw2k.dll, which can only be used with a Windows 2000 CA.

Windows 2000 Server CA and KM Server on the Same Server with a Root Windows 2000 Server CA

1. Ensure that the Expolicyw2k.dll file is registered on the server.
2. Ensure that the Windows 2000 Server CA issues certificates that are valid for longer than two years.

Windows 2000 Server CA and KM Server on the Same Server with a Subordinate Windows 2000 Server CA

1. Ensure that the Expolicyw2k.dll file is registered on the server.
2. Install the root CA certificate in the local machine store on the server.
3. Ensure that the subordinate Windows 2000 Server CA issues certificates that are valid for longer than two years.
4. Ensure that the root Windows 2000 Server CA issues certificates that have an expiration date that is later than the expiration date for the subordinate CA.

Windows 2000 Server CA and KM Server on the Same Server with a Subordinate Windows 2000 Server CA Using a Third-Party Root CA

1. Ensure that the Expolicyw2k.dll file is registered on the server.
2. Install the root CA certificate in the local machine store on the server.
3. Ensure that the root CA issuer and subject names are identical.
4. Ensure that the subordinate Windows 2000 Server CA issues certificates that are valid for longer than two years.
5. Ensure that the root CA issues certificates that have an expiration date that is later than the expiration date for the Windows 2000 Server subordinate CA.

Windows 2000 Server CA and KM Server on Separate Servers with a Root Windows 2000 Server CA in the Same Domain

1. Ensure that the Expolicyw2k.dll file is registered on the Windows 2000 Server CA.
2. Install Certificate Services Web Enrollment Support on the KM server.
3. Verify that the **Configuration Directory** registry key is set properly. Refer to the "KM Server Cannot Find the Windows 2000 Server CA" section of this white paper.
4. Ensure that the root Windows 2000 Server CA issues certificates that have an expiration date that is later than two years from the date the certificate is issued.

Windows 2000 Server CA and KM Server on Separate Servers with a Root Windows 2000 Server CA in a Different Domain

1. Ensure that the involved domains are trusted in both directions.
2. Ensure that the Expolicyw2k.dll file is registered on the Windows 2000 Server CA.
3. Install Certificate Services Web Enrollment Support on the KM server.
4. Install the fix that is described in Knowledge Base article Q262288 on the KM server.
5. Verify that the **Configuration Directory** registry key is set properly. Refer to the "KM Server Cannot Find the Windows 2000 Server CA" section of this white paper.
6. Ensure that the root Windows 2000 Server CA issues certificates that have an expiration date that is later than two years from the date the certificate is issued.
7. Add the KM server administrator accounts with "manage" permissions to the CA security settings.

Windows 2000 Server CA and KM Server on Separate Servers with a Subordinate Windows 2000 Server CA in the Same Domain

1. Ensure that the Expolicyw2k.dll file is registered on the Windows 2000 Server CA.
2. Install the root CA certificate in the local machine store on the KM server.
3. Install Certificate Services Web Enrollment Support on the KM server.
4. Verify that the **Configuration Directory** registry key is set properly. Refer to the "KM Server Cannot Find the Windows 2000 Server CA" section of this white paper.

5. Ensure that the subordinate Windows 2000 Server CA issues certificates that are valid for longer than two years.
6. Ensure that the root Windows 2000 Server CA issues certificates that have an expiration date that is later than the expiration date for the subordinate CA.

Windows 2000 Server CA and KM Server on Separate Servers with a Subordinate Windows 2000 Server CA in a Different Domain

1. Ensure that the Expolicyw2k.dll file is registered on the Windows 2000 Server CA.
2. Install the root CA certificate in the local machine store on the KM server.
3. Install Certificate Services Web Enrollment Support on the KM server.
4. Install the fix that is described in Knowledge Base article Q262288 on the KM server
5. Verify that the **Configuration Directory** registry key is set properly. Refer to the "KM Server Cannot Find the Windows 2000 Server CA" section of this white paper.
6. Ensure that the subordinate Windows 2000 Server CA issues certificates that are valid for longer than two years.
7. Ensure that the root Windows 2000 Server CA issues certificates that have an expiration date that is later than the expiration date for the subordinate CA.
8. Add the KM server administrator accounts with "manage" permissions to the CA security settings.

Windows 2000 Server CA and KM Server on Separate Servers with a Subordinate Windows 2000 Server CA Using a Third-Party Root CA

1. Ensure that the Expolicyw2k.dll file is registered on the Windows 2000 Server CA.
2. Install the root CA certificate in the local machine store on the KM server.
3. Install Certificate Services Web Enrollment Support on the KM server.
4. Ensure that the subordinate Windows 2000 Server CA issues certificates that are valid for longer than two years.
5. Ensure that the root CA issue certificates that have an expiration date that is later than the expiration date for the Windows 2000 Server subordinate CA.

Upgrading Windows NT 4.0 Certificate Server to Windows 2000 Server

You can easily upgrade a computer running Windows NT 4.0 Certificate Server (installed with the Windows NT 4.0 Option Pack) to Windows 2000 Server, if it is not in a hierarchy and is installed on an existing Exchange Server 5.5 KM server. If the computer running Windows NT 4.0 Certificate Server already issues certificates to Exchange Server KM server, the Certificate Server database is converted during the upgrade, and no further actions are required.

Important Install Certificate Services Web Enrollment Support on the computer running Windows NT Server 4.0 before you upgrade to Windows 2000 Server.

Installing Trusted Root Certification Authorities

This section provides detailed steps to install trusted root certification authorities (CAs) to the local information store of a computer running Windows 2000 Server and Exchange Server 5.5 Key Management server (KM server). KM server requires that the root certificate of a third-party or foreign CA be included as a trusted root certification authority in the information store of the computer that KM server is installed on.

Note All client computers must also have the root CA certificate installed in the information store or browser to use X.509 V3 certificates in a public key infrastructure (PKI) hierarchy. You can perform the following steps to deploy a root certificate to a client computer, or you can use Group Policy to deploy trusted root certification authorities to Windows 2000 Server computers in a Windows 2000 Server domain.

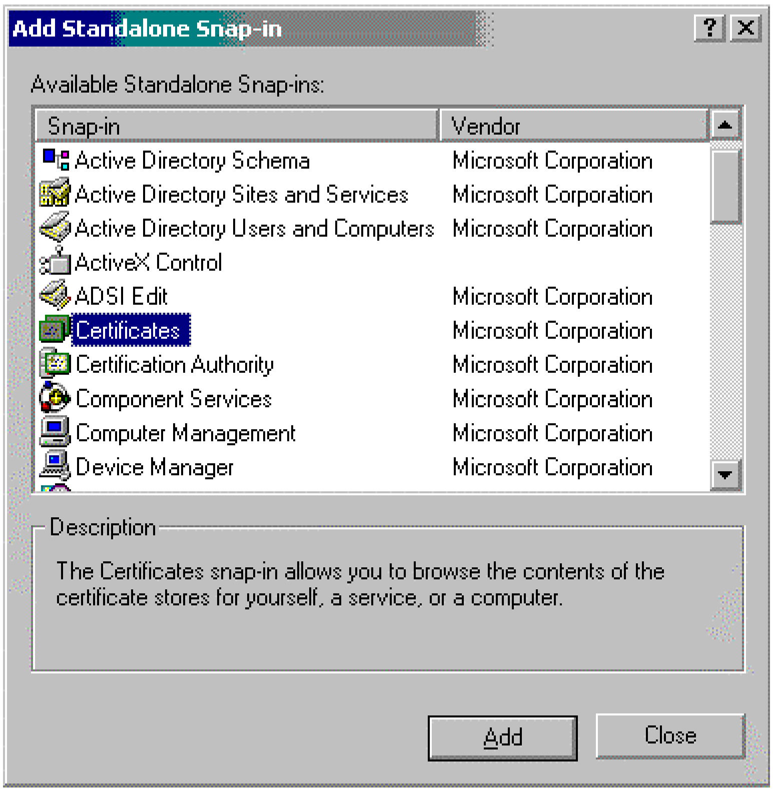
Installing a Root Certificate

On the local computer on which KM server is installed, open the Certificates snap-in:

a. Click the **Start** button, click **Run**, and then type **mmc.exe** to start Microsoft Management Console (MMC).

b. Click **Console**, click **Add/Remove Snap-in**, and then click **Add**.

c. When the **Add Standalone Snap-in** dialog box is displayed, click **Certificates**, click **Add**, and then click **Close**.



Add Standalone Snap-in

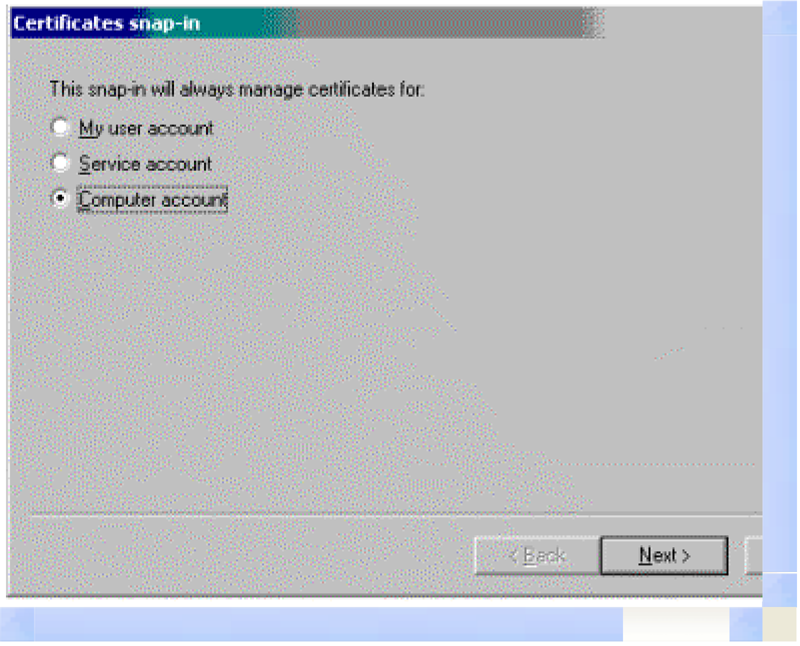
Available Standalone Snap-ins:

Snap-in	Vendor
Active Directory Schema	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Computers	Microsoft Corporation
ActiveX Control	
ADSI Edit	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation

Description

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

1. The snap-in prompts you to provide a user account, service account, or computer account. Click **Computer account**, and then click **Next**.



Certificates snap-in

This snap-in will always manage certificates for:

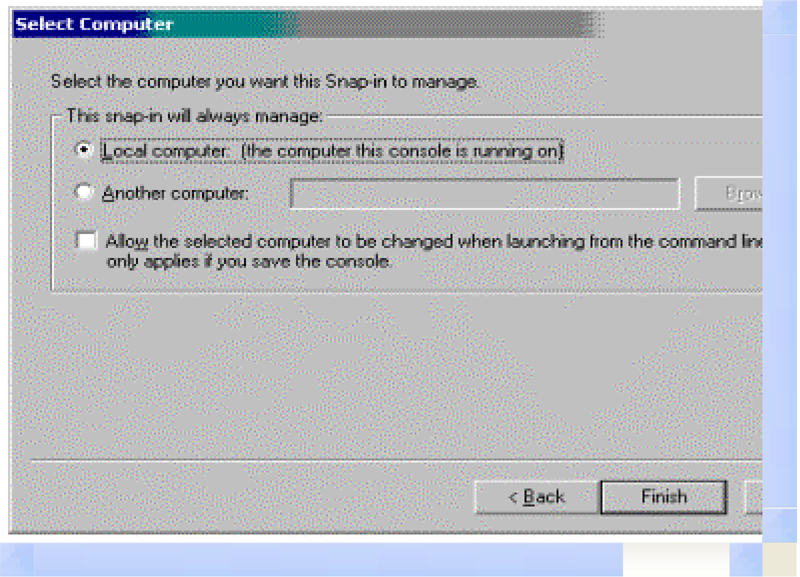
○ My user account

○ Service account

● Computer account

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

2. When the **Select Computer** dialog box is displayed, assuming that you are running the wizard on the local computer, click **Local computer**, and then click **Finish**.



Select Computer

Select the computer you want this Snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

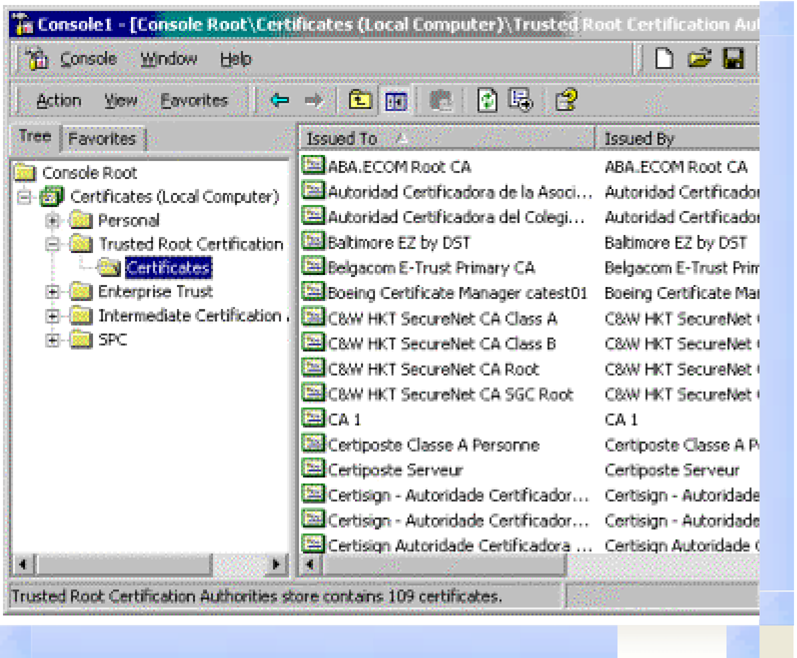
○ Another computer:

□ Allow the selected computer to be changed when launching from the command lin only applies if you save the console.

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

3. The snap-in dialog box is displayed again. Click **Close**, and then click **OK**. The snap-in is ready to import a root certificate.

4. In the following window, in the left pane, click to expand the **Certificates (Local Computer)** folder, click to expand the **Trusted Root Certification Authorities** folder, right-click the **Certificates** folder, and then click **All Tasks...Import** to start the Certificate Import Wizard.

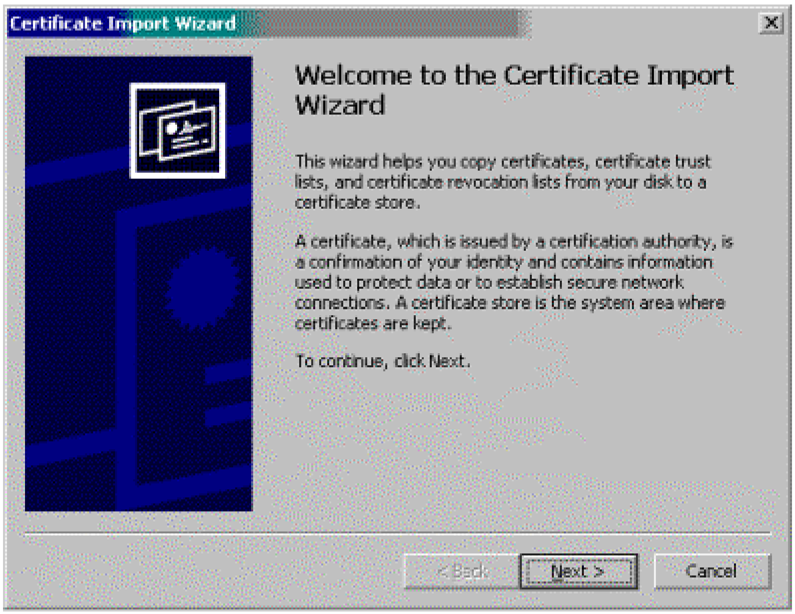

Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Au
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
SPC

Issued To	Issued By
ABA.ECOM Root CA	ABA.ECOM Root CA
Autoridad Certificadora de la Asoci...	Autoridad Certificado
Autoridad Certificadora del Colegi...	Autoridad Certificado
Baltimore EZ by DST	Baltimore EZ by DST
Belgacom E-Trust Primary CA	Belgacom E-Trust Prim
Boeing Certificate Manager catest01	Boeing Certificate Ma
C&W HKT SecureNet CA Class A	C&W HKT SecureNet
C&W HKT SecureNet CA Class B	C&W HKT SecureNet
C&W HKT SecureNet CA Root	C&W HKT SecureNet
C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet
CA 1	CA 1
Certiposte Classe A Personne	Certiposte Classe A P
Certiposte Serveur	Certiposte Serveur
Certisign - Autoridade Certificador...	Certisign - Autoridade
Certisign - Autoridade Certificador...	Certisign - Autoridade
Certisign Autoridade Certificadora ...	Certisign Autoridade

Trusted Root Certification Authorities store contains 109 certificates.

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

5. When the **Certificate Import Wizard** dialog box is displayed, click **Next**.



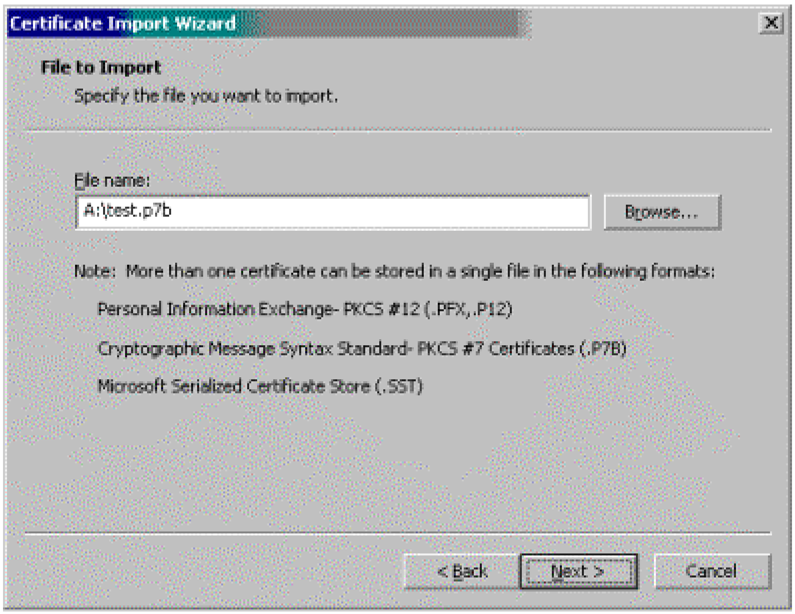
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

6. When the **File to Import** dialog box is displayed, click **Browse** to browse for the file name of the file that you want to import. The file type should be PKCS #12 (*.pfx) or PKCS #7 (*.p7b). Click **Next**.



File to Import

Specify the file you want to import.

File name:

A:\test.p7b

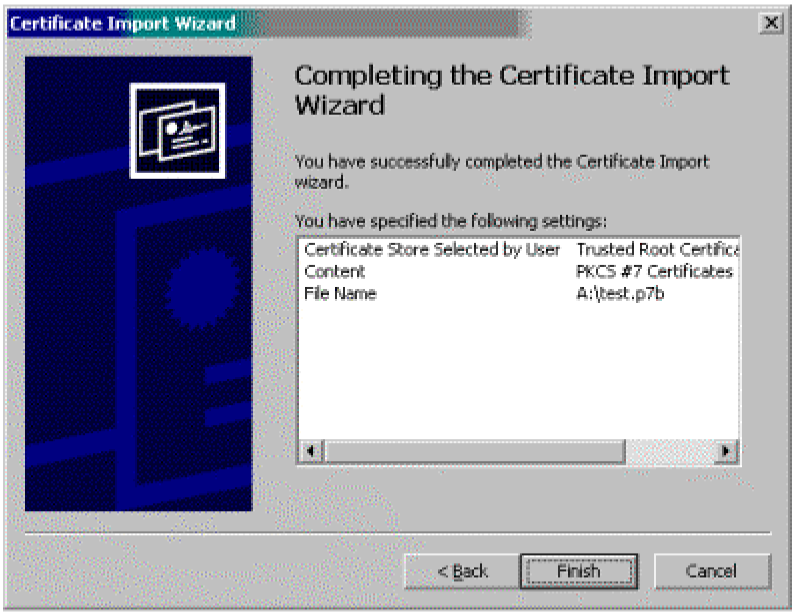
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

7. The file is imported and the following dialog box is displayed. To finish the Certificate Import Wizard, click **Finish**.



Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	PKCS #7 Certificates
File Name	A:\test.p7b

A message is displayed that says, "The import was successful." Click **OK**.

KM Server Configuration

Exchange Server 5.5 Service Pack 3 must be installed, and Key Management server (KM server) must be installed and functional, to perform the procedures in this white paper. Perform the following steps in this section of this white paper to configure KM server to issue X.509 V3 certificates.

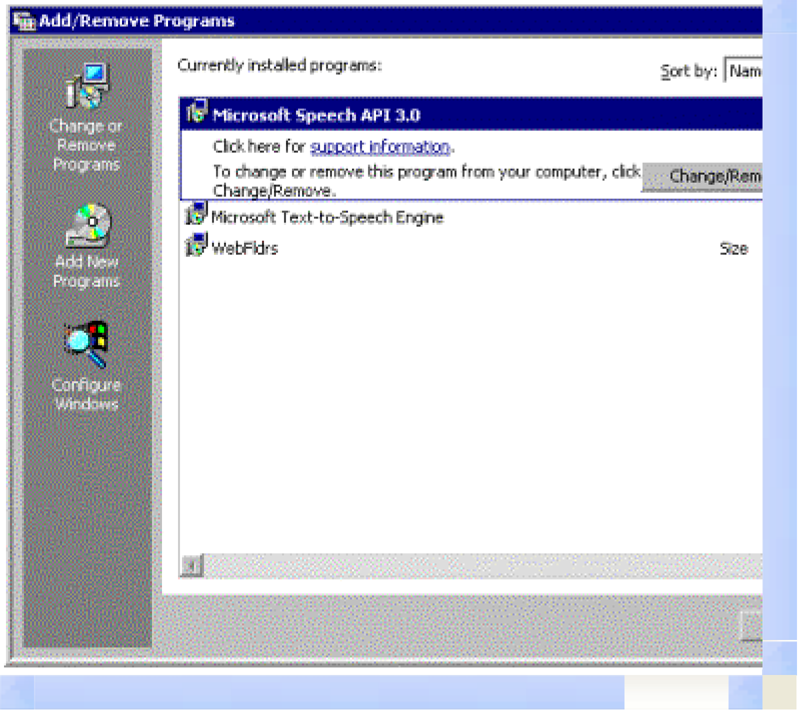
Installing Certificate Services Web Enrollment Support on KM Server

To install KM server, you must install the Windows 2000 Server Certification Authority (CA) Web Enrollment Support before you enable X.509 V3 certificates to be issued.

Note You only need to install the Certificate Services Web Enrollment Support on the KM server if Certificate Server is not installed on the same computer that KM server is installed on.

To install Web Enrollment Support on the KM server:

1. Click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**. When an **Add/Remove Programs** dialog box similar to the following is displayed, click **Configure Windows**.



Add/Remove Programs

Currently installed programs:

Sort by: Nam

Microsoft Speech API 3.0

Click here for support information.

To change or remove this program from your computer, click Change/Remove.

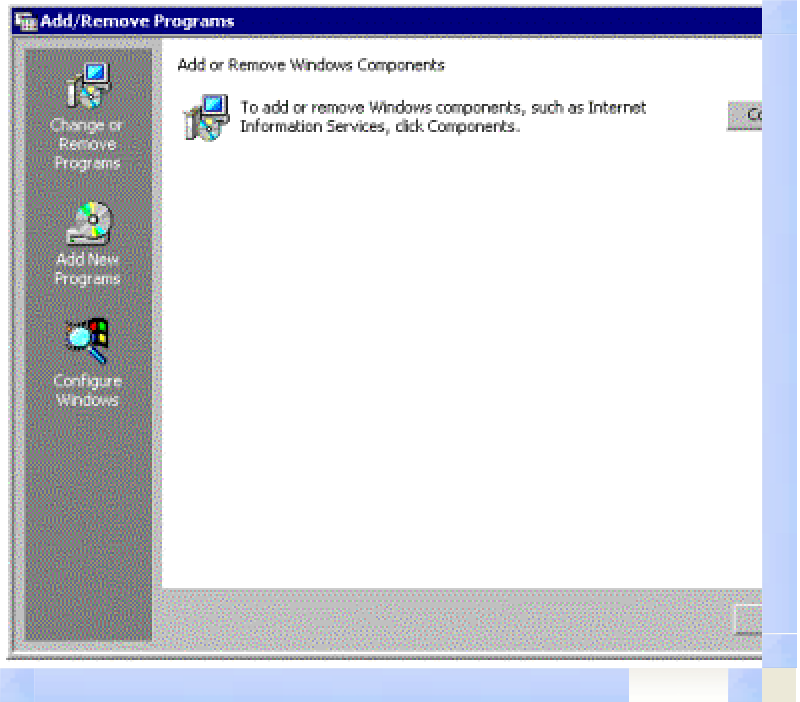
Microsoft Text-to-Speech Engine

WebFldrs

Size

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

3. When the **Add or Remove Windows Components** dialog box is displayed, click **Components**.



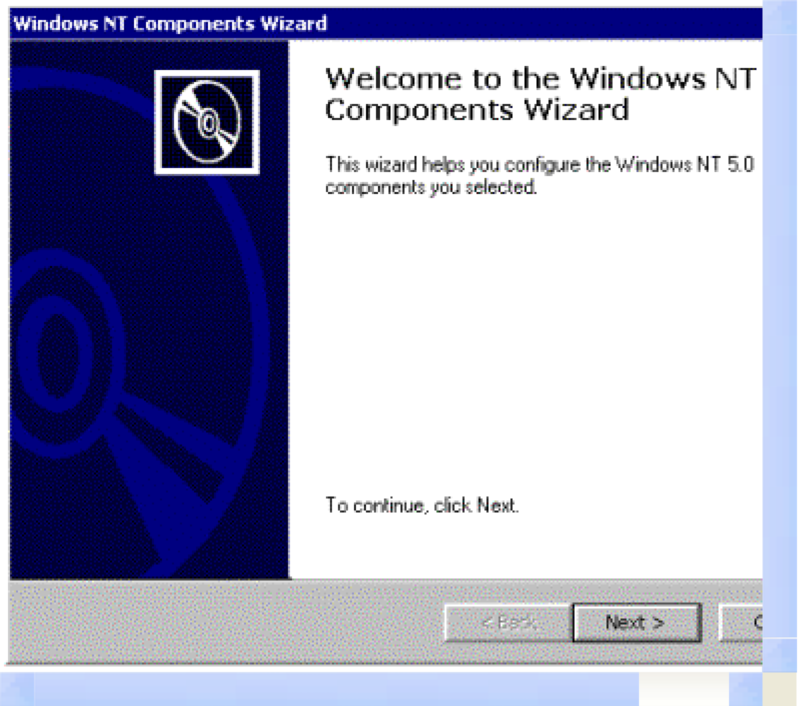
Add/Remove Programs

Add or Remove Windows Components

To add or remove Windows components, such as Internet Information Services, click Components.

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

4. When a dialog box similar to the following is displayed, click **Next**.



Windows NT Components Wizard

Welcome to the Windows NT Components Wizard

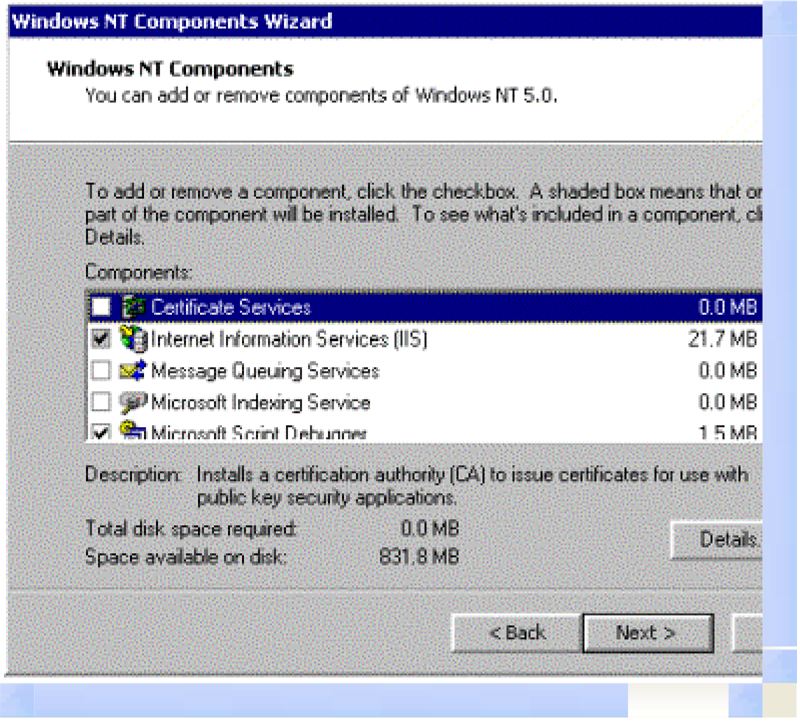
This wizard helps you configure the Windows NT 5.0 components you selected.

To continue, click Next.

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

5. When the **Windows NT Components** dialog box is displayed, click to select the **Certificate Services** check box, and then click **Details**.

   Note If you want to use the Web components of the Certificate Services, you must also click to select the **Internet Information Services (IIS)** check box.



Windows NT Components Wizard

Windows NT Components
You can add or remove components of Windows NT 5.0.

To add or remove a component, click the checkbox. A shaded box means that or part of the component will be installed. To see what's included in a component, cl Details.

Components:

□	Certificate Services	0.0 MB
☑	Internet Information Services (IIS)	21.7 MB
□	Message Queuing Services	0.0 MB
□	Microsoft Indexing Service	0.0 MB
☑	Microsoft Script Debugger	1.5 MB

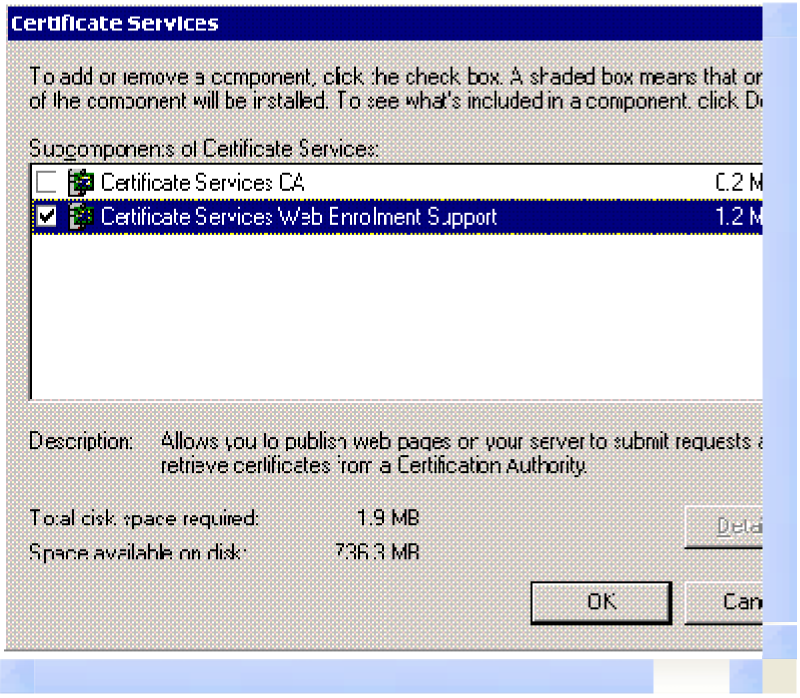
Description: Installs a certification authority (CA) to issue certificates for use with public key security applications.

Total disk space required: 0.0 MB
Space available on disk: 831.8 MB

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

6. Click to select the **Certificate Services Web Enrollment Support** check box. This allows your KM server to communicate with the certificate server.

Click **OK.**



Certificate Services

To add or remove a component, click the check box. A shaded box means that or
of the component will be installed. To see what's included in a component, click D

Subcomponents of Certificate Services:

- ☐ Certificate Services CA 0.2 M
- ☑ Certificate Services Web Enrolment Support 1.2 M

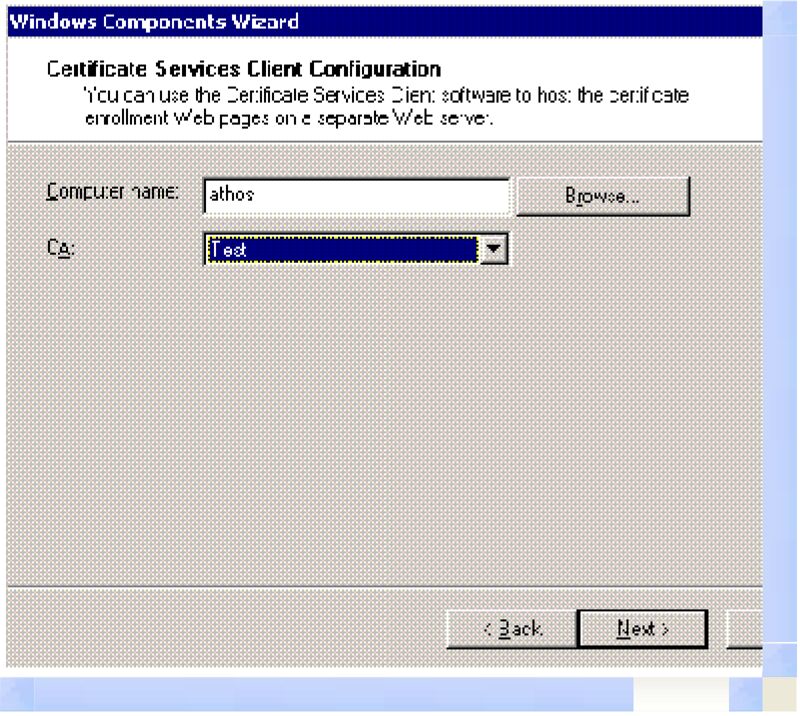
Description: Allows you to publish web pages on your server to submit requests a
retrieve certificates from a Certification Authority.

Total disk space required: 1.9 MB

Space available on disk: 736.3 MB

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

7. When the **Certificate Services Client Configuration** dialog box is displayed, in the **Computer name** box, type the name of the remote Certificate Server, and then press the **ENTER** key. A list of available CAs is displayed. Click **Next**.



Windows Components Wizard

Certificate Services Client Configuration

You can use the Certificate Services Client software to host the certificate enrollment Web pages on a separate Web server.

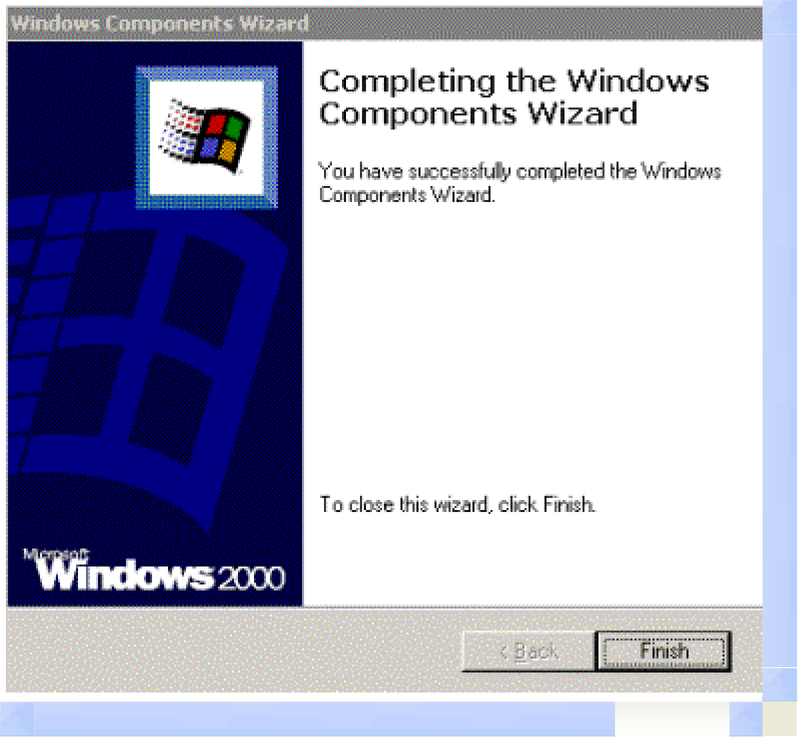
Computer name: athos

CA: Test

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

8. When a dialog box that asks if you want to stop the Internet Information Services is displayed, click **OK**.

9. After Internet Information Services stop and restart, the following dialog box is displayed. Click **Finish**.



Windows Components Wizard

Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

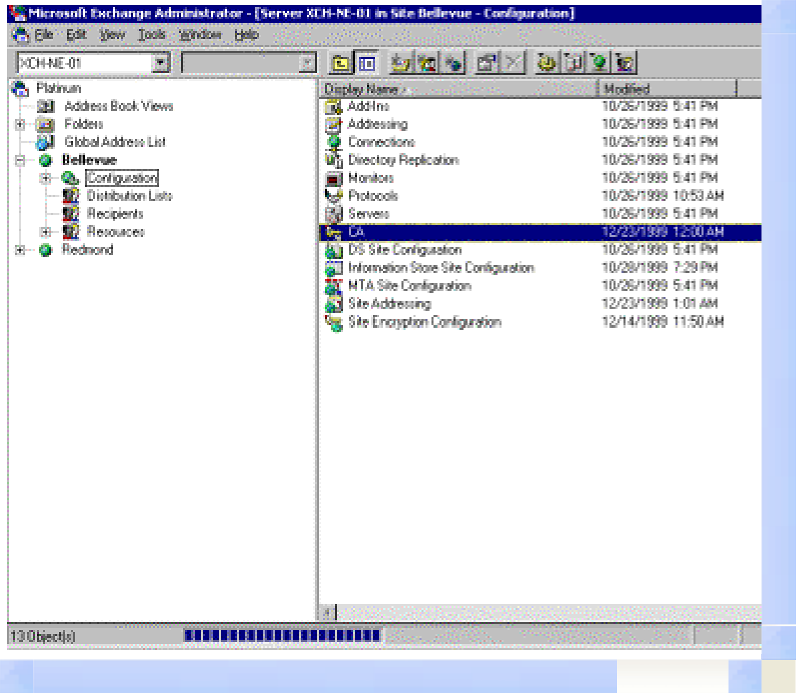
If your browser does not support inline frames, click here to view on a separate page.

Enabling X.509 V3 Certificates on the KM Server

After you install Certificate Services Web Enrollment Support on an Exchange Server 5.5 KM server, perform the following steps to enable X.509 V3 certificates in KM server:

Note If the Exchange Server KM server resides in a Windows NT Server 4.0 domain, you must install a fix to enable communications with a Windows 2000 CA. Please refer to Knowledge Base article Q262288 for additional information.

1. Start the Microsoft Exchange Administrator program, and under the site that the KM server is in, click the **Configuration** container, and then double-click **CA**.

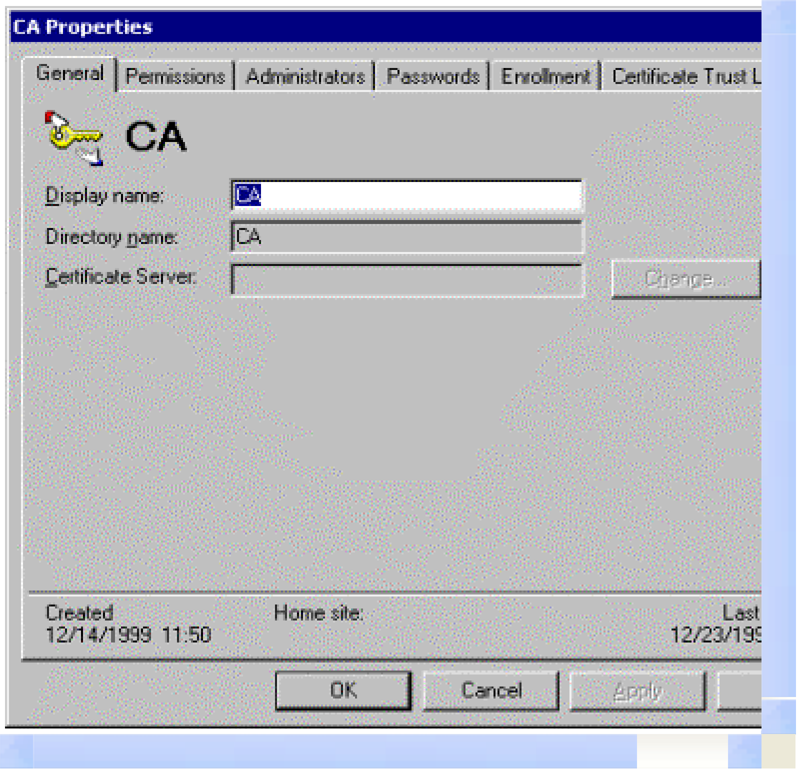

Microsoft Exchange Administrator - [Server XCH-NE-01 in Site Bellevue - Configuration]
File Edit View Tools Window Help
XCH-NE-01
13 Object(s)

Platinum
Address Book Views
Folders
Global Address List
Bellevue
Configuration
Distribution Lists
Recipients
Resources
Redmond

Display Name	Modified
Add-Ins	10/26/1999 5:41 PM
Addressing	10/26/1999 5:41 PM
Connections	10/26/1999 5:41 PM
Directory Replication	10/26/1999 5:41 PM
Monitors	10/26/1999 5:41 PM
Protocols	10/26/1999 10:53 AM
Servers	10/26/1999 5:41 PM
CA	12/23/1999 12:00 AM
DS Site Configuration	10/26/1999 5:41 PM
Information Store Site Configuration	10/28/1999 7:29 PM
MTA Site Configuration	10/26/1999 5:41 PM
Site Addressing	12/23/1999 1:01 AM
Site Encryption Configuration	12/14/1999 11:50 AM

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

2. KM server prompts you to provide the KM server password, which is "password" (without the quotation marks), if the password has not been changed after installation. When the following **CA properties** dialog box is displayed, click the **Enrollment** tab.



Display name: CA
Directory name: CA
Certificate Server:

Created
12/14/1999 11:50

Home site:

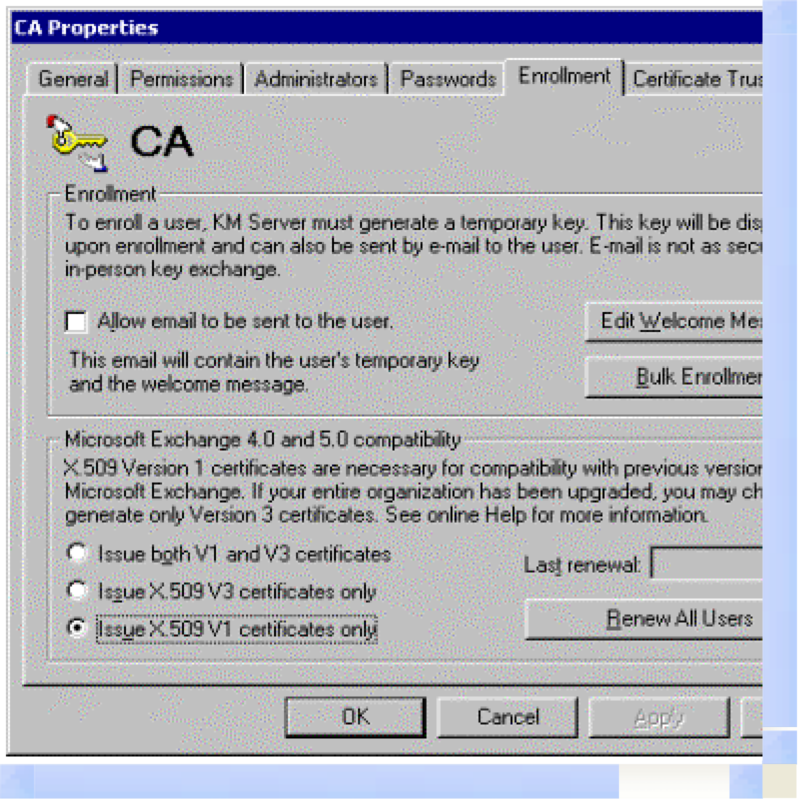
Last
12/23/199

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

3. On the **Enrollment** tab, click either **Issue both V1 and V3 certificates** or **Issue X.509 V3 certificates only,** as applicable.

Warning If your Exchange Server organization uses legacy clients (Outlook

97 or earlier), *do not* select **Issue X.509 V3 certificates only**. After you select **Issue *X*.509 V3 certificates only**, those clients are not able to use Exchange Server advanced security, which includes decrypting previously encrypted e-mail.



Enrollment

To enroll a user, KM Server must generate a temporary key. This key will be dis upon enrollment and can also be sent by e-mail to the user. E-mail is not as secu in-person key exchange.

□ Allow email to be sent to the user.

This email will contain the user's temporary key and the welcome message.

Microsoft Exchange 4.0 and 5.0 compatibility

X.509 Version 1 certificates are necessary for compatibility with previous versior Microsoft Exchange. If your entire organization has been upgraded, you may ch generate only Version 3 certificates. See online Help for more information.

○ Issue both V1 and V3 certificates

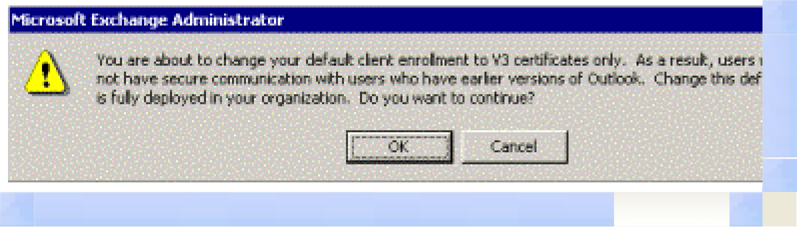
○ Issue X.509 V3 certificates only

● Issue X.509 V1 certificates only

Last renewal:

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

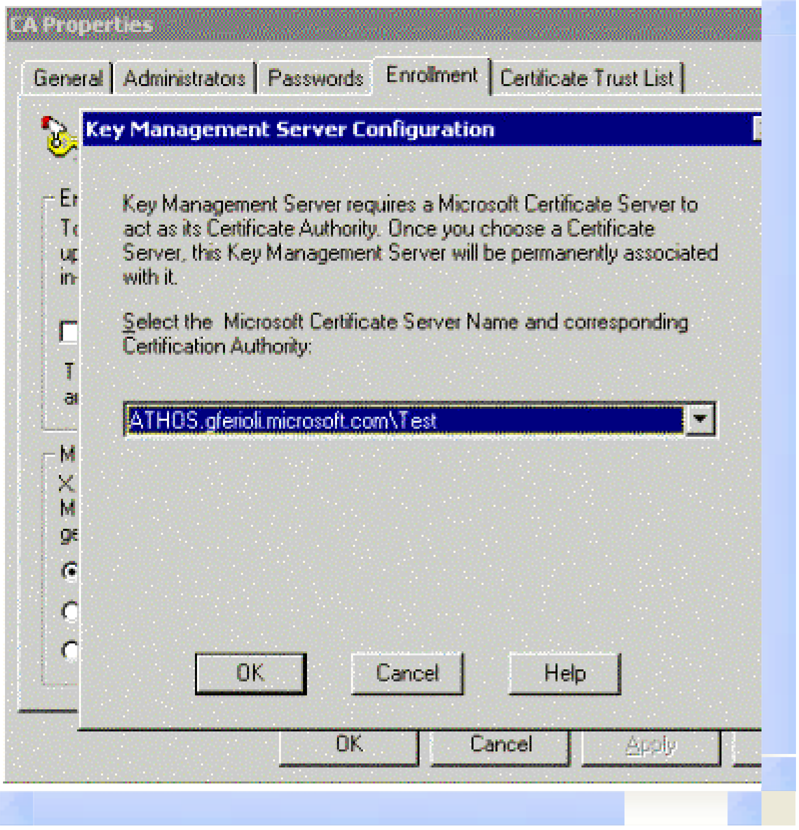
4. If you click **Issue X.509 V3 certificates only**, the following warning message is displayed. To continue, click **OK**.



You are about to change your default client enrolment to V3 certificates only. As a result, users not have secure communication with users who have earlier versions of Outlook. Change this def is fully deployed in your organization. Do you want to continue?

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

5. The **Key Management Server Configuration** dialog box lists all of the available Certificate Servers in the enterprise. Click the correct server, and then click **OK**.


CA Properties

Key Management Server Configuration

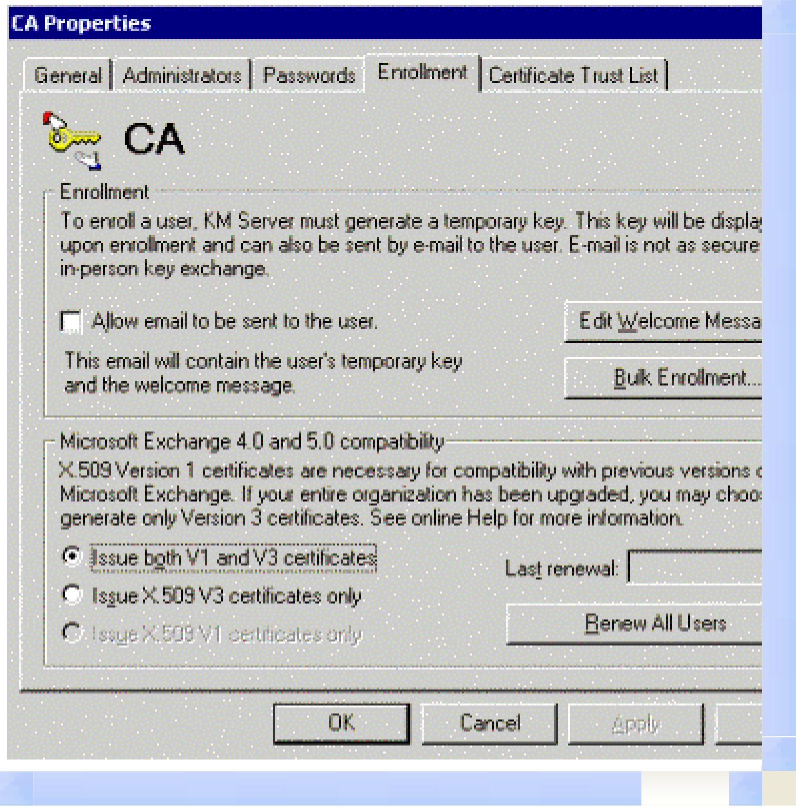
Key Management Server requires a Microsoft Certificate Server to act as its Certificate Authority. Once you choose a Certificate Server, this Key Management Server will be permanently associated with it.

Select the Microsoft Certificate Server Name and corresponding Certification Authority:

ATHOS.gferioli.microsoft.com\Test

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

KM server is now ready to issue X.509 V3 certificates.


CA Properties

Enrollment

To enroll a user, KM Server must generate a temporary key. This key will be displa upon enrollment and can also be sent by e-mail to the user. E-mail is not as secure in-person key exchange.

□ Allow email to be sent to the user.

This email will contain the user's temporary key and the welcome message.

Microsoft Exchange 4.0 and 5.0 compatibility

X.509 Version 1 certificates are necessary for compatibility with previous versions o Microsoft Exchange. If your entire organization has been upgraded, you may choo generate only Version 3 certificates. See online Help for more information.

● Issue both V1 and V3 certificates

○ Issue X.509 V3 certificates only

○ Issue X.509 V1 certificates only

Last renewal:

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

Troubleshooting

If you want to use 128-bit Secure/Multipurpose Internet Mail Extensions (S/MIME) security with Exchange Server 5.5 Key Management server (KM server), you must perform a number of key steps properly. This section provides troubleshooting steps that you can perform if you experience problems.

Installing KM Server and Windows 2000 CA in a Windows NT Server 4.0 Resource Domain

To operate the KM server and the Windows 2000 CA in an existing Windows NT Server 4.0 domain, you need to apply a fix to the KM server to enable Windows NT Server 4.0 domain support. Please see Knowledge Base article Q262288 for information on how to obtain this fix and apply it to the KM server.

Note Windows 2000 mixed mode domains do not require this fix.

KM Server Cannot Find the Windows 2000 Server CA

A common problem that you may experience if you enable X.509 V3 certificates with Exchange Server 5.5 KM server is a KM server that does not detect the Windows 2000 Server certification authority (CA). (For more information, see the "Enabling X.509 V3 Certificates on the KM Server" section of this white paper.) This problem may be caused by one of the following conditions:

- Certificate Services Web Enrollment Support is not installed on the KM server.
- The Expolicy.dll or Expolicyw2k.dll file is not registered on the Windows 2000 Server CA.
- The Windows 2000 Server CA was incorrectly installed as an enterprise CA.
- The Windows 2000 Server CA was installed by using an account that does not have directory service write access or Domain Administrator privileges.

Note If the Windows 2000 Server CA was installed with a shared configuration folder on a separate server (for more information, see the "Certification Authority Setup" section of this white paper), KM server must maintain a mapped drive connection to that location.

Windows 2000 KM Server in Windows NT Server 4.0 Domain Does Not Find Web Client

When you install the CA and KM server in a Windows NT Server 4.0 domain, the Certificate Services Web Enrollment Support client must be able to find the shared CA folder on the CA. If you receive an error message (ID number c1031dab) that states that a certificate services Web client is not installed when the KM server enables a V3 certificate, ensure that the following registry key is present on the KM server:

> **HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \CertSvc \Configuration**

The default settings are:

> **ConfigurationDirectory** REG_SZ = \\*CA_name**shared_folder*

Where *CA_name* is the name of the Windows 2000 Server CA and *shared_folder* is the name of the CA configuration folder.

Restart the KM Server service after you edit this registry key.

Hierarchy Is Invalid Error Message

The following error message may be displayed:

The hierarchy of the MS Certificate Servers for your KM server is invalid. ID# c1031daf.

This error message may be caused by one of the following issues:

- The certificate has an invalid expiration date. The certificates that are issued by the CA to the KM server for S/MIME users are only valid for one year. The certificates issued to the KM server for S/MIME users must be valid for at least two years. For more information about how to correct the expiration date, see the "Changing the Certificate Expiration Date" section of this white paper.
- KM server links certificates by name only. For every certificate in the hierarchy, the subject-issuer pairs must match. This problem occurs almost exclusively when KM server issues a CA hierarchy with a third-party root CA. If the subject and issuer names are not identical on the root certificate, this error message is displayed when KM server attempts to validate the certificate chain.

Removing Advanced Security from a Mailbox Results in Error Message "The Operation Could Not Be Completed" c1031d92

This error message occurs if the KM server administrator account that is used to remove the advanced security from a mailbox has no "manage" permissions on the related CA server. Add the list of KM server administrators to the CA's **Security** tab, and grant the KM server administrators manage permissions.

KM Server Reports c1031d9f

This error message occurs if the CA server is running in a domain that is different from the domain of the KM server and the fix that is described in Knowledge Base article Q262288 is not applied on the Windows 2000 server where Exchange Server 5.5 KM server is running. To resolve this problem, install the fix that is described in Q262288.

The KM Server Certificate Is Immediately Revoked by the CA

The CA may immediately revoke the KM server certificate; this is not an error it is a normal procedure that the KM server performs in conjunction with the issuing CA to ensure that the KM server can build and validate the certificate chain. Client e-mail certificates are issued properly, even if the CA immediately revokes the KM server certificate.

KM Server Forklift Upgrade Process

If you want a Windows 2000 Server Certificate Server to issue X.509 V3 certificates to a computer running Windows 2000 Server and Exchange Server 5.5 Service Pack 3 KM server, you may need to upgrade from an existing Windows NT Server 4.0 environment. One method to migrate the Exchange Server 5.5 KM server database from Windows NT Server 4.0 to Windows 2000 Server is to perform a "forklift upgrade." To perform a forklift upgrade, you copy the KM server database and log files from the computer running Windows NT Server 4.0 and Exchange Server 5.5 KM server, to a computer running Windows 2000 Server and Exchange Server 5.5 Service Pack 3 KM server. The computer running Windows 2000 Server and Exchange Server 5.5 Service Pack 3 KM server must have the same host name as the computer running Windows NT

Server 4.0 and Exchange Server 5.5 KM server. To perform a forklift upgrade:

1. Set up Windows 2000 Server on the target computer. Make sure that you set up the computer running Windows 2000 Server by using the same host and machine name as the computer running Windows NT Server 4.0 and Exchange Server 5.5 KM server. The server should be disconnected from the network at this point.
2. Stop the Exchange Server services, such as the Information Store and the MTA, on the computer that is running Windows NT Server 4.0 and Exchange Server.
3. Disconnect the computer running Windows NT Server 4.0 and Exchange Server 5.5 KM server from the network.

   Copy the KM server database and log files from the computer running Windows NT Server 4.0 and Exchange Server 5.5 KM server to a shared network drive. For example, the following files are considered KM server database and log files:

   - KM server database and log files
   - Information store database and log files
   - Directory database and log files
4. Delete the Windows NT Server 4.0 KM server machine account from the domain.
5. Connect the computer running Windows 2000 Server to the subnet in which it will reside.
6. Set up Exchange Server 5.5 with KM server on the computer running Windows 2000 Server that you set up in step 1.
7. Add the computer running Windows 2000 Server and Exchange Server 5.5 KM server to the same Exchange Server site that the computer running Windows NT Server 4.0 and Exchange Server 5.5 KM sever was a member of.
8. Set up Exchange Server 5.5 Service Pack 3 on the computer running Windows 2000 Server and Exchange Server 5.5 KM server.
9. Shut down all of the Exchange Server services on the computer running Windows 2000 Server and Exchange Server 5.5 KM server.

   Note Make sure that you record the KM server startup password before you shut down the Exchange Server services, because you need to use the same password on the computer that is running Windows 2000 Server.
10. Remove the KM server database and log files from the computer running Windows 2000 Server and Exchange Server 5.5 KM server.
11. Copy the KM server database and log files (originally from the computer running Windows NT Server 4.0 and Exchange Server 5.5 KM server) from the shared network drive that you copied them to in step 3, to the computer running Windows 2000 Server and Exchange Server 5.5 KM server.
12. Start all of the Exchange Server services on the computer running Windows 2000 Server and Exchange Server 5.5 KM server.

After you complete these steps, the Exchange Server 5.5 KM server database is migrated from the computer running Windows NT Server 4.0 to the computer running Windows 2000 Server and Exchange Server 5.5 Service Pack 3 KM server.

Exchange 2000 Server

At the time that this white paper was written, Microsoft Exchange 2000 Server had not been released. This section contains information about the planned new features of Key Management server (KM server) in Exchange 2000 Server.

KM Server Key Export and Import

Exchange 2000 Server incorporates a key export and import feature that enhances the organizational flexibility of sites that use advanced security, by allowing them to migrate users' key history to a new location. After the key history is migrated to the new location, those users can access their old keys, and therefore can read e-mail that was encrypted in the old location.

KM server archives and stores keys so that they can be recovered at a later time. This allows users to recover valuable encrypted e-mail even if they lose their keys. KM server keeps these key histories in a database and maps them to a specific mailbox by Distinguished Name (DN). Currently, if a user moves to a new organization or site, this key history is lost. To remedy this situation, the user must decrypt all of his or her e-mail with the Sectool tool (included with the Microsoft Exchange Server Resource Kit), re-enroll after the move to the new organization or site, and then re-encrypt the e-mail with a new key. In Exchange 2000 Server, You can bulk export keys to a file that can be imported by another KM server. After you import the file, the user can access the old keys and decrypt the old e-mail. This feature vastly improves organizational flexibility for companies that have implemented advanced security.

Backing Up KM Server and Certificate Server

The KM server database in Exchange Server 5.5 is not included in the Exchange Server panel in Windows NT Backup. To back up the KM server database, an administrator has to stop the service and perform the backup manually. In Exchange 2000 Server, the KM server database has been added to the Exchange Server panel of Windows NT Backup to allow automatic backup without service interruption. The ESE97 application programming interface (API) and Jet database engine provide the ability to back up online databases.

Important Back up the Certificate Server and KM server at the same time, because both the Certificate Server and KM server maintain the revocation status of the certificates. When a certificate is revoked, it is marked as revoked in the KM server and the Certificate Server. For example, if a KM server backup is performed before a revocation, a Certificate Server backup is performed after the revocation. Both are then restored, and the certificate is marked revoked in the KM server, but not in the Certificate Server. New Certification Revocation Lists (CRLs) published by the Certificate Server would not contain the certificate, and there would be no way to revoke them again in KM server.

Multipurpose Certificate Servers

The removal of the policy module (the Expolicy.dll file) from Exchange 2000 Server allows a Certificate Server to issue certificates to KM server users, as well as other certificates for other purposes, by using the enterprise version of Certificate Server templates. The templates define the extensions that appear in the certificate. KM server users need two templates, which are included with Windows 2000 Server. Public key infrastructure (PKI) hierarchies are also fully supported with Windows 2000 Server.

Starting the Key Management Service

There are two procedures you must perform to start the Key Management Service. Perform the first procedure after you install Windows 2000 Server but before you install Exchange 2000 Server, and perform the second procedure after you install Exchange 2000 Server and the Key Management Service.

After you install Windows 2000 Server but before you install Exchange 2000 Server, install Certificate Services. When you install Exchange 2000 Server, be sure that you select **Microsoft Exchange Key Management Services** in the

Component Selection window of the Installation Wizard.

After you install Exchange 2000 Server, you must perform the following steps to start the Key Management Service:

1. Start the Active Directory Sites and Services snap-in, click **View**, and then click **Show Services Node**.
2. Click **Services**, point to **Public Key Services**, and then click **Certificate Templates**.
3. In the MachineEnrollmentAgent template, click **Properties**.
4. Click the **Security** tab, add the Authenticated Users group, and then assign it Read permissions.
5. Add Enroll permission to the Exchange KMServers group.
6. In the ExchangeUser template, click **Properties**.
7. Click the **Security** tab, add the Exchange KMServers group, and then assign it Enroll permissions.
8. In the ExchangeUserSignature template, click **Properties**.
9. Click the **Security** tab, add the Exchange KMServers group, and then assign it Enroll permissions.

Note Do not install more than one KM server for each administrative group. Although Exchange 2000 Server allows you to install multiple KM servers in a single administrative group, Microsoft recommends that you install only one KM server for each administrative group.

Additional References

Knowledge Base Articles

Q192044 XADM: Setting Up X509v3 Certificates on Exchange 5.5 SP1 KMS with Local Certificate Server

Q242466 XADM: Error Message: The Key Management Server Is Unable to Operate

Q247814 XADM: Key Management Server Cannot Grant V3 Certificates to Users with Long Distinguished Names

Q218802 XADM: Can't Enroll Using X.509 V3 Certificates

Q216653 XADM: Certificate Server is Exclusive to Exchange Advanced Security

Q197965 XGEN: FAQs on High and Low Encryption in Exchange Server

Q216922 Certificate Server Does Not Create Backups of Installed Keys

Q264862 XADM: No Certificate Revocation List Distribution Points Extension in X.509 V3 Certificate

Q262288 Exchange 5.5 KMS Does Not Work with Windows 2000 Certificate Server in a Windows NT 4.0 Domain

Q242276 XADM: KM Server with Subordinate CA Displays Error Message: The Hierarchy of the MS Certificate Servers for Your KM Server Is Invalid c1031daf

Resources

The latest security information from Microsoft is available at the following Web site:

http://www.microsoft.com/security

Information for software developers is available through the Microsoft Developer Network (MSDN™) at the following Web site:

http://msdn.microsoft.com

Additional white papers about Windows 2000 Server and security are available at the following Web site:

http://www.microsoft.com/windows2000/technologies/security/default.asp

Secure/Multipurpose Internet Mail Extensions (S/MIME) Internet standards are available at the following Web site:

http://www.imc.org/ietf-smime

Documents

U.S. Government

The National Institute of Standards and Technologies (NIST), in conjunction with the Department of Defense (DOD) and the National Security Agency (NSA), has published information on U.S. Government federal public key infrastructure (PKI) efforts. Published documents are available at the following Web site:

http://csrc.nist.gov/pki

For More Information

The latest information about the Windows 2000 Server operating system is available at the following Web site:

http://www.microsoft.com/windows2000/default.asp

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

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

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

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.