INSTALLAZIONE CERTIFICATION AUTHORITY SU WINDOWS 2003 SERVER

Windows Server 2003 can be used as a Certificate Authority (also known as CA) to provide extended security by offering support for Digital Certificates.

Digital Certificates can be granted to users based upon their roles and group membership. For example, a regular user that wants to enroll for a certificate will only be allowed to enroll for a specific set of Digital Certificates, while another user that is a member of the Domain Admins group will be allowed to enroll for a different set of certificates that can be used for a variety of functions, including Recovery Agents, IPSec, SSL and so on.

User Digital Certificates are valid for different purposes, including:

- Allowing data on disk to be encrypted
- Protecting e-mail messages
- Proving the user's identity to a remote computer

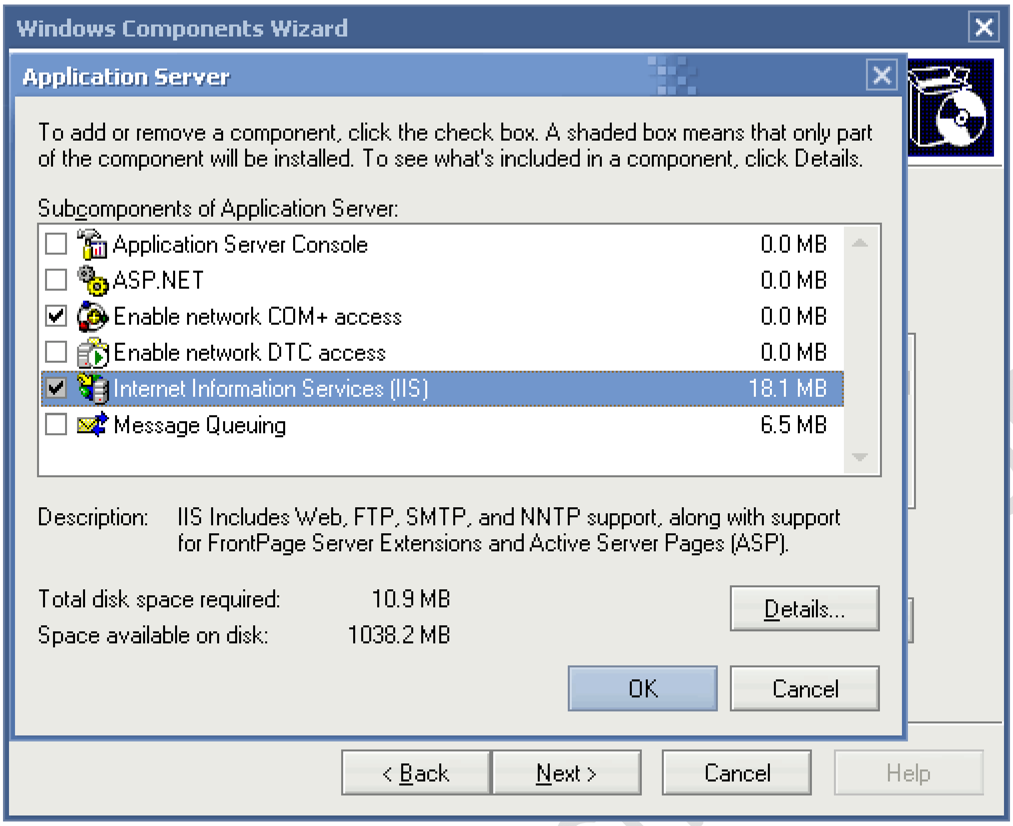
and more.

Note: There may be scenarios where a company might opt to use 3rd party issued Digital Certificates instead of creating their own, especially when that company's users will be dealing with out-of-the-company users, exchanging encrypted e-mail messages between themselves and these outside users, or when using SSL on a secured web site. This is because the outside users might not be willing to trust the company's internal CA.

Step 1: Install the IIS Service

In order to install the CA you will first need to install IIS on a Windows Server 2003 computer. On Windows Server 2003 IIS is not installed with the default Windows 2003 installation.

1. Click Start > Control Panel > Add or Remove Programs.
2. In Add or Remove Programs, click Add/Remove Windows Components.
3. Under Components, click on Application Server (but do NOT select it) and press on the Details button.
4. In the Application Server window click to select IIS and click Ok.



Windows Components Wizard

Application Server

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

Subcomponents of Application Server:

□ Application Server Console	0.0 MB
□ ASP.NET	0.0 MB
☑ Enable network COM+ access	0.0 MB
□ Enable network DTC access	0.0 MB
☑ Internet Information Services (IIS)	18.1 MB
□ Message Queuing	6.5 MB

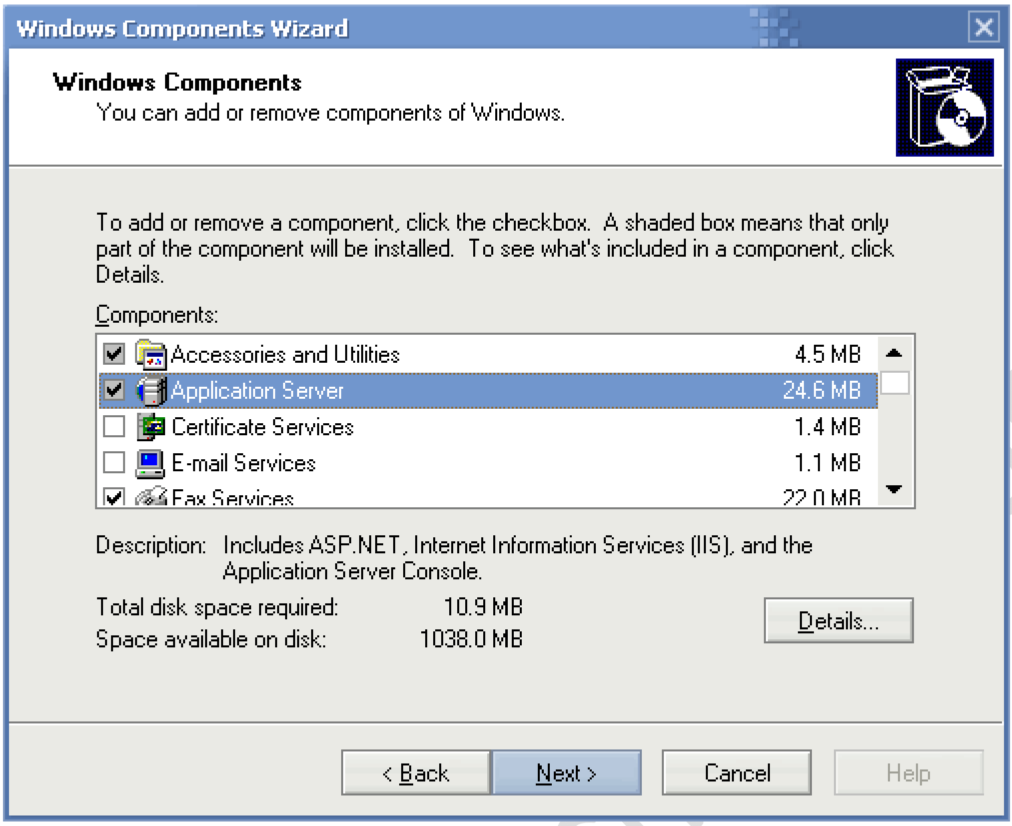
Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 10.9 MB

Space available on disk: 1038.2 MB

Fig.1

5. Click Next



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

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

Components:

☑ Accessories and Utilities 4.5 MB

☑ Application Server 24.6 MB

□ Certificate Services 1.4 MB

□ E-mail Services 1.1 MB

☑ Fax Services 22.0 MB

Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.

Total disk space required: 10.9 MB

Space available on disk: 1038.0 MB

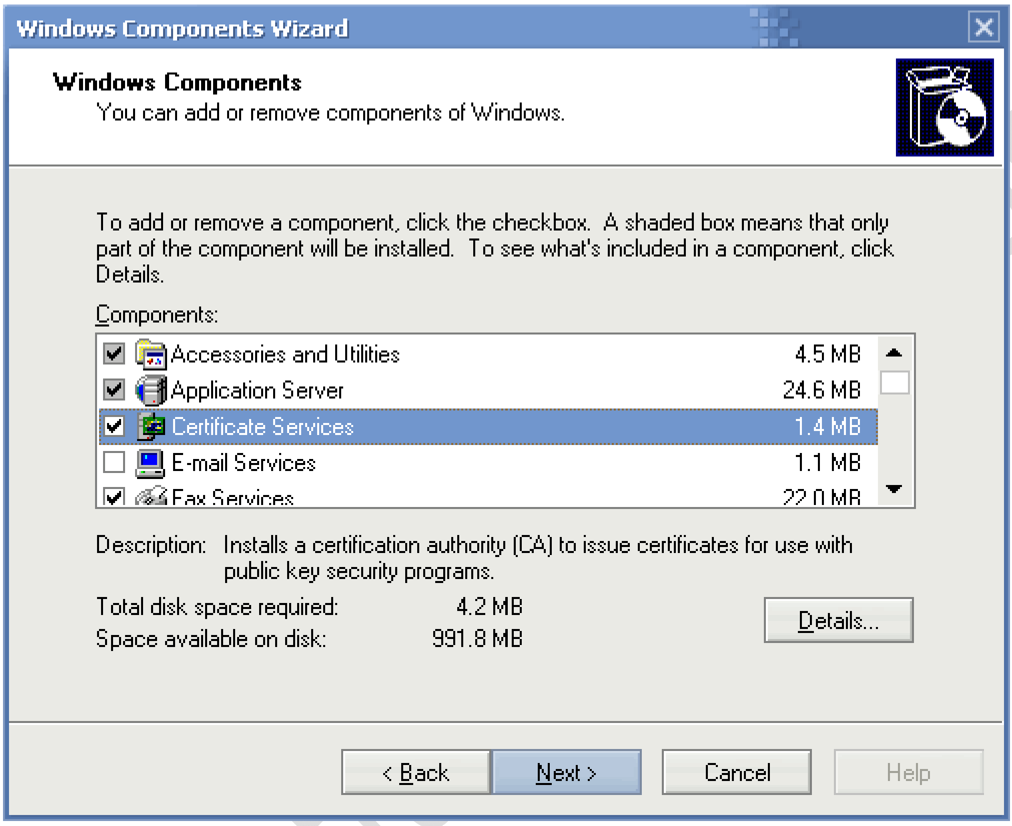
Fig.2

6. After the wizard completes the installation, click Finish.

Step 2: Install the CA Service

To install the CA service perform the following steps:

1. Click Start > Control Panel > Add or Remove Programs.
2. In Add or Remove Programs, click Add/Remove Windows Components.
3. Under Components, select Certificate Services.



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

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

Components:

☑	Accessories and Utilities	4.5 MB
☑	Application Server	24.6 MB
☑	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
☑	Fax Services	22.0 MB

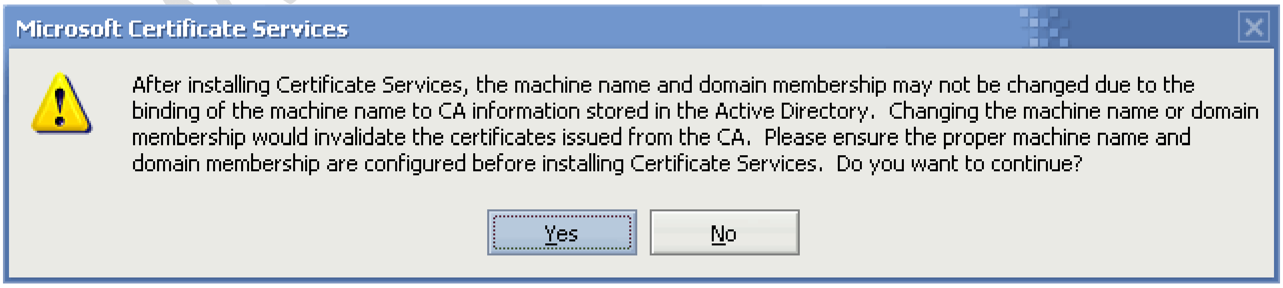
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 4.2 MB

Space available on disk: 991.8 MB

Fig.3

5. You will get a warning about domain membership and computer renaming constraints, and then click Yes.

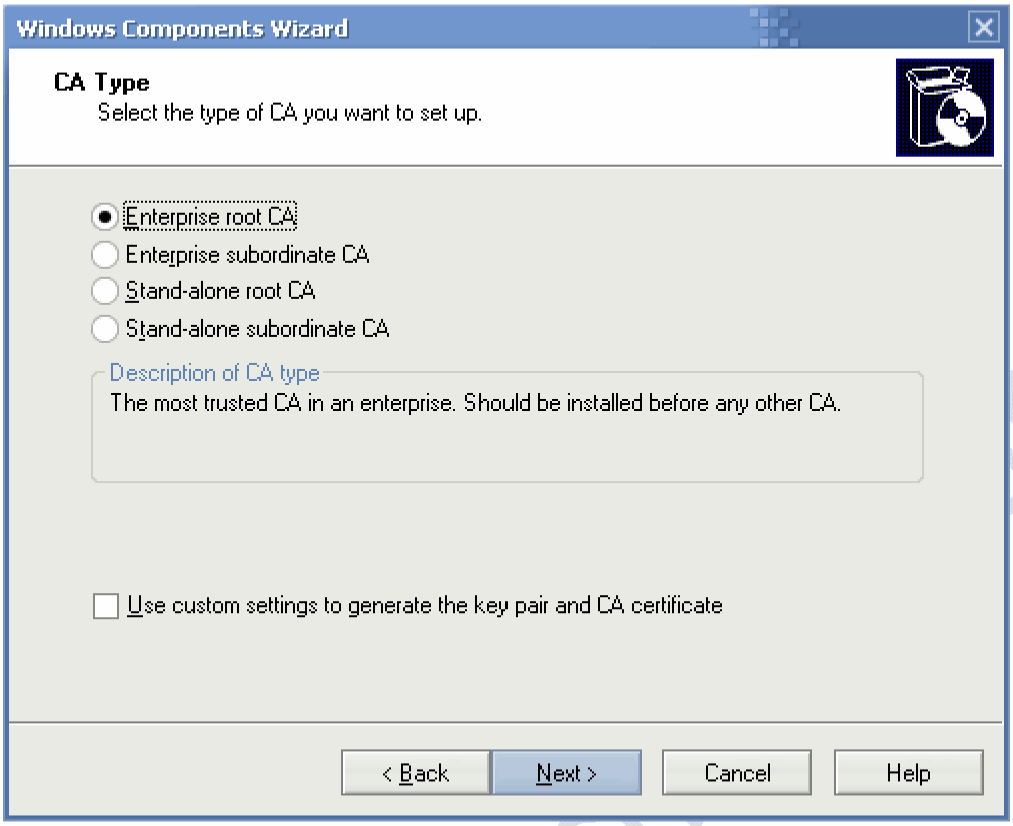


Microsoft Certificate Services

After installing Certificate Services, the machine name and domain membership may not be changed due to the binding of the machine name to CA information stored in the Active Directory. Changing the machine name or domain membership would invalidate the certificates issued from the CA. Please ensure the proper machine name and domain membership are configured before installing Certificate Services. Do you want to continue?

Fig.4

6. On the CA Type page, click Enterprise root CA, and then click Next.



Windows Components Wizard

CA Type

Select the type of CA you want to set up.

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

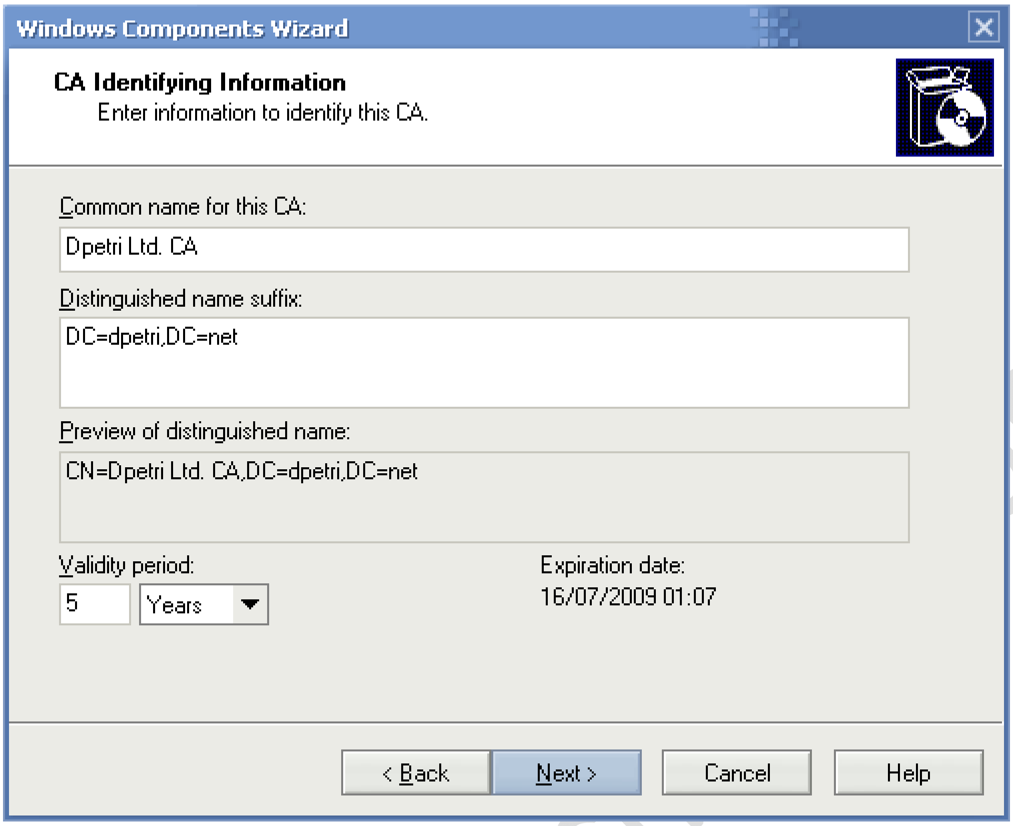
Description of CA type

The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

Fig.5

7. On the CA Identifying Information page, in the Common name for this CA box, type the name of the server, and then click Next.



Windows Components Wizard

CA Identifying Information

Enter information to identify this CA.

Common name for this CA:

Dpetri Ltd. CA

Distinguished name suffix:

DC=dpetri,DC=net

Preview of distinguished name:

CN=Dpetri Ltd. CA,DC=dpetri,DC=net

Validity period:

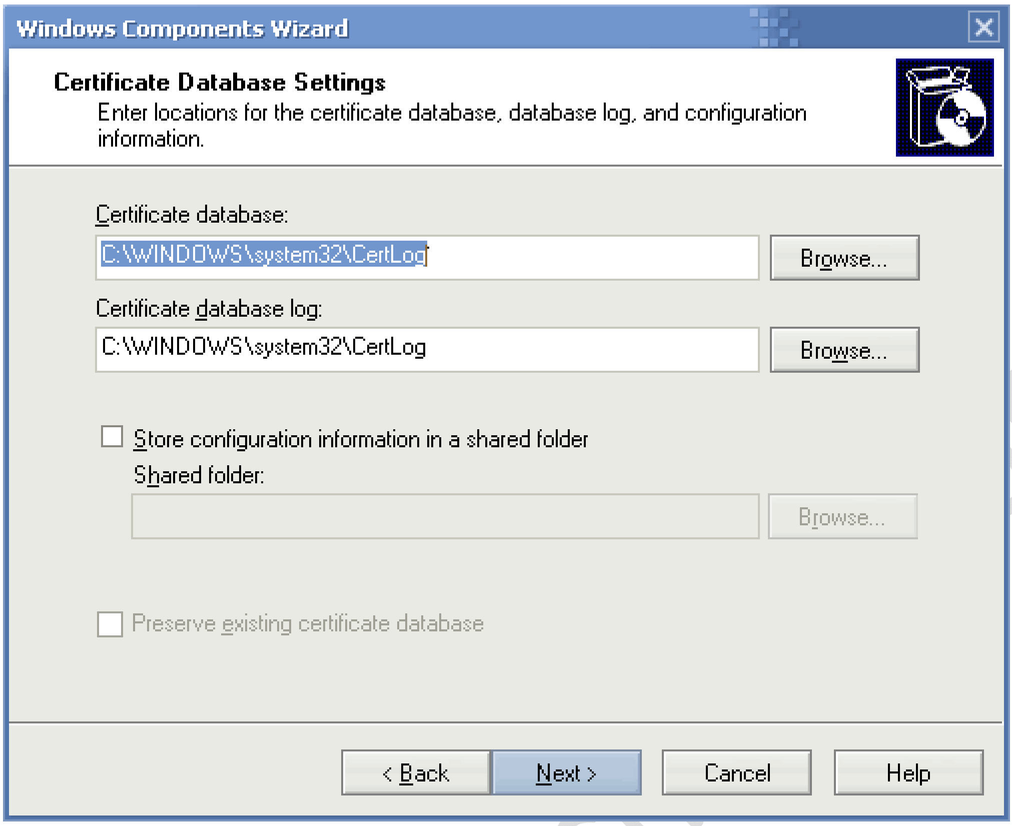
5 Years

Expiration date:

16/07/2009 01:07

Fig.6

8. On the Certificate Database Settings page, accept the defaults in the Certificate database box and the Certificate database log box, and then click Next.


Windows Components Wizard

Certificate Database Settings

Enter locations for the certificate database, database log, and configuration information.

Certificate database:
C:\WINDOWS\system32\CertLog

Certificate database log:
C:\WINDOWS\system32\CertLog

☐ Store configuration information in a shared folder

Shared folder:

☐ Preserve existing certificate database

Fig.7

9. You will get a prompt to stop Internet Information Services, click Yes.
10. Enable Active Server Pages (ASPs), by clicking Yes.
11. When the installation process is completed click Finish.

Step 3: Obtain a User Digital Certificate from the CA

After installing and configuring the CA on your domain you will now need to ask your users (at least those who will require message security) to enroll for a Digital Certificate.