



Operating System

Certificate Service Web Pages

Beta 3 Technical Walkthrough

Abstract

A set of Web pages is provided with the Certificate Services found in the Microsoft® Windows® 2000 operating system. These Web pages provide a simple way of performing many of the common tasks that are performed against a Certificate Authority (CA). This walkthrough will focus on the process of requesting, CA certificates, user certificates, and other special certificates.

© 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, the BackOffice logo, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA
0499*

CONTENTS

INTRODUCTION	1
BEFORE YOU BEGIN.....	2
Confirming the Web Page Settings	2
CONNECTING TO THE WEB PAGES.....	3
INSTALLING CA CERTIFICATES	4
REQUESTING A CERTIFICATE	10
COMPLETING A PENDING REQUEST	16
VERIFYING ISSUED CERTIFICATE.....	19
Internet Explorer 4.0	19
Internet Explorer 5.0	19
REQUESTING AN ADVANCED CERTIFICATE.....	20
ENROLLING USING A PKCS#10 REQUEST FILE	27
KNOWN ISSUES	32
Error When Accessing the Web Pages	32
Cannot Log into Web Pages	32
Must Set Pages to Basic Authentication or They Are Remote	32
FOR MORE INFORMATION	33
Before You Call for Support	33
Reporting Problems	33

INTRODUCTION

Certificate Service for the Microsoft® Windows® 2000 operating system provides sample Web pages. These sample pages allow you to connect to the service with a Web browser, and to do common tasks such as requesting the Certificate Authority (CA) Certificate, requesting certificates from a CA, processing a certificate request file, or processing a smart card enrollment file.

These Web pages can be used by anyone who needs to request a certificate from the Microsoft CA. The Web pages behave differently depending on the type of CA to which you are connecting:

The Enterprise CA will require you to log on to the Web pages using your user ID. You will then request a certificate base by selecting a *Certificate template*. The CA will then find your account in Microsoft Active Directory™ directory service, and will generate a certificate based on the information in the Active Directory and the template you chose. When requesting a certificate from an Enterprise CA, you need to provide very little information.

A stand-alone CA, however, will not ask for a login ID. It will simply look at the certificate request information you provide and issue a certificate based on that information. By default the standalone CA will not immediately issue the certificate; an administrator must first approve your request using administration tools. This means that you will have to visit the Web pages twice: the first time to submit the request, and the second time to retrieve the certificate. It is possible for the administrator to configure the CA to issue a certificate immediately, and in that case you will receive your certificate immediately after your request.

BEFORE YOU BEGIN

Before you begin, you will need access to a Microsoft Certificate Service. If you do not have access to a Microsoft Certificate Service, then you can install the certificate service by following the walkthrough entitled *Setting up a Windows 2000 Certificate Authority*.

The Web pages are located on <http://ServerName/CertSrv> where *ServerName* is the name of the CA machine.

If you connect to the Certificate Services Web pages and encounter an error, check to ensure that the pages are installed. It is possible that the Microsoft Internet Information Server (IIS) is not installed or was installed after the Certificate Service. In that case, the Web pages will not be installed.

Confirming the Web Page Settings

If you are using an Enterprise CA, you need to first make sure the security is set correctly on the Web pages. (Note that you need to do this only if you will be connecting to an Enterprise CA. If you are connecting to a standalone CA, you can skip this process.)

An Enterprise CA requires the certificate requestor to be authenticated by the page so that it can determine the correct information to put in certificate. If you do not have authentication set for the Web pages in an Enterprise CA, the pages will fail to generate a certificate; or, if a certificate is generated, it will be useless.

To confirm the security settings

1. Click the **Start** button, point to **Programs**, point to **Administrative Tools**, and click **Internet Service Manager**.
2. Open the local Web site, and navigate to the **CertSrv** virtual directory (located in the default Web site). If you cannot locate **CertSrv**, check to make sure that the Certificate Service is installed. You may need to uninstall and reinstall the Certificate Service to make this virtual directory appear.
3. Right-click **CertSrv**, and select **Properties** from the context menu.
4. Select the **Directory Security** tab.
5. Under **Anonymous access and authentication control** and click **Edit**.
6. Clear all check boxes except **Integrated Windows NT authentication**.
7. Click **OK**, and close all dialog boxes.

CONNECTING TO THE WEB PAGES

Open your browser and connect to `http://ServerName/CertSrv` where *ServerName* is the name of the server holding the Web pages. These pages have been written specifically to support Netscape Navigator 3.0 and later, and Microsoft Internet Explorer 4.0 and later.

If you are connecting to an Enterprise CA you will be required to log on to the Web pages. You may or may not see a dialog asking for a user ID and password. This will depend on the authentication scheme negotiated between the browser and the Web server. If you see a dialog asking for a user ID and password, enter the information.

After connecting, you will see a page with three options:

- Retrieve a root certificate or CRL
- Request a certificate
- Check a pending certificate

If the CA to which you are connecting is an Enterprise CA and your computer is a member of the Enterprise then you can skip the first choice.

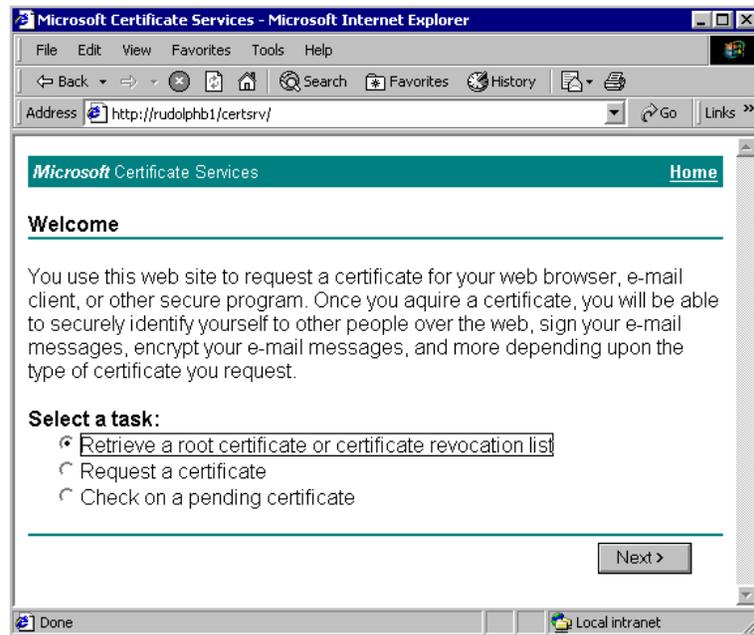
If however you are connecting to a standalone CA, then you will need to retrieve the root certificate and specify that you trust it before you take advantage of Public Key Infrastructure (PKI).

The following sections detail each of these activities.

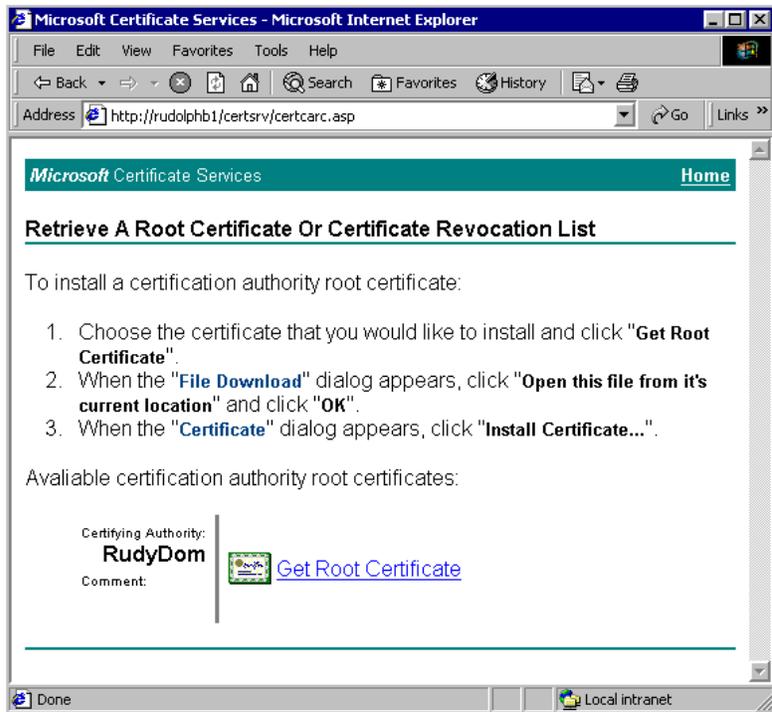
INSTALLING CA CERTIFICATES

To install certificates

1. After connecting to the Web page (<http://ServerName/CertSrv/>), you should see the following screen:



2. Click **Retrieve a root certificate or certificate revocation list** and click **Next**. You will see a screen similar to the one below:

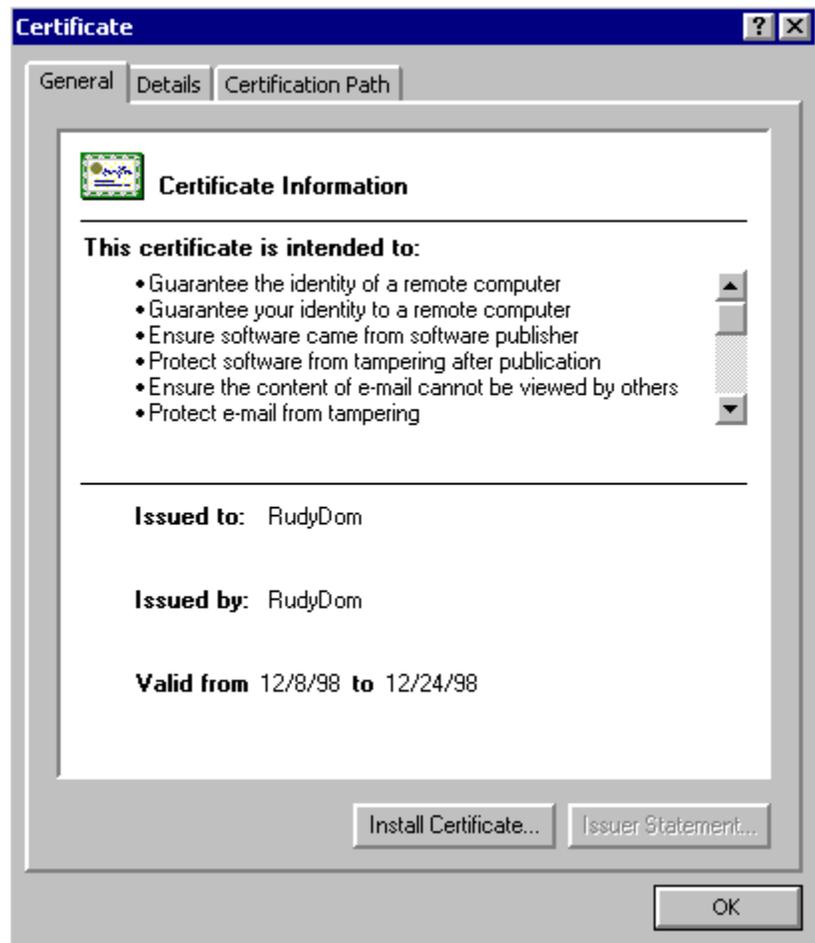


Follow the instructions on this screen to install the CA certificate into the trusted root store on your machine. After you install this certificate, your system will then trust certificates issued by this CA. This means that if an application you are using tries to use a certificate that is issued by this CA, it will be successful. For example, if it tries to verify secure mail or IP Security (IPSec) protocols, the application will succeed in the verification.

3. Click the **Get Root Certificate** link. The subsequent dialogs will depend on your browser and operating system. The following dialog boxes appear if you are running Windows 2000.
4. Click **Open this file from its current location**. Click **OK**.



5. Read the certificate details and decide if you trust the CA. If you decide to trust this certificate for all of the listed intended uses, click the **Install Certificate** button.

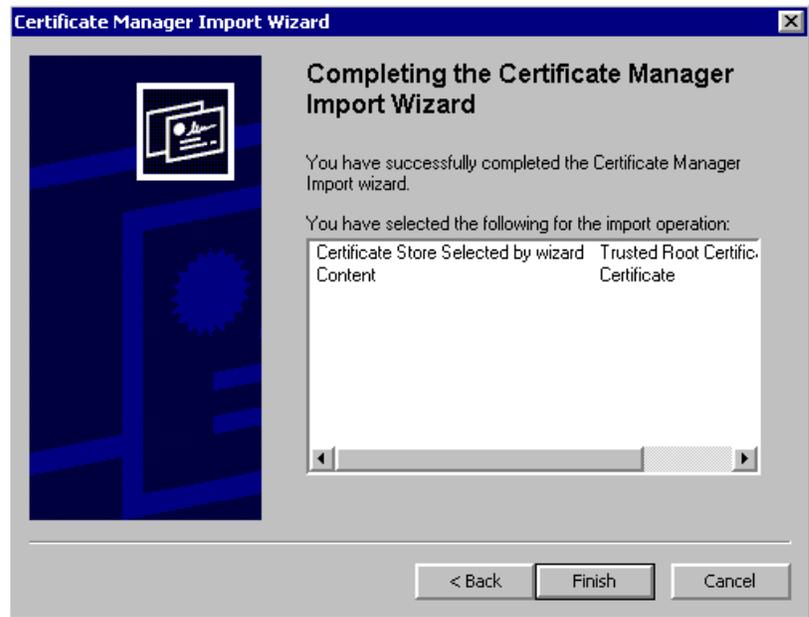


- This will start the **Certificate Manager Import Wizard**. Click **Next**.



- The wizard will then ask you to select the new stores for the certificate. Select **Automatic**, and click **Next**.

- The wizard will indicate where it is storing the certificate. A CA root certificate should be stored in the root store and a subordinate CA certificate in the Intermediate CA store. Click **Finish**.



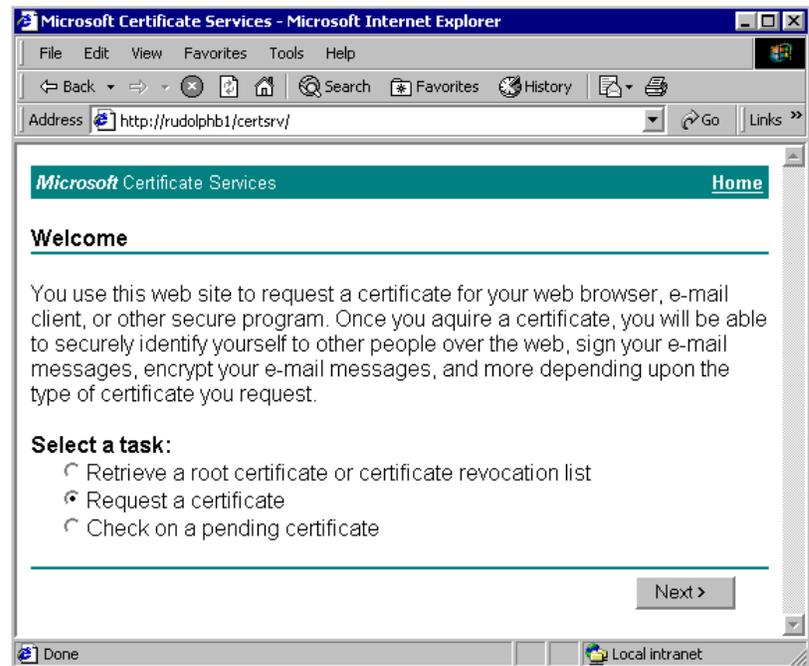
- If the import operation completes successfully, you will then see the following message. Click **OK**. Now you can move on to requesting a certificate.



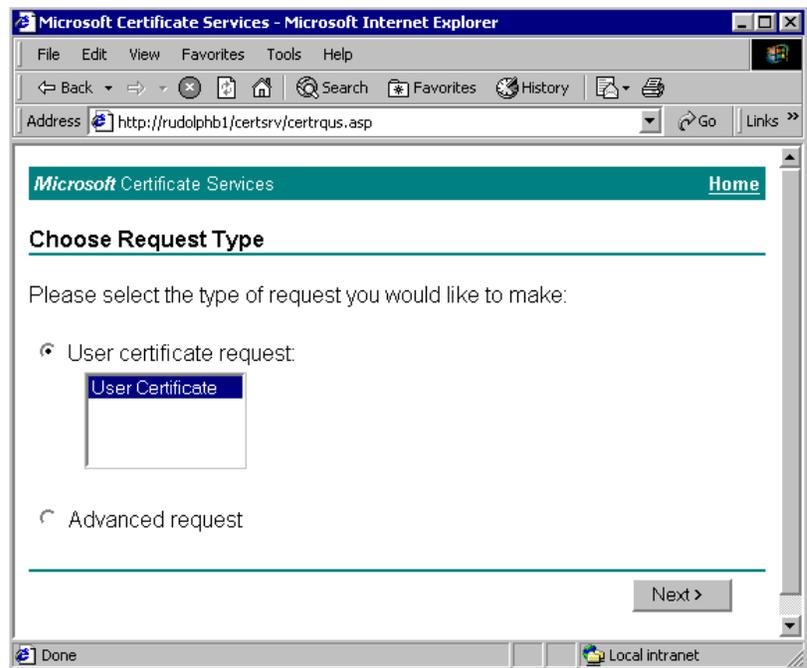
REQUESTING A CERTIFICATE

To install certificates

1. Connect to the Web page (<http://ServerName/CertSrv>), and check the **Request a Certificate** option on the main Certificate Services Web page. This allows you to request a certificate.
2. Click **Request a Certificate**, and then click **Next**.



3. Click **User certificate request**.
4. Click **User Certificate** in the list box. On this screen, you may see more than one entry in the list box. Click **Next**.



The contents of the list box depends on the type of CA to which you are connecting and the certificates that the CA is configured to issue.

If you are connecting to an Enterprise CA, you will see **User Certificate** and possibly other options. Generally, a User Certificate is the right choice for client authentication, a Web browser, and email. In some cases, you may see different options depending on what type of certificates the administrator has enabled for this Enterprise CA.

The list box will contain Web browser and email protection if you are connecting to a stand-alone CA.

5. Complete the **User Certificate - Identifying Information** and click **Next**.

If you are connecting to a standalone CA you will see the following page.

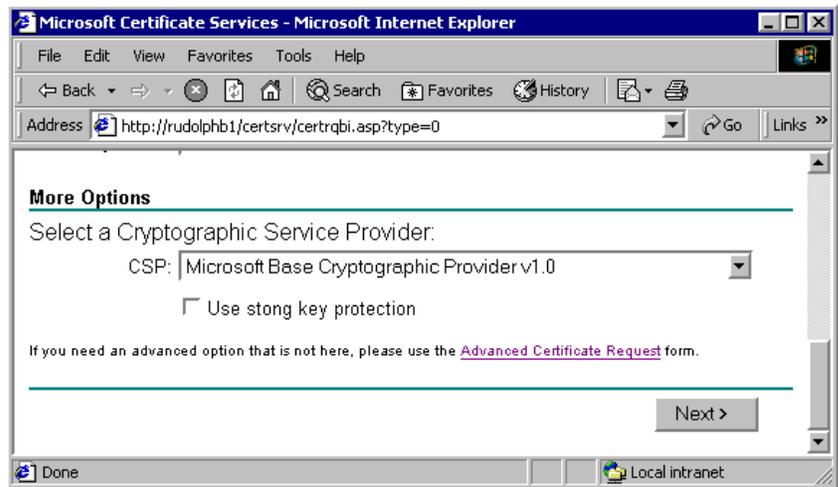
If you are connecting to an Enterprise CA the information will be retrieved from the Active Directory and this page will not request further details.

The screenshot shows a Microsoft Internet Explorer browser window displaying the 'Microsoft Certificate Services' web page. The address bar shows the URL: <http://rudolphb1/certsrv/certrqbi.asp?type=0>. The page content includes a header for 'Microsoft Certificate Services' with a 'Home' link. The main heading is 'User Certificate - Identifying Information'. Below this, a message asks the user to fill in identifying information for their certificate. The form contains the following fields and values:

- Name: NoBody
- E-Mail: NoBody@Microsoft.com
- Company: Microsoft Corporation Inc.
- Department: Windows NT
- City: Redmond
- State: Washington
- Country: US

Below the form, there is a prompt: 'Please enter a friendly name for your certificate:' followed by a 'Friendly Name' field containing 'My certificate'. At the bottom of the form area, there is a 'More Options >>' button. At the bottom right of the page, there is a 'Next >' button. The browser's status bar at the bottom shows 'Done' and 'Local intranet'.

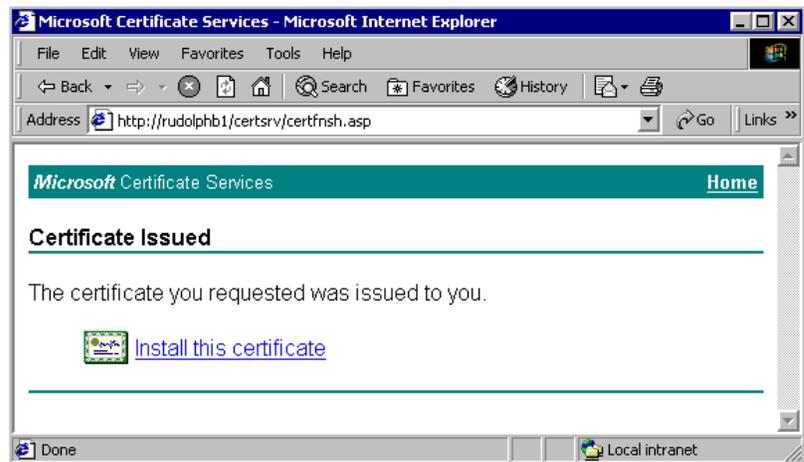
6. If you click the **More Options** button, you will be able to set the Cryptographic Service Provider (CSP). Generally, you should not need to select a CSP. You need a CSP if you are configuring additional options, such as enrolling for a smart card or using a different public key algorithm. Do not change the CSP setting unless you know you need to select a different CSP. Click **Next**.



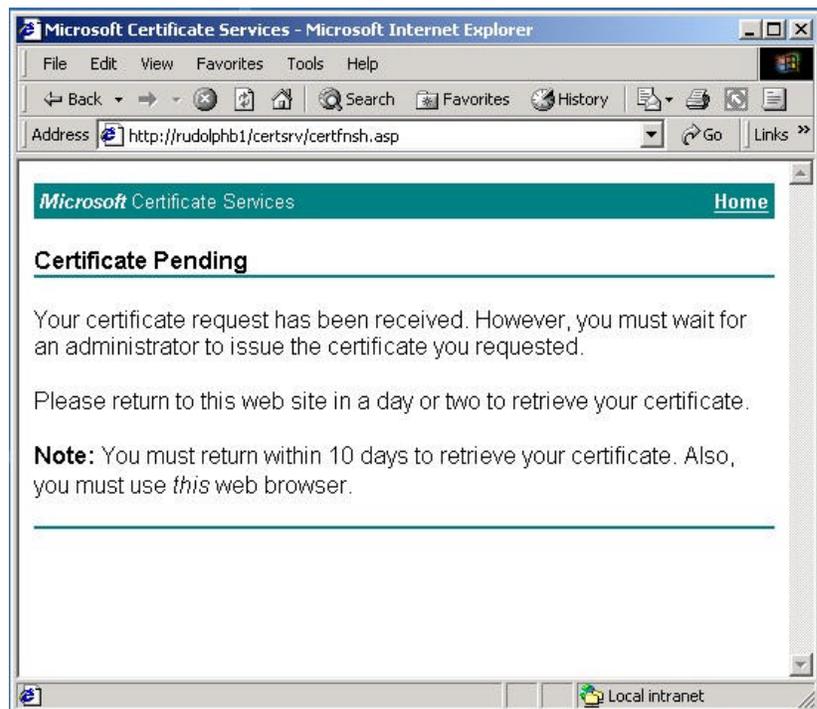
7. The pages will now generate a privatekey pair and a certificate request with the information you provided.

The request is then sent to the CA for processing.

8. If the CA is set up to approve the request automatically, you will be issued the new certificate. Click the **Install this certificate** link.



9. If your CA is setup to require administrative approval before issuing a certificate, you will see the following screen. Refer to the section, "Completing a Pending Request" in this walkthrough document.



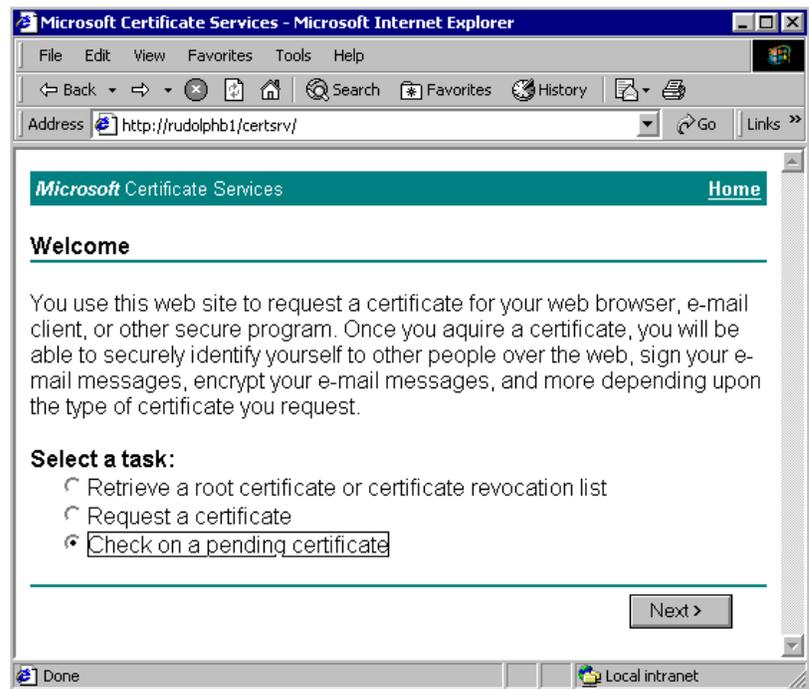
Otherwise, you will see the following screen. Your certificate is now installed. Click **OK**.



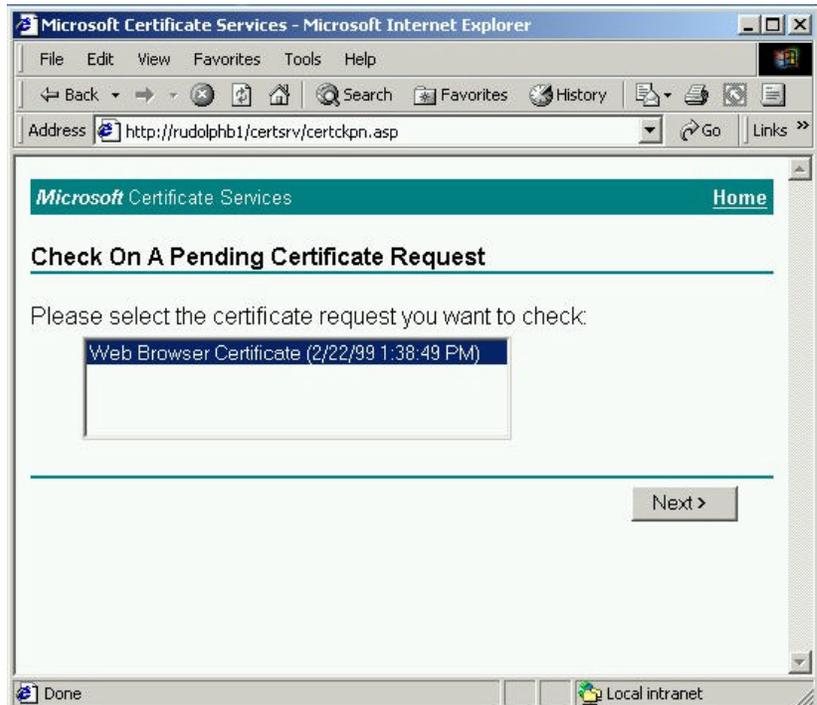
COMPLETING A PENDING REQUEST

To complete a certificate request that requires administrative approval

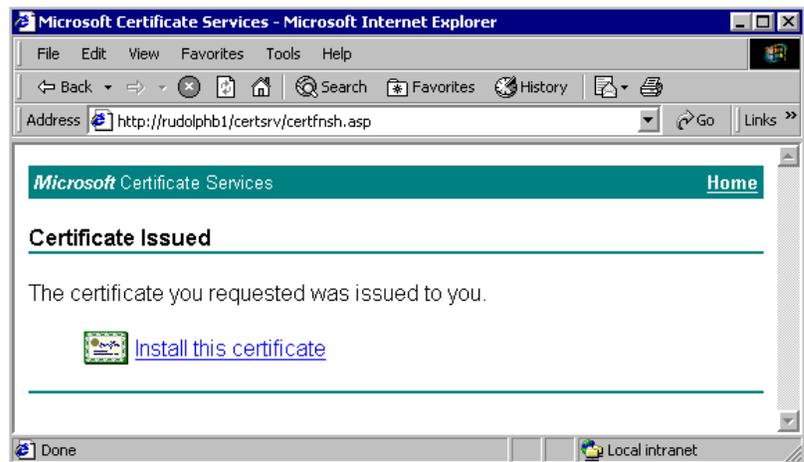
1. If you did not immediately receive a certificate when you made your certificate request, you can check the status of your request by returning to the Web pages (<http://ServerName/CertSrv>). Click **Check on a pending certificate** and then click **Next**.



2. Your approved certificate requests will appear in the list box. Select one, and click **Next**.



3. Click the **Install this certificate** link.



4. Your certificate is now installed. Click **OK**.



VERIFYING ISSUED CERTIFICATE

To view or verify that the certificate was downloaded, complete the appropriate procedure below.

Internet Explorer 4.0

To verify the certificate if you are using Internet Explorer version 4.0,

1. From the **View** menu, select **Internet Options**
2. Select the **Content** tab.
3. Click the **Personal** button.
4. Find the certificate you downloaded. Doubleclick it to see the details. If the certificate is not listed, the download was not successful.

Internet Explorer 5.0

To verify the certificate if you are using Internet Explorer version 5.0

1. From the **View** menu, select **Internet Options**
2. Select the **Content** tab.
3. Press the **Certificates** button. This will start the Certificate Manager user interface.
4. Using the Certificate Manager interface, find the certificate you downloaded. Double-click it to see the details. If the certificate is not listed, the download was not successful.

Alternatively, you can start the Certificate Manager user interface from Windows 2000.

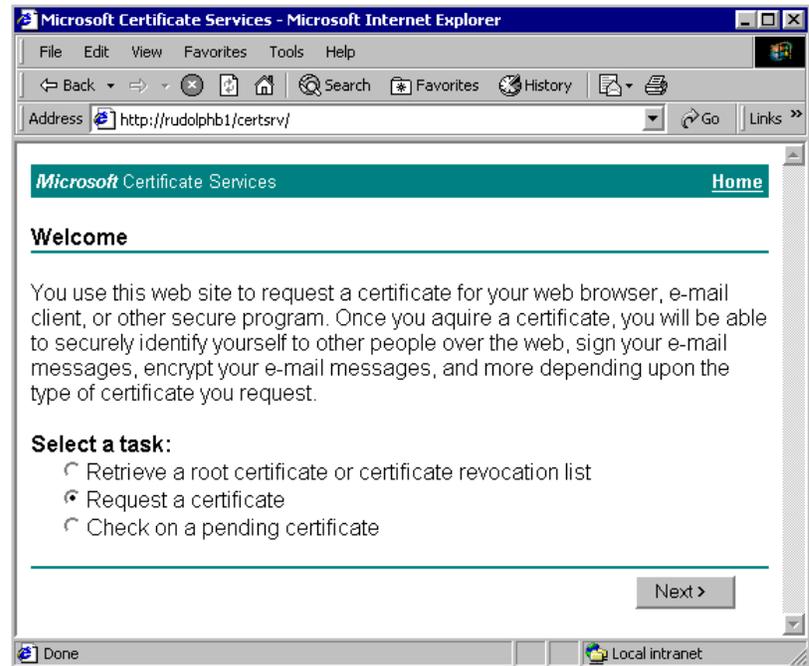
1. From the **Start** menu, point to **Programs**.
2. Point to **Administrative Tools** and then select **Certificate Manager**.
3. Using the Certificate Manager interface, find the certificate you downloaded. Double-click it to see the details. If the certificate is not listed, the download was not successful.

REQUESTING AN ADVANCED CERTIFICATE

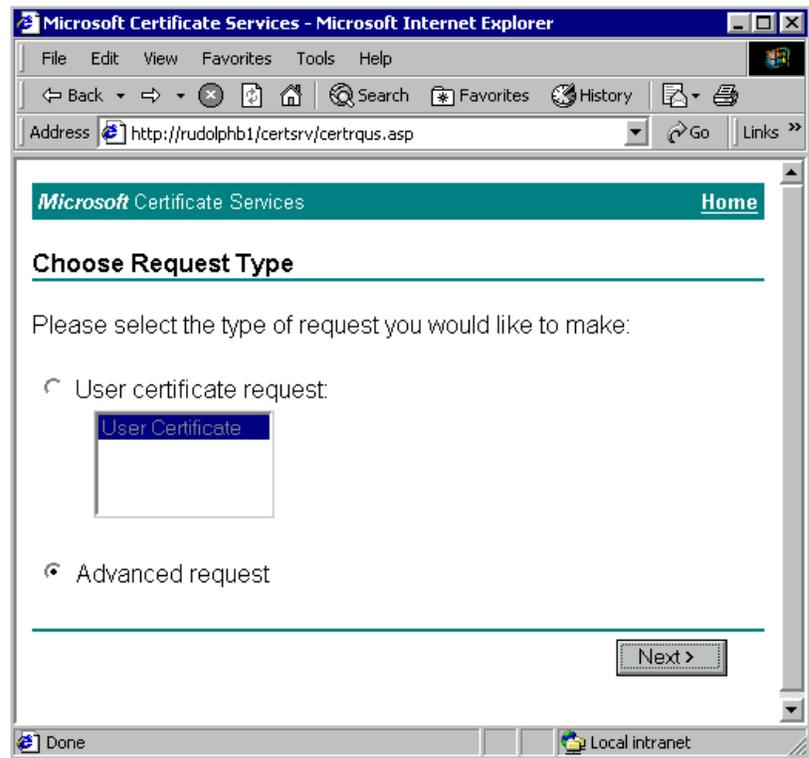
You will use the advance options if you need to make a special certificate request to the CA. For example, you may need to request a certificate for your Windows 2000 system for IP Security (IPSec) or you may need a certificate with a special key length. In these cases, you will use the advanced certificate requests.

To request an advanced certificate

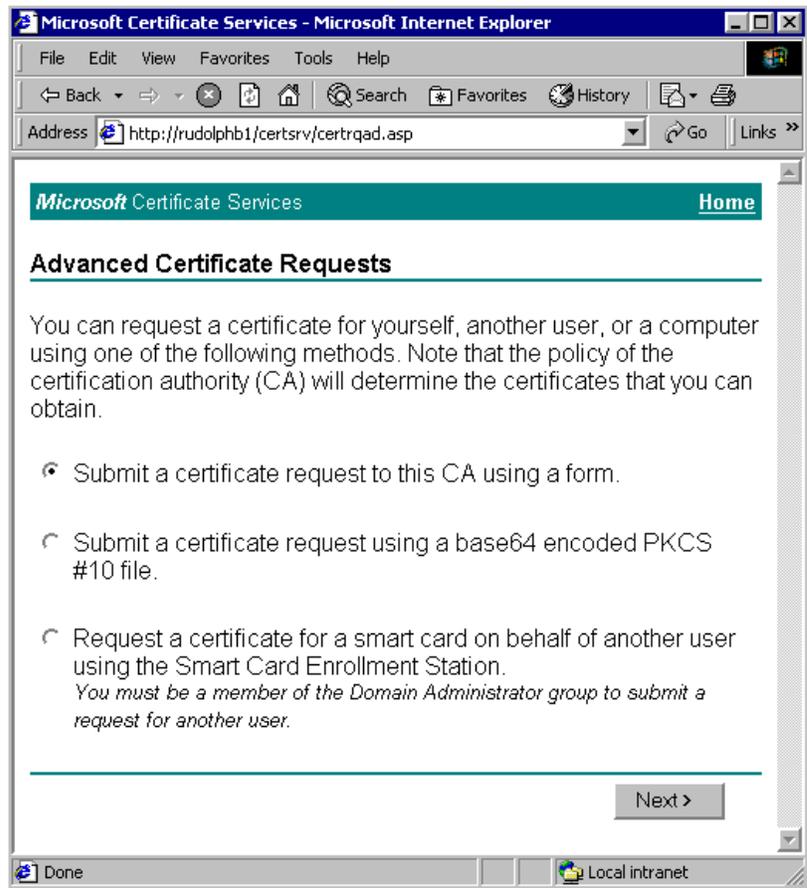
1. Go the primary Web page (<http://ServerName/CertSrv/>). Click **Request a Certificate**, and then click **Next**.



2. Click **Advanced request**, and then click **Next**.



3. Click **Submit a certificate request to this CA using a form** and then click **Next**. The two other options on this screen are discussed later in this document.



4. Complete the requested information, and click **Next**.

The screenshot shows a web browser window titled "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar contains "http://rudolphb1/certsrv/certrqma.asp". The page content includes a header "Microsoft Certificate Services" with a "Home" link. Below the header is the title "Advanced Certificate Request". The form is divided into several sections:

- Identifying information:** A series of text input fields containing: Name: NoBody, E-Mail: NoBody@Microsoft.com, Company: Microsoft Corporation Inc., Department: Windows NT, City: Redmond, State: Washington, and Country: US.
- Certificate Friendly Name:** A text input field containing "My certificate".
- Certificate Template:** A dropdown menu with "User" selected.
- Cryptographic Service Provider:** A dropdown menu with "Microsoft Base Cryptographic Provider v1.0" selected, and an unchecked checkbox labeled "Use strong key protection".

If you are connecting to an Enterprise CA, you will see the **Certificate Template** drop-down list box. You will see templates for those options that you have permissions to request only. If the list does not contain a template that you need, ask your administrator to give you permissions to request certificates. In most cases, you only need to select a Certificate Template. All other fields are optional; the CA will provide the other information based on the template you selected. The exceptions are the WebServer and IPsec Offline templates. These require you to fill in all of the other text box fields.

There are actually two templates for IPsec. The IPsec Online template is meant to be used by Windows 2000 systems that have entries in the Active Directory. The IPsec Offline template is meant to be used with PKCS#10 certificate request files from non-Windows 2000-based systems.

If you are connecting to a standalone CA, you will see an **Extended Key** usage field instead of the template field. This field indicates the purpose of the certificate. Choose the Extended Key usage most appropriate for you. For a

stand-alone CA, you will need to fill in all the fields. For example, if you want an IPsec certificate, use the IPsec Extended Key usage.

You will not need to change the **Cryptographic Service Provider** field unless you either need a different public key algorithm or you are using a special hardware device such as a smart card.

The screenshot shows a web browser window titled "Microsoft Certificate Services - Microsoft Internet Explorer". The address bar contains "http://rudolphb1/certsrv/certrqma.asp". The main content area has the following fields and options:

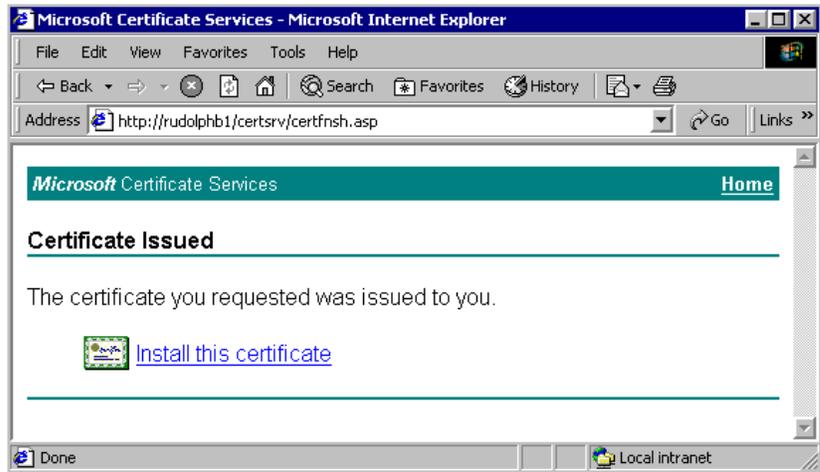
- Key Size: 512 (common key sizes: 512, 1024, 2048, 4096)
- Hash Algorithm: SHA/RSA
- Key Spec: Exchange Signature
- Key Generation Options:**
 - Create new key set
 - Set the container name
 - Use existing key set
 - Enable strong private key protection
 - Mark keys as exportable
 - Use local machine store
You must be an administrator to generate a key in the local machine store.
- Additional Options:**
 - Save certificate to a file
 - Save request to a PKCS #10 file
- Attributes: [Empty text box]

A "Submit >" button is located at the bottom right of the form area.

- **Key Size.** This depends on the application you are using and the Windows version you are running. In general, it is a good idea to select a size of 1024, however the export version of Windows 2000 cannot create an Exchange key larger than 512. If you are creating a certificate that will only be used for signing, then you can use the larger key sizes. For example IPsec certificates only need to be a signature key.
- **Hash Algorithm.** Unless you know that you need to change it, leave the Hash Algorithm as the default.
- **Key Spec.** This determines if the certificate will be used for encryption or only for signing operations.
- **Use local machine store** If you are requesting an IPsec certificate, you should also select **Use local machine store**, This places the Keys and the certificate in the machine store so that system processes such as IPsec can use them.

-
- **Save request.** click Save request to a PKCS #10 file under Additional Options. This creates a create a request file that you can then send to another CA. You would typically use this option if sending a request to Verisign or a non-Microsoft Certificate Service.
5. The pages will now generate a private key pair and a certificate request with the information you provided.
 6. The request is then sent to the CA for processing.

7. If the CA is set up to approve the request automatically, you will be issued the new certificate. Click the **Install this certificate** link. Otherwise, you will need to go to the section entitled “Completing a Pending Request,” earlier in this document.



8. Your certificate is now installed. Click **OK**.

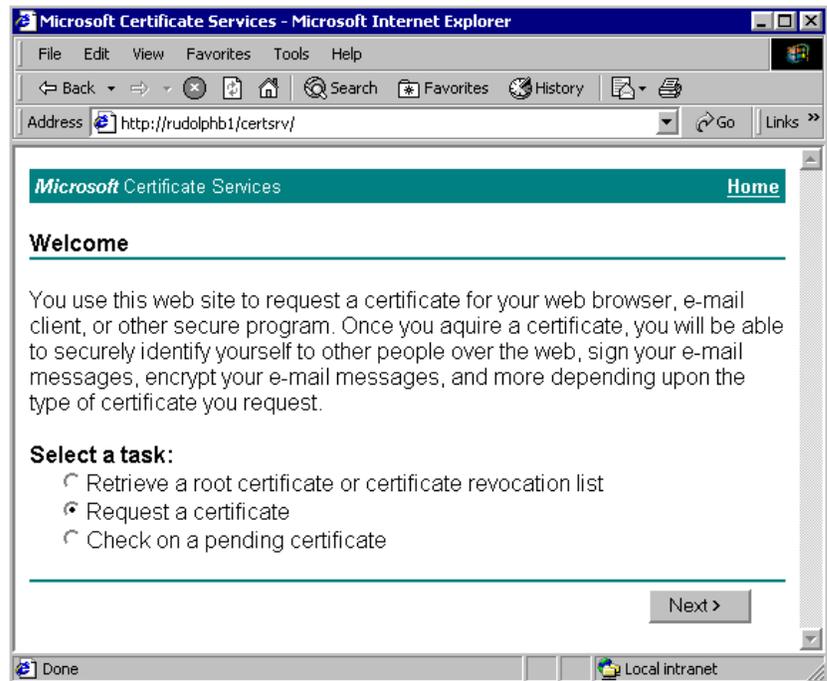


ENROLLING USING A PKCS#10 REQUEST FILE

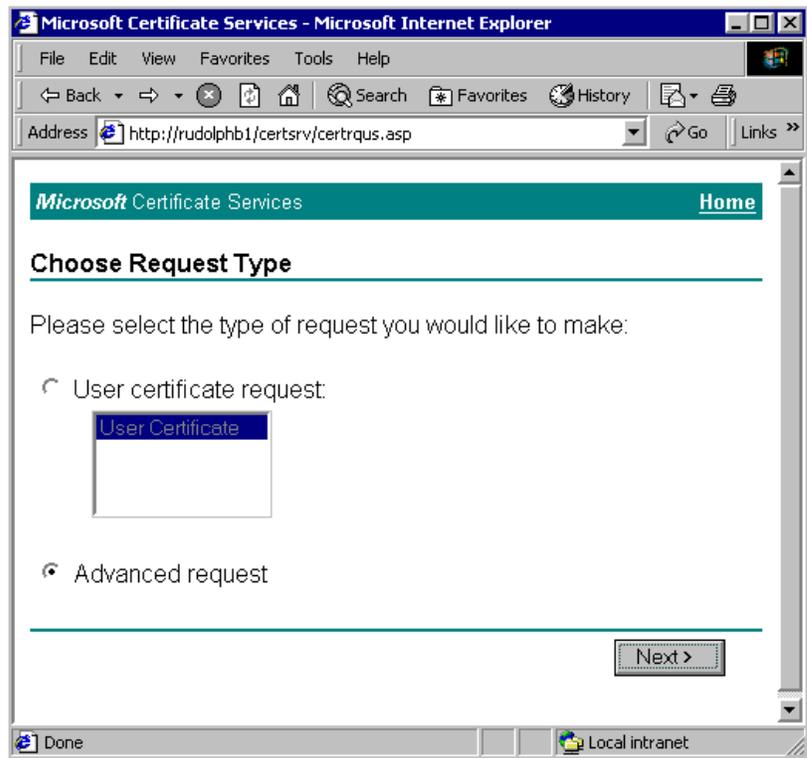
A number of devices and services generate PKCS#10 certificate request files. For example IIS, a subordinate CA, and IPSec devices can generate these files. These files contain all of the information and instructions needed to issue a certificate. Use the steps below to process this file and generate the certificate.

To process a PKCS#10 certificate request file

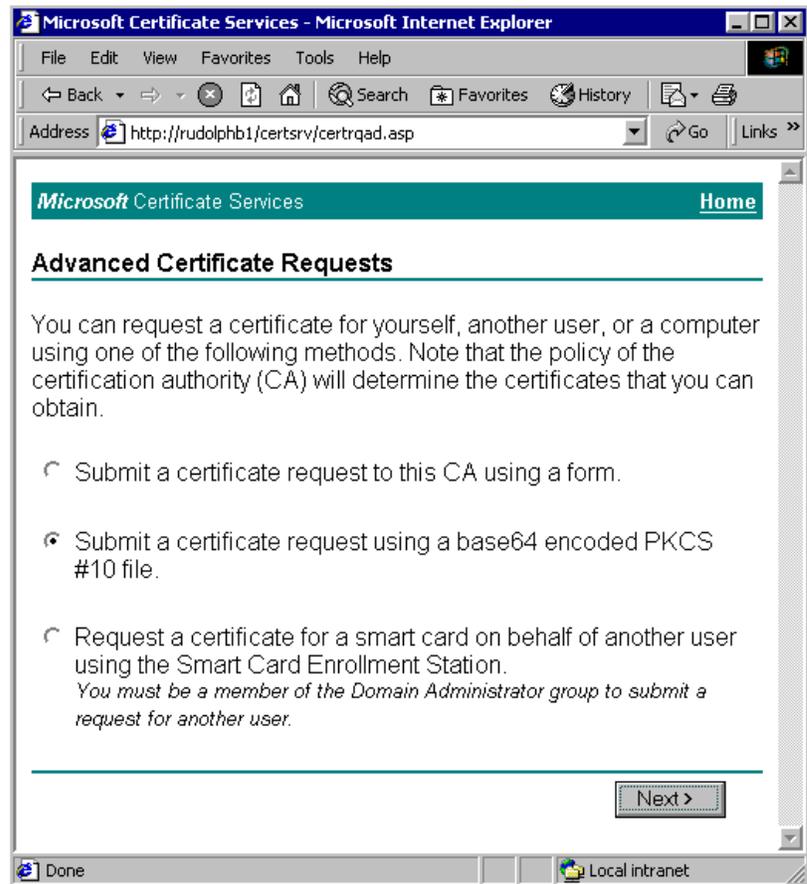
1. Go the primary Web page (<http://ServerName/CertSrv>).
2. Click **Request a Certificate**, and then click **Next**.



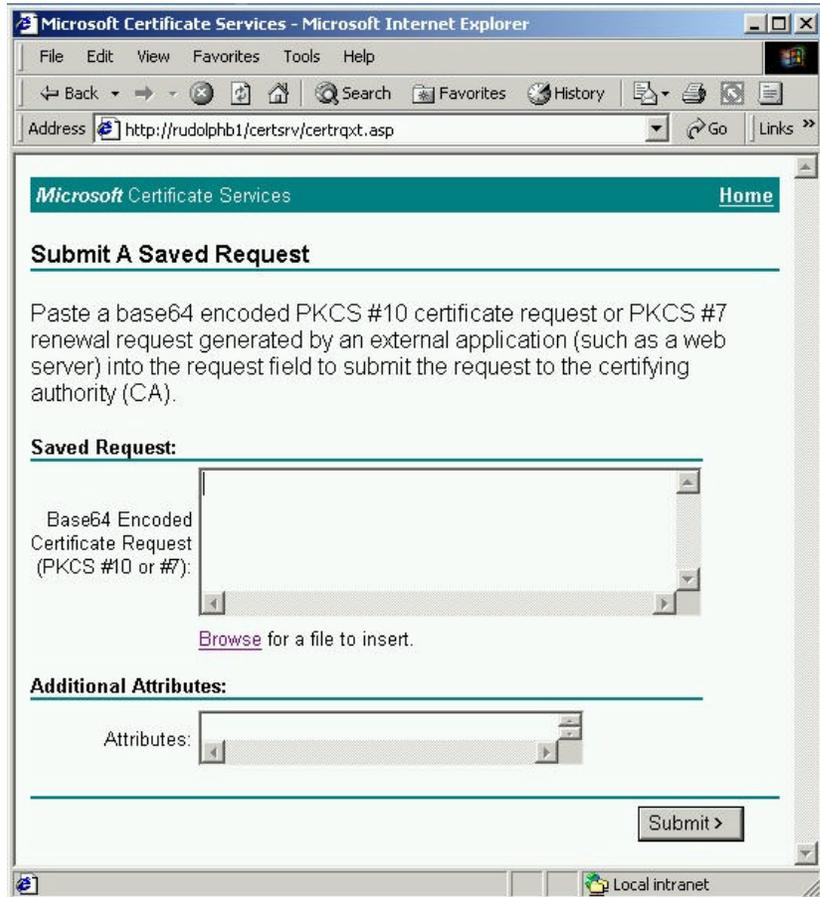
3. Click **Advanced request**, and then click **Next**.



4. Click **Submit a certificate request using a base64 encoded PKCS#10 file** and then click **Next**.

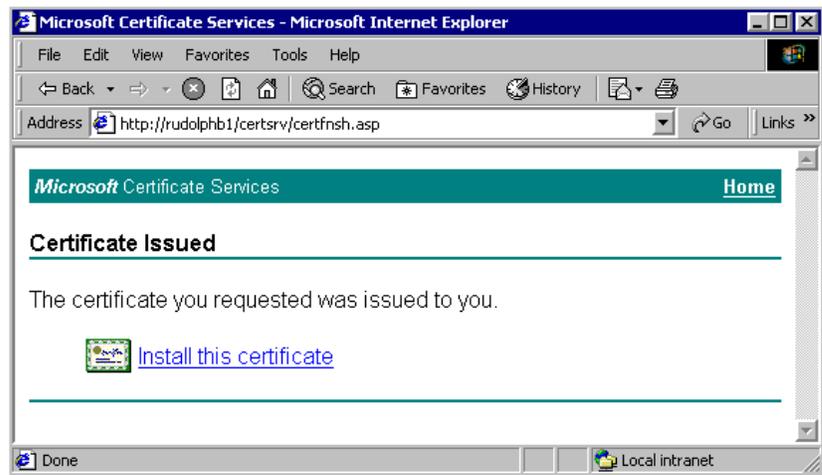


5. Follow the instructions for submitting a saved request. Paste the base64 encoded PKCS#10 in the text box, and then click **Submit**.



6. The Web pages will now generate a private key pair and a certificate request with the information you provided. The request is then sent to the CA for processing. When the processing is finished, the following dialog will be displayed.

Click the **Install this certificate** link.



7. Your certificate is now installed. Click **OK**.



KNOWN ISSUES

Error When Accessing the Web Pages

If you are encountering errors when connecting to the Web pages, check the following:

- Check to ensure the pages are actually installed. If the CA was installed before IIS, the pages may not be installed.
- Another alternative is that for an Enterprise CA the pages must require the user to authenticate. If the pages are set to allow anonymous connections then the CA will either not generate certificates or will generate junk certificates.

Cannot Log into Web Pages

If the Web pages negotiate basic authentication with the browser then your account must have the privilege to log onto the server. By default, only domain administrators have this privilege. You will need to change this default if you are using the Netscape browser.

Must Set Pages to Basic Authentication or They Are Remote

If the Web pages are located on a different server than the CA, you must set the pages to use basic authentication rather than NTLM if the CA is an Enterprise CA. In addition, you might secure these pages using Secure Sockets Layer (SSL) to protect the passwords.

FOR MORE INFORMATION

For the latest information on Microsoft Windows2000 network operating system, visit our World Wide Web site at <http://www.microsoft.com/windows/server/> and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows2000 Beta 3, visit 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 by way of 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 Windows 2000 Beta 3 distribution media for some of the known issues.