Certificate Request Generation and Certificate Installation Instructions for IIS 5

April 14, 2006

1. Generating the Certificate Request

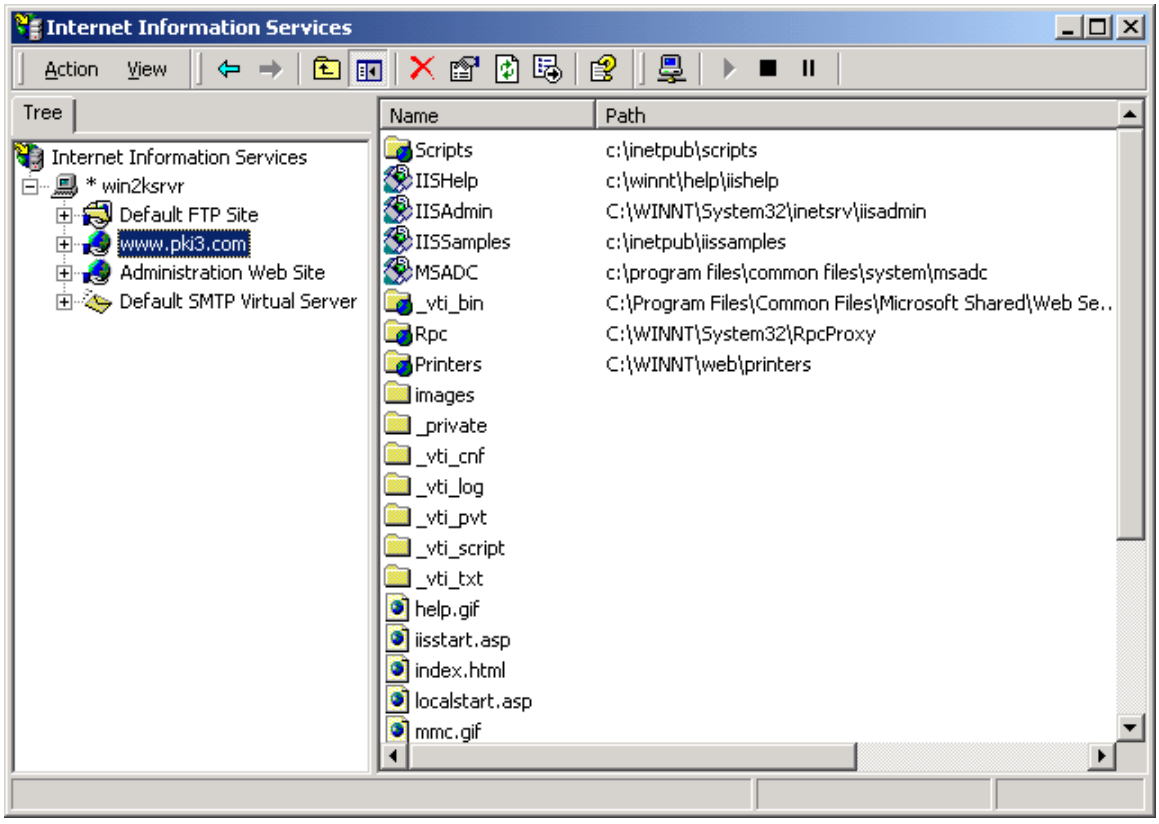
In this procedure, you will use the Internet Information Services (IIS) Console to generate a public and private key pair to support Secure Sockets Layer (SSL) encryption services. You will also generate the Public Key Cryptography Standard (PKCS) #10 certificate request and prepare it for submission to the Operational Research Consultants (ORC) External Certificate Authority (ECA).

1.1 Start the Internet Information Services Console

Click the **Start** button, point at **Programs**, and then point at **Administrative Tools**. From the submenu, click **Internet Services Manager**. The *Internet Information Services Microsoft Management Console* (MMC) displays.

1.2 Expand the Server

Figure 1-1. The Internet Information Microsoft Management Console

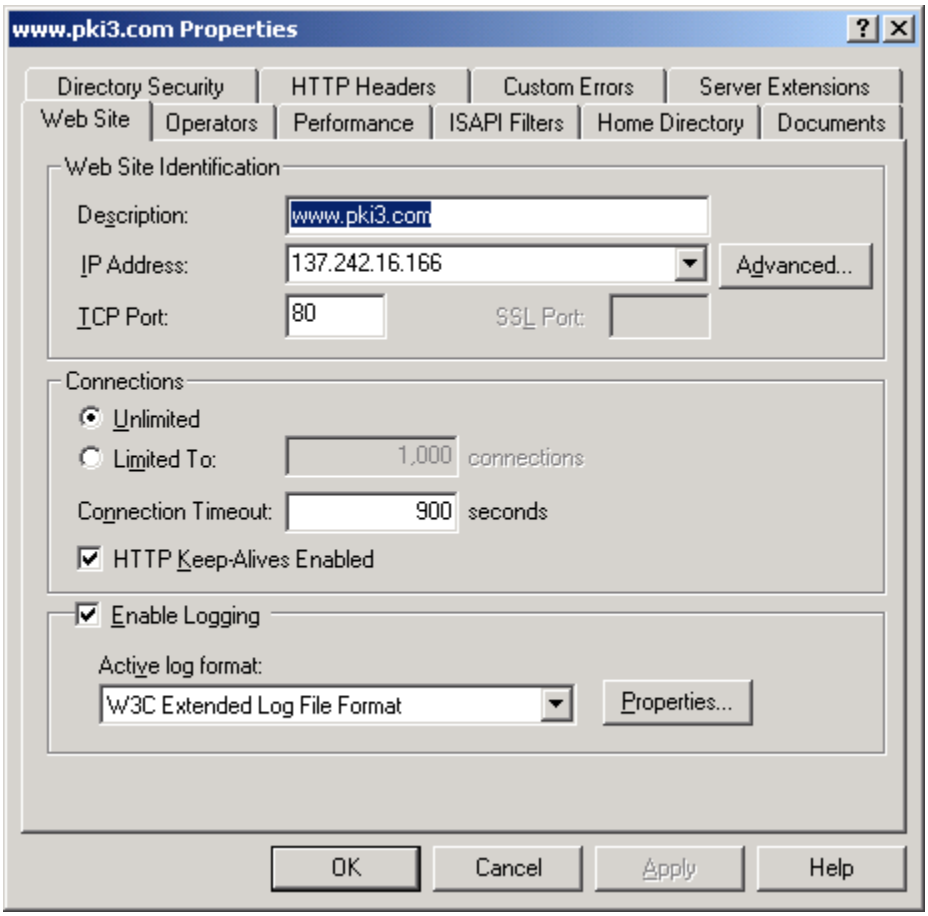


In the Console tree (the left panel), expand * *your server name.*

1.3 Open the Properties Dialog Box

Click the desired Web site. Right click the desired Web site and from the shortcut menu, click **Properties**. Alternately, click the **Action** menu and then click **Properties**. The **Administration Web Site Properties** dialog box appears.

Figure 1-2. The Internet Information Management Console

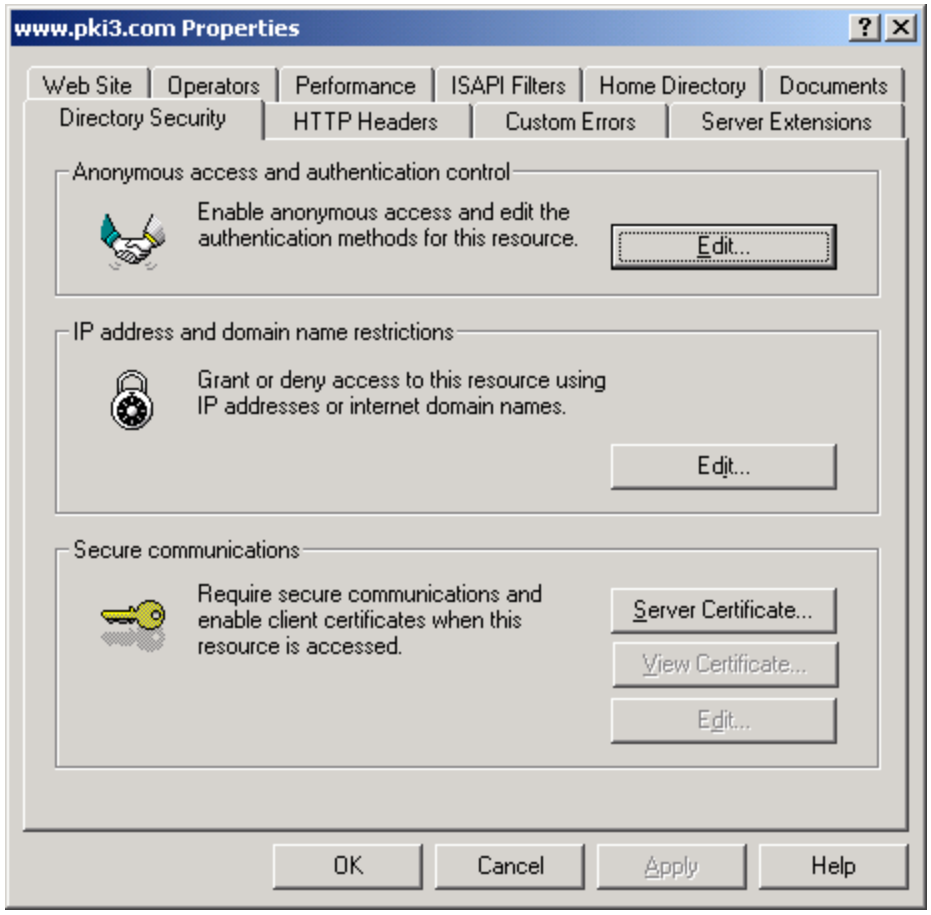


Note: The SSL Port number may not be available at this time. If it is available to be set, then assign the SSL Port to **443**. This is the default port used for SSL communication.

1.4 Access the Directory Security Tab

Click the **Directory Security** tab. Under **Secure communications**, click **Server Certificate**.

Figure 1-3. The Directory Security Tab



1.5 The Welcome to the Web Server Certificate Screen

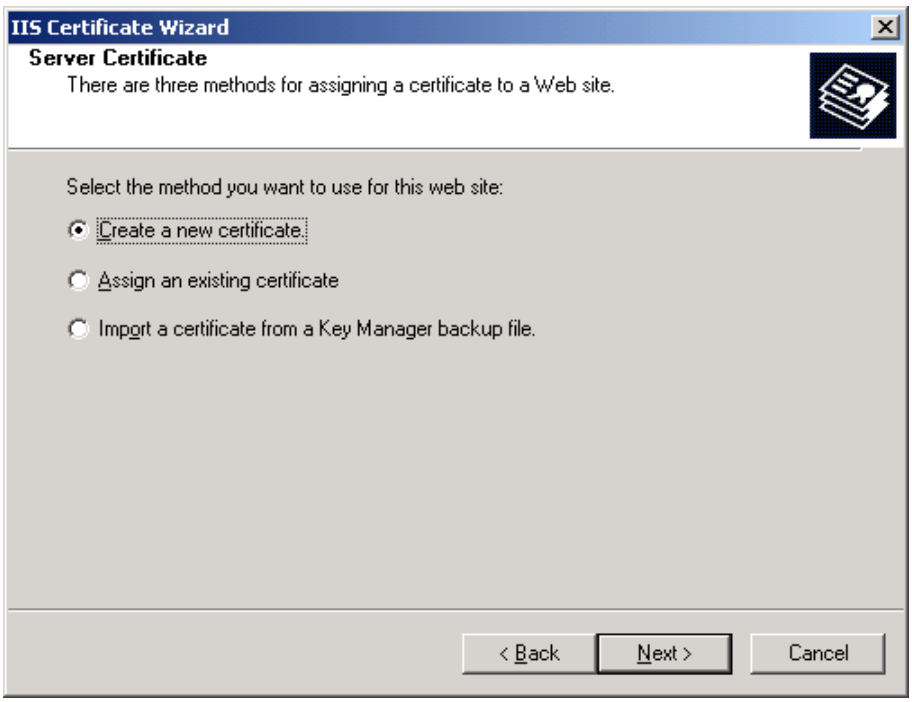
The **Welcome to the Web Server Certificate** wizard appears. Read the information and then click **Next**.

Figure 1-4. The Welcome to the Web Server Certificate Screen

1.6 The IIS Certificate Wizard Screen

The **IIS Certificate** wizard appears. Confirm that the **Create a New Certificate** button is selected and then click **Next**.

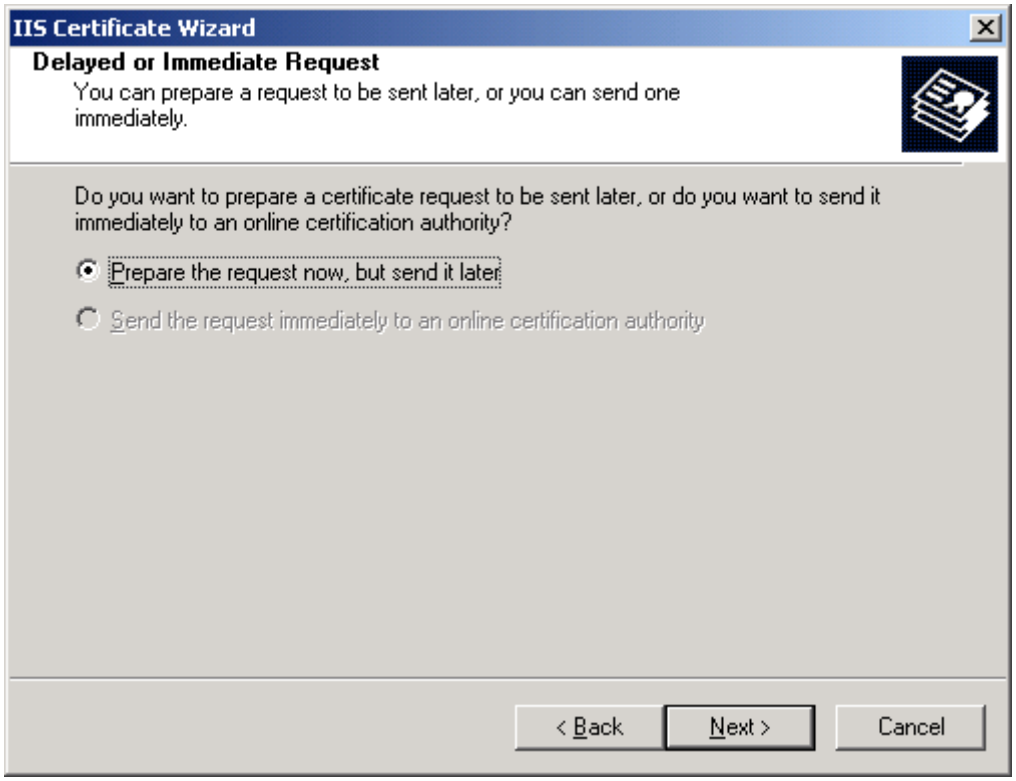
Figure 1-5. The Create a New Certificate Screen



1.7 The Delayed or Immediate Request Screen

The **Delayed or Immediate Request** screen appears.

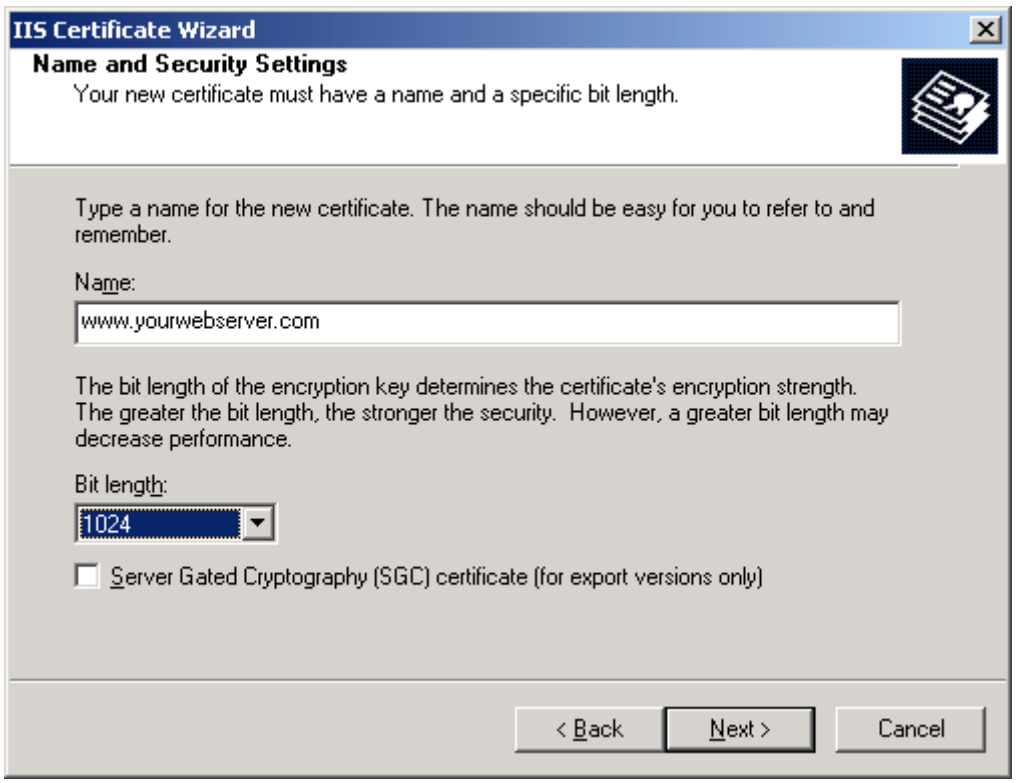
Figure 1-6. The Delayed or Immediate Request Screen



Click the **Prepare the request now, but send it later** button and then click **Next**. The **Name and Security Settings** screen appears.

1.8 The Name and Security Settings Screen

Figure 1-7. The Name and Security Settings Screen



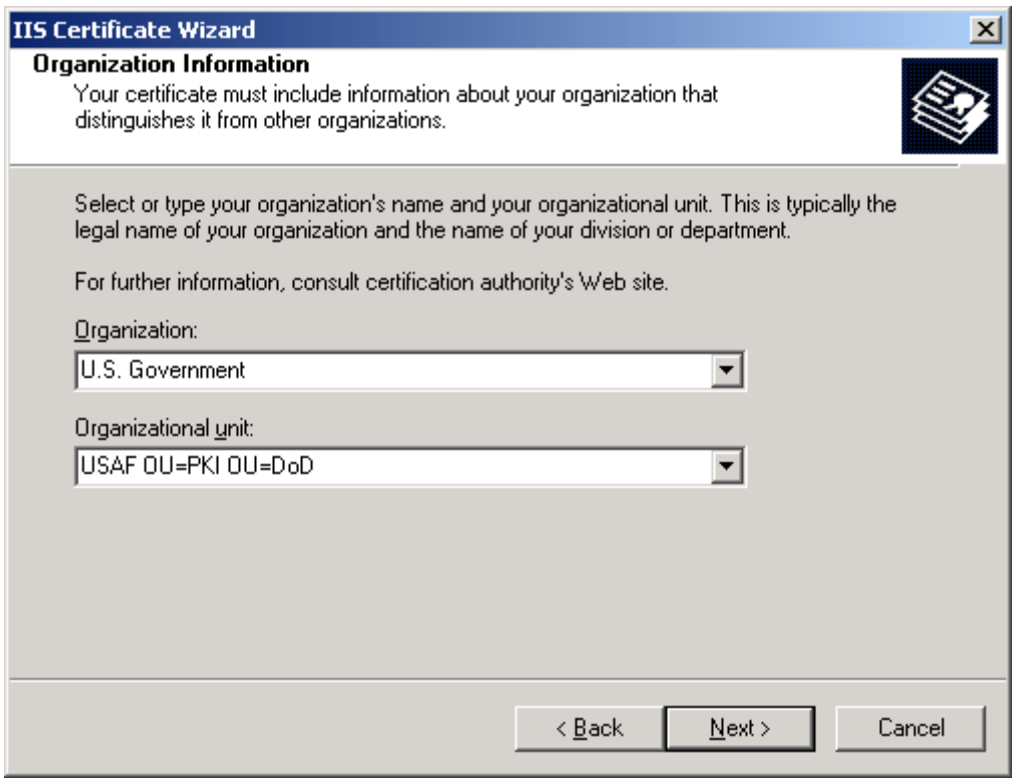
Note: The default name given to this certificate is the name of the Web site that was selected, and the bit length is set to 512.

Click the **Bit Length** arrow and select **1024** for the bit length. Click **Next**. The **Organization Information** screen appears.

1.9 The Organization Information Screen

In the **Organization** box, type **U.S. Government,** and in the **Organizational Unit** box, type **<Your Company Name>, OU=ORC OU=ECA**.

Figure 1-8. The Organization Information Screen



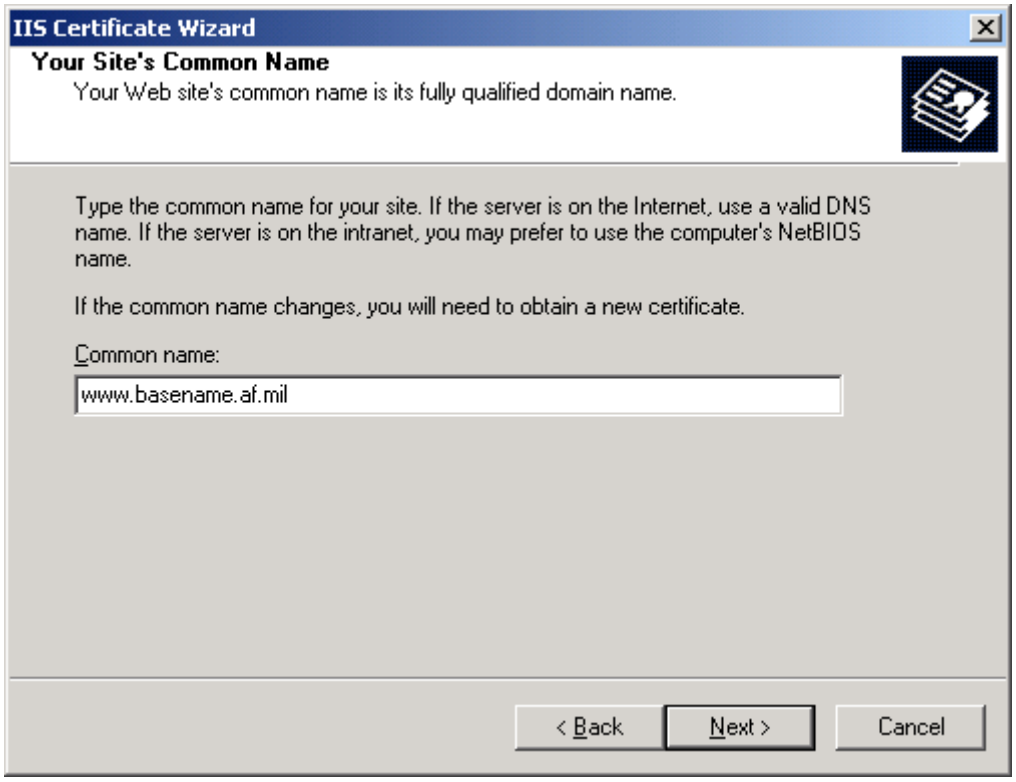
Click **Next**. The **Your Site's Common Name** screen appears.

Note: The text is case-sensitive. There is a space after the letters **U.S.** and the word **Government**. There is also a space after your company name and the letters **OU=ORC**. There is another space after the letters **ORC** and the letters **OU=ECA**.

1.10 The Your Site's Common Name Screen

In the **Common Name** text box, type the domain name of your Web site, for example, *www.testcompany.com* and then click **Next**. The **Common Name** is the Fully Qualified Domain Name (FQDN) of the server that the certificate will be installed on (e.g. *www.testcompany.com*).

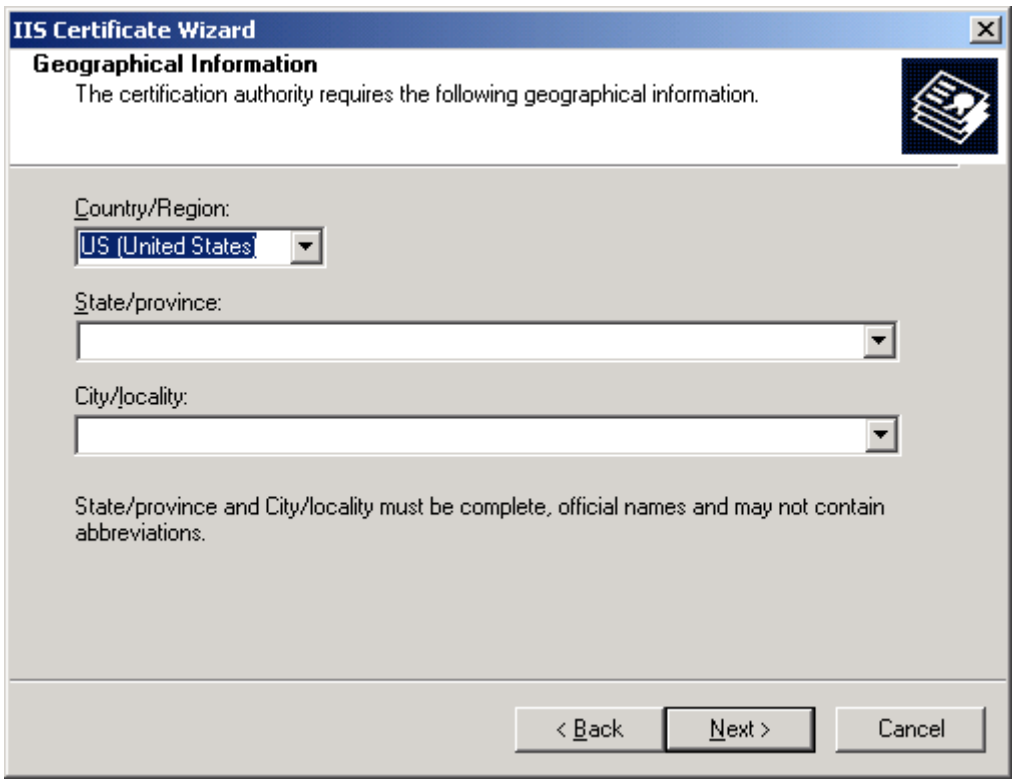
Figure 1-9. The Your Site's Common Name Screen



Click **Next** to display the **Geographical Information** screen.

1.11 The Geographic Information Screen

Figure 1-10. The Geographical Information Screen



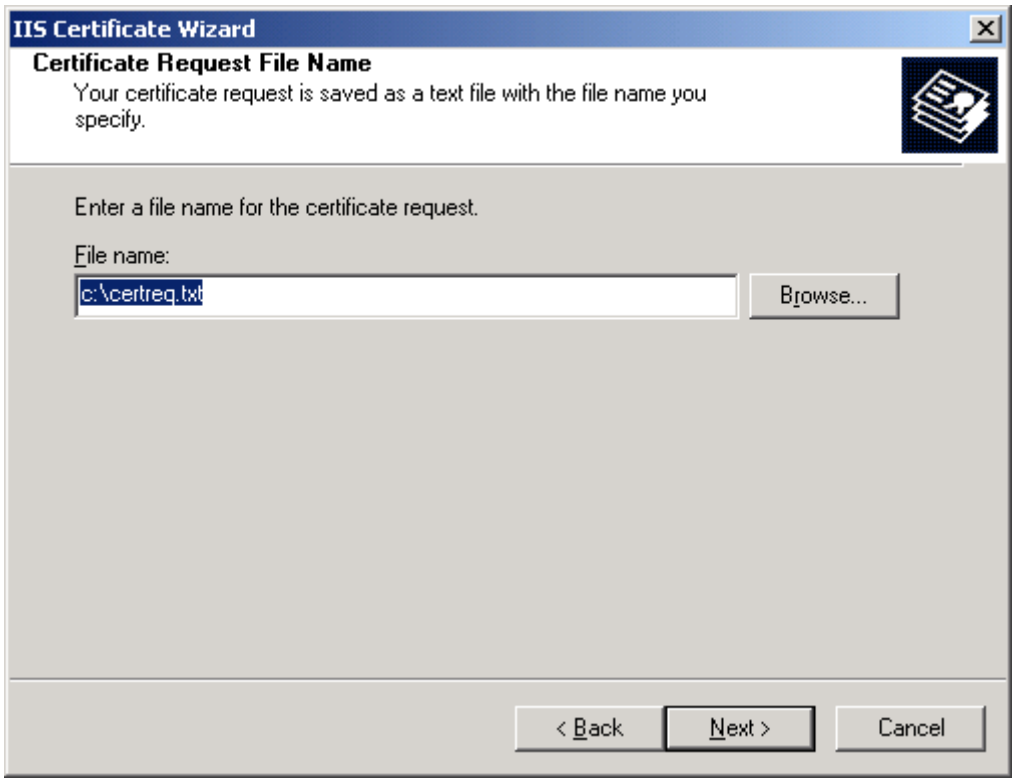
Type the following information in the appropriate text boxes.

- In the **Country/Region** box, type **US** (United States). Normally, this does not need to be changed.
- In the **State/province** box, press **Spacebar**. To move to the **City/locality** field, press **TAB** or click the **City/locality** box.
- In the **City/locality** box, press **Spacebar**.
- Click **Next**. The **Certificate Request File Name** screen appears.

1.12 The Certificate Request File Name

In the **File name** box, enter a file name. Remember the folder where the file is saved. You may also click **Browse** to locate the desired folder. The file name should have a **.txt** extension and is saved in a text format. Click **Next.**

Figure 1-11. The Certificate Request File Name Screen

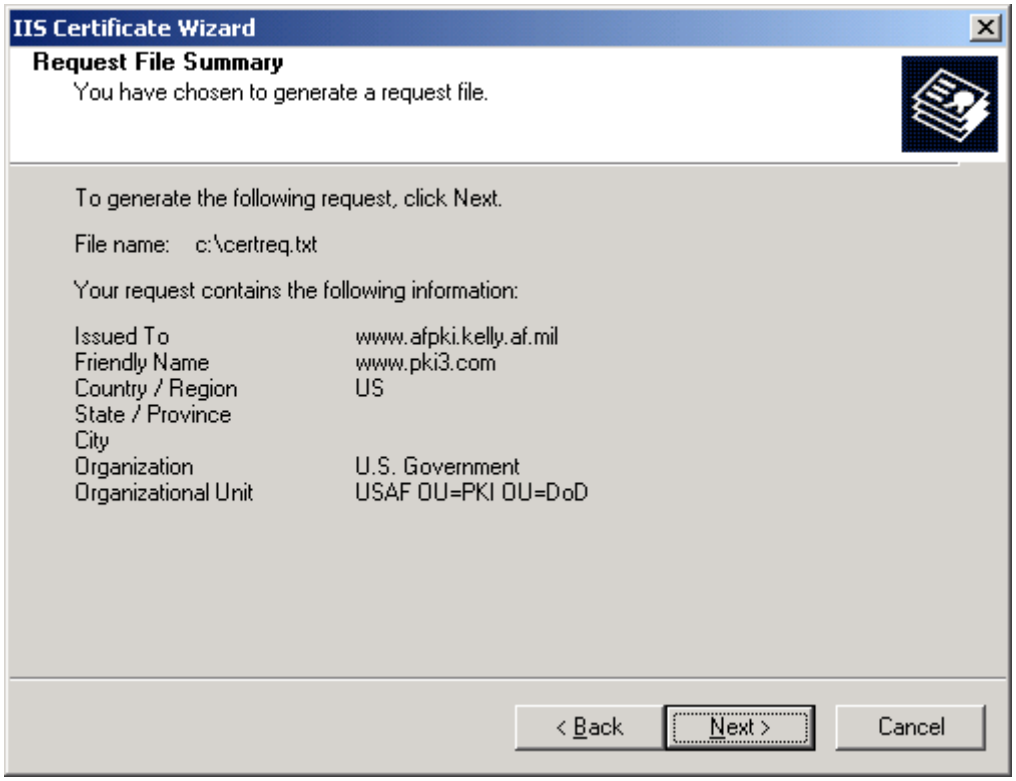


1.13 The Request File Summary Screen

After a few moments, the **Request File Summary** screen appears. Read through the summary information on the screen.

- If changes need to be made, click **Back** as many screens as necessary to make changes.
- After making the changes, click **Next** as many times as needed to get back to this screen.
- Click **Next** to display the **Completing the Web Certificate Wizard** screen.

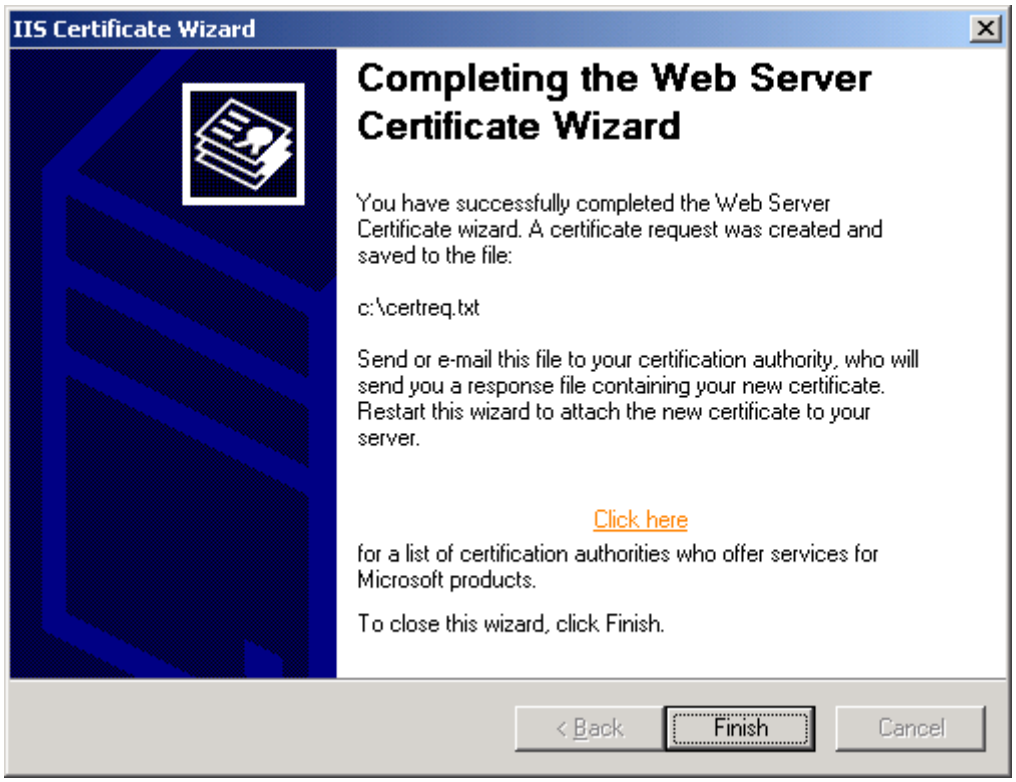
Figure 1-12. The Request File Summary Screen



1.14 The Completing the Web Server Certificate Wizard Screen

The screen informs you that the certificate request has been successfully completed. This screen displays the file folder and the file name of the certificate request. Click **Finish**.

Figure 1-13. The Completing the Web Server Certificate Wizard Screen



1.15 What's Next

At this point, you will use your Web browser to communicate with the *Certificate Authority* server to submit your certificate request. You will need to open **Windows Notepad** to copy and paste information from the clipboard during this operation.

2. Installing the Certificate in IIS5

In this section, you will install the certificate you retrieved (as per the notification email) to the *Microsoft IIS5* Web server. If you have not yet received your notification email do not attempt to perform these steps. You will need to start the **Internet Service Manager**.

Note: In this example, SSL is applied to the *Default Web Site*, which is the default Web site installed by *Windows NT/ IIS5*.

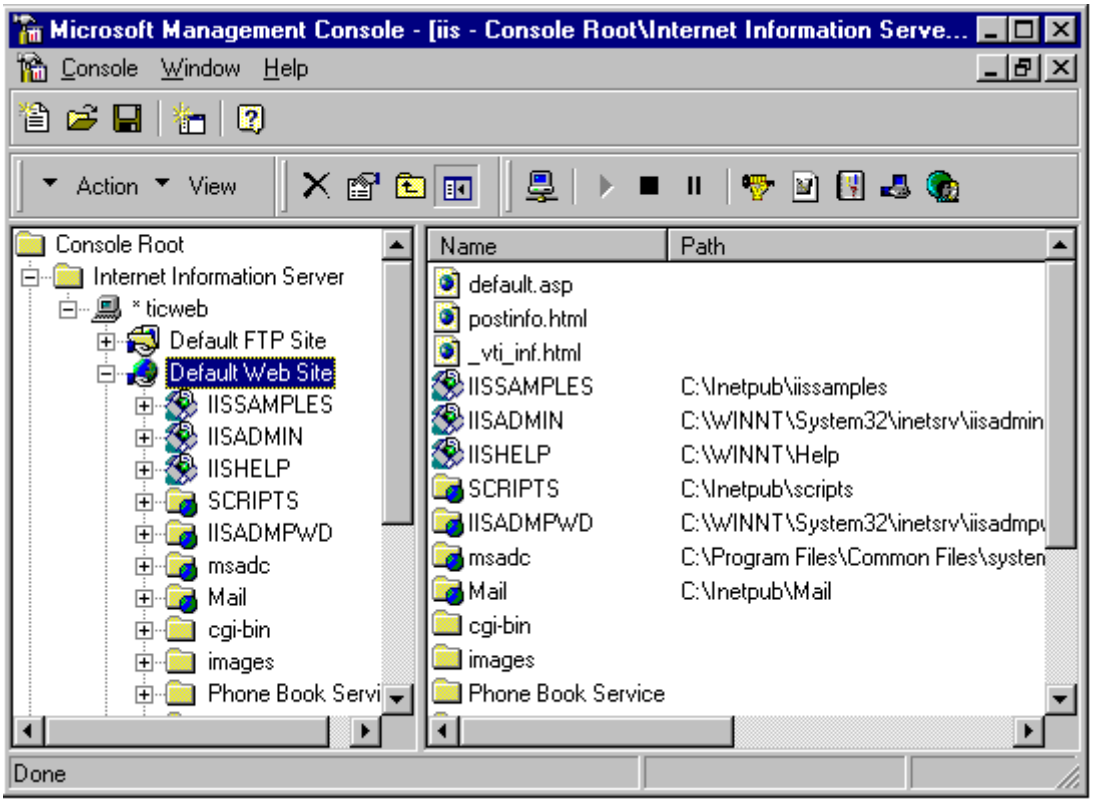
2.1 Start the Internet Information Service Manager

Click the **Start** button, point at **Programs**, and then point at **Administrative Tools**. From the submenu, click **Internet Services Manager**. The *Internet Information Services Microsoft Management Console* (MMC) displays.

2.2 Expand the Server

In the Console tree (the left panel), expand * *your Web server name.*

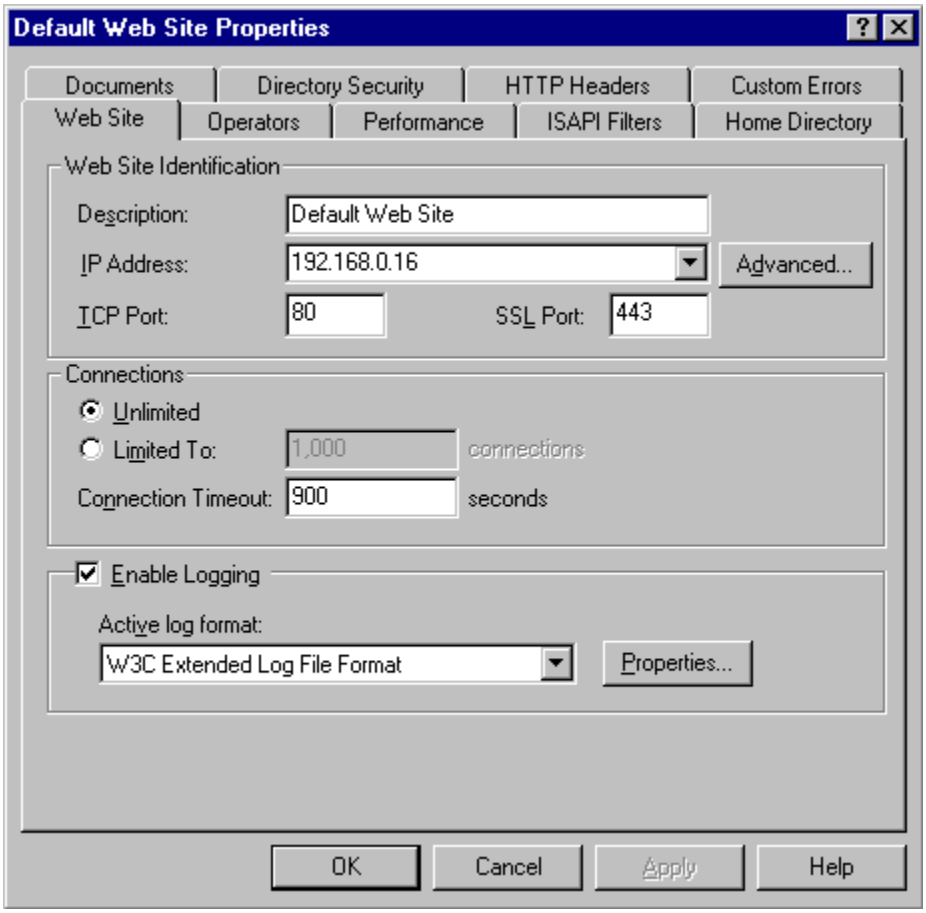
Figure 4-1. The Internet Information Microsoft Management Console



2.3 Open the Properties Dialog Box

Right click the desired Web site and from the shortcut menu, click **Properties**. The selected **Web Site Properties** dialog box appears. Set the SSL Port to the number **443**.

Figure 4-2. The Website Properties Screen



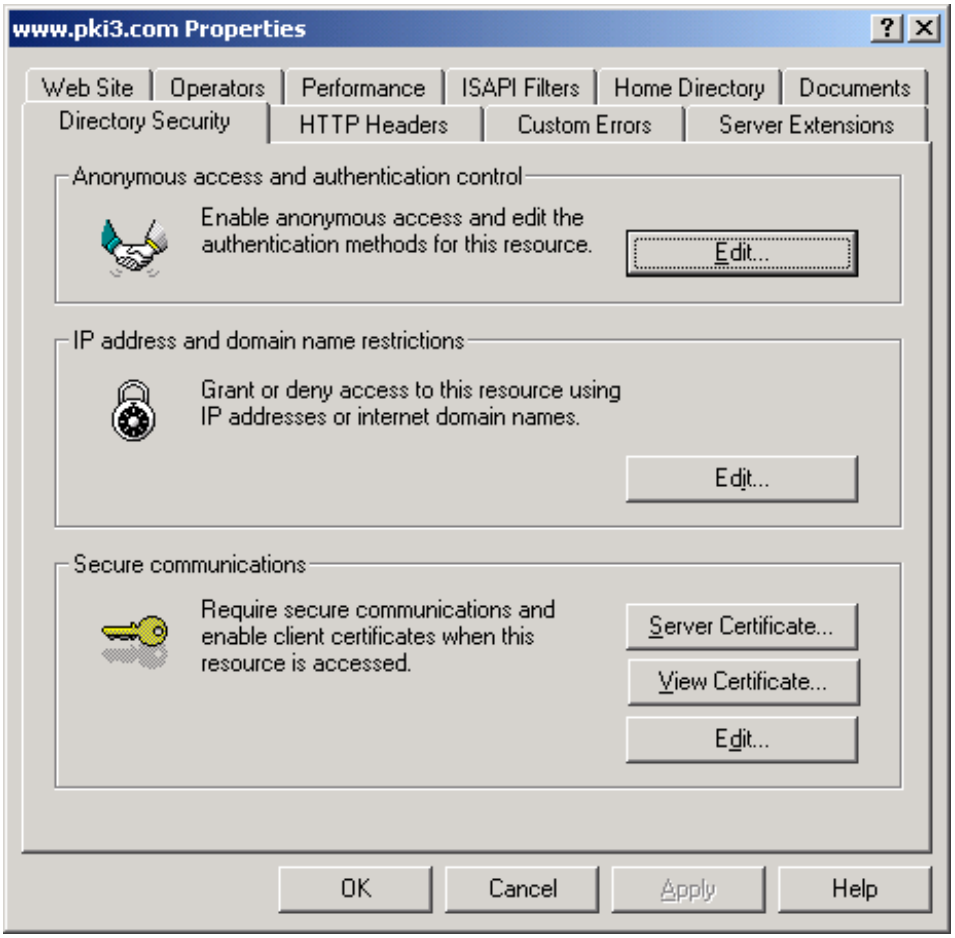
Note: The SSL port is shown as 443, which is the default port for SSL function. This block may be grayed out if no certificate has ever been installed on this Web site. If so, you must return to this screen after the certificate is installed and set the SSL port to 443. Failure to do so will deny you access to your Web site when you turn SSL on.

2.4 Access the Directory Security Tab

Click the **Directory Security** tab

In the **Secure communications** section, click **Server Certificate**. This will display the **Welcome to the Web Server Certificate Wizard**.

Figure 4-3. The Directory Security Tab



2.5 Initialize the Web Server Certificate Wizard

Click **Next** to display the **Pending Certificate Request** screen.

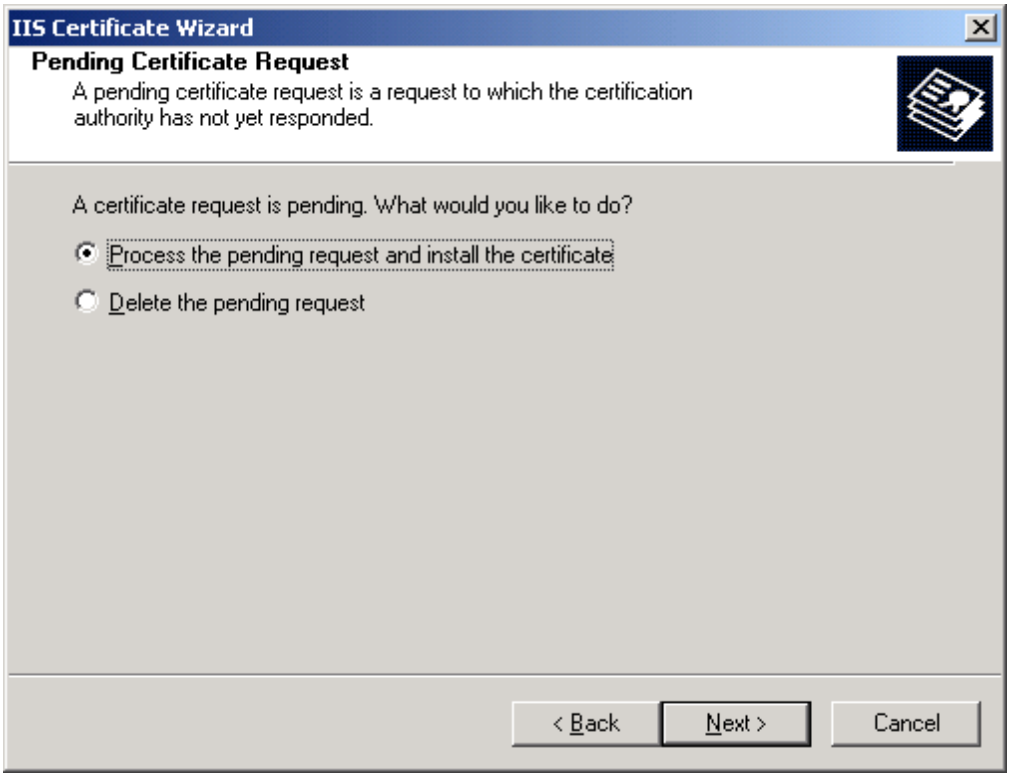
Figure 4-4. The Welcome to the Web Server Certificate Wizard Screen

2.6 The Pending Certificate Request Screen

Select **Process the pending request and install the certificate**.

Click Next

Figure 4-5. The Pending Certificate Request Screen

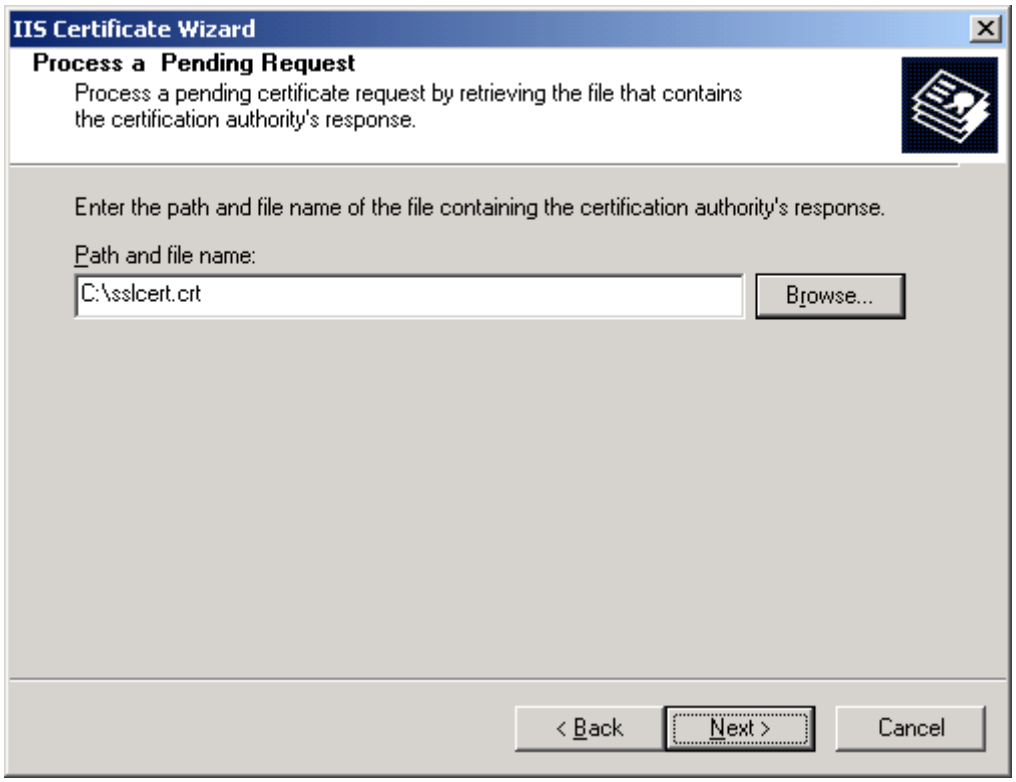


Click **Next** to display the **Process a Pending Request** screen.

2.7 The Process a Pending Request screen

Enter the file name and path of the certificate you saved in the previous section. Or, you may click **Browse** to find the certificate.

Figure 4-6. The Process a Pending Request Screen

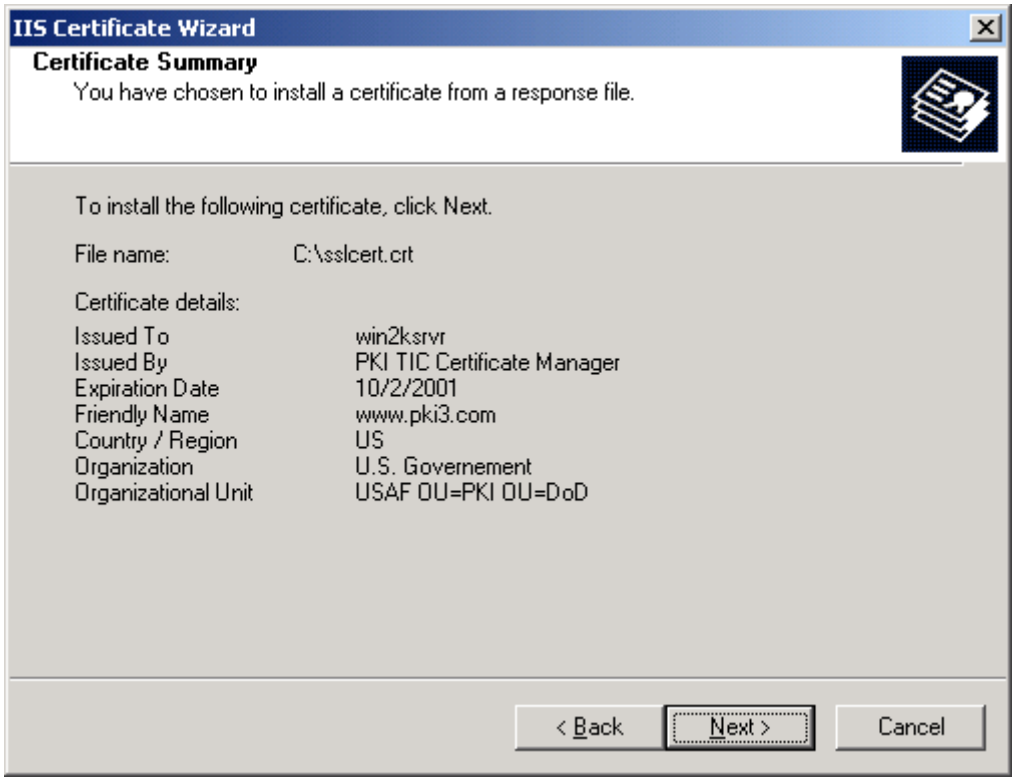


Click **Next** to display the **Certificate Summary** screen.

2.8 The Certificate Summary Screen

Read the information contained in this screen and then click **Next**.

Figure 4-7. The Certificate Summary Screen



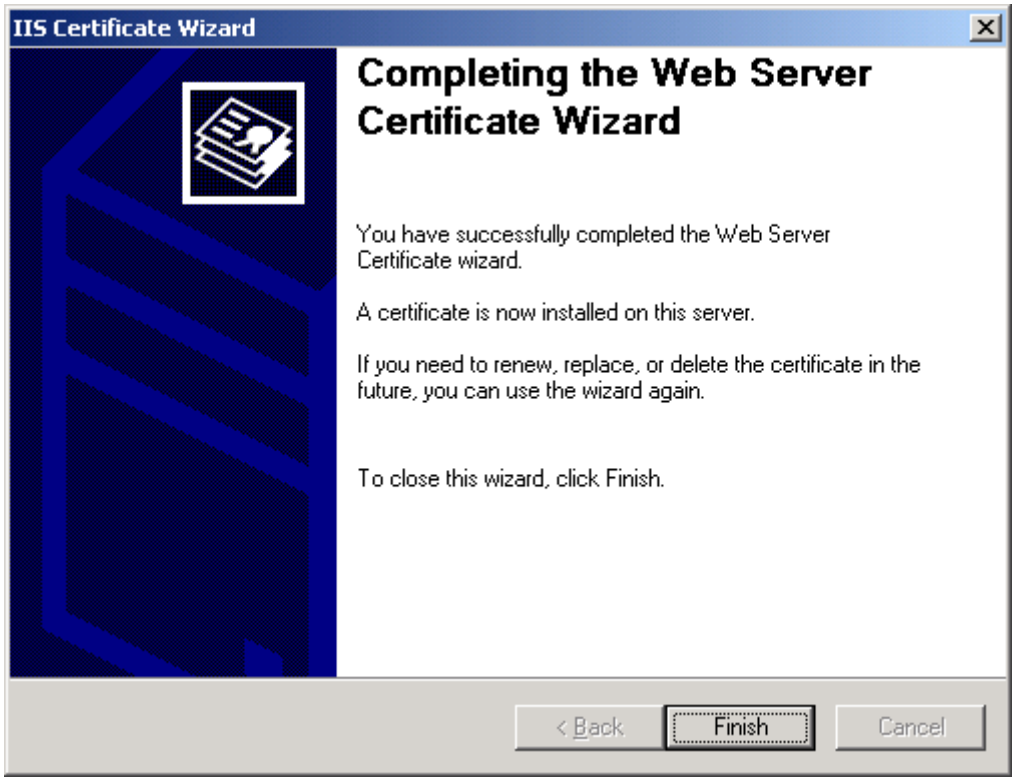
Note: If changes need to be made, click **Back** as many screens as needed and make the necessary changes. Click **Next** as many times as needed to return to this screen.

This will display the **Completing the Web Server Certificate Wizard** screen.

2.9 The Completing the Web Server Certificate Wizard Screen

Click **Finish** to return to the **Directory Security** tab.

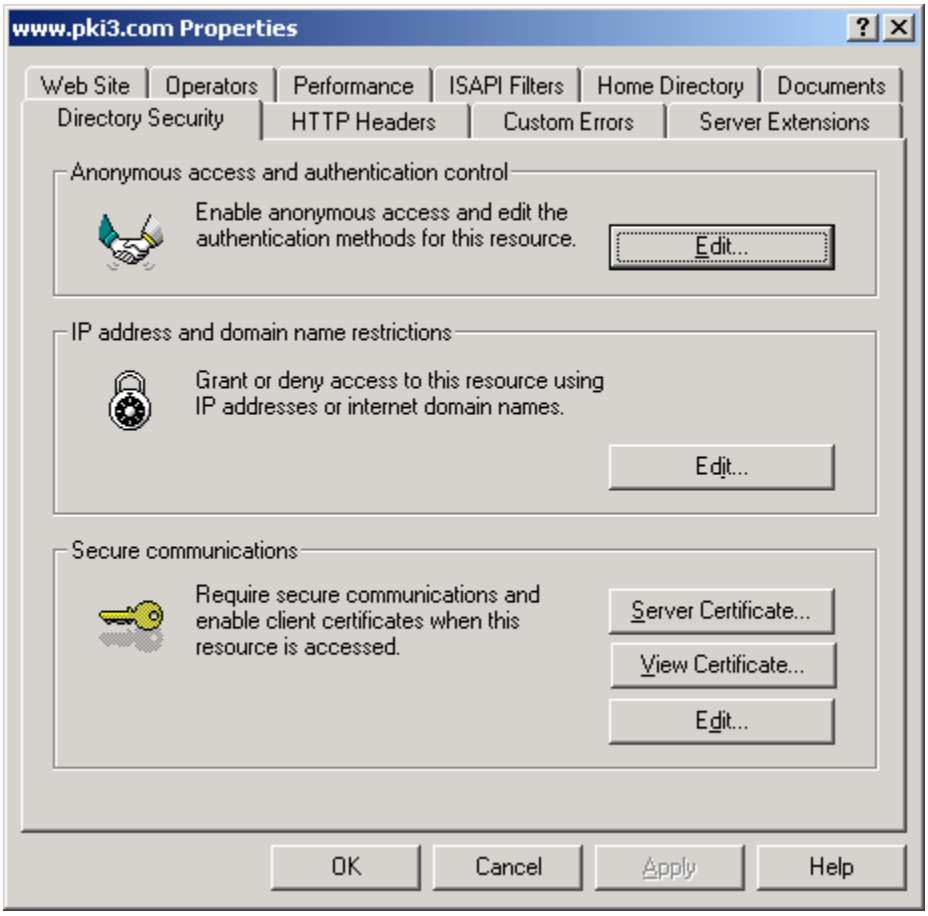
Figure 4-8. The Completing the Web Server Certificate Wizard Screen



Notice that under the **Secure communications** section, the **View Certificate** and **Edit** buttons are now available.

2.10 The Edit Secure Communications Screen

Figure 4-9. The Directory Security Tab After Processing a Certificate Request



In the **Secure communications** section, click the **Edit** button. The **Secure Communications** dialog box appears.

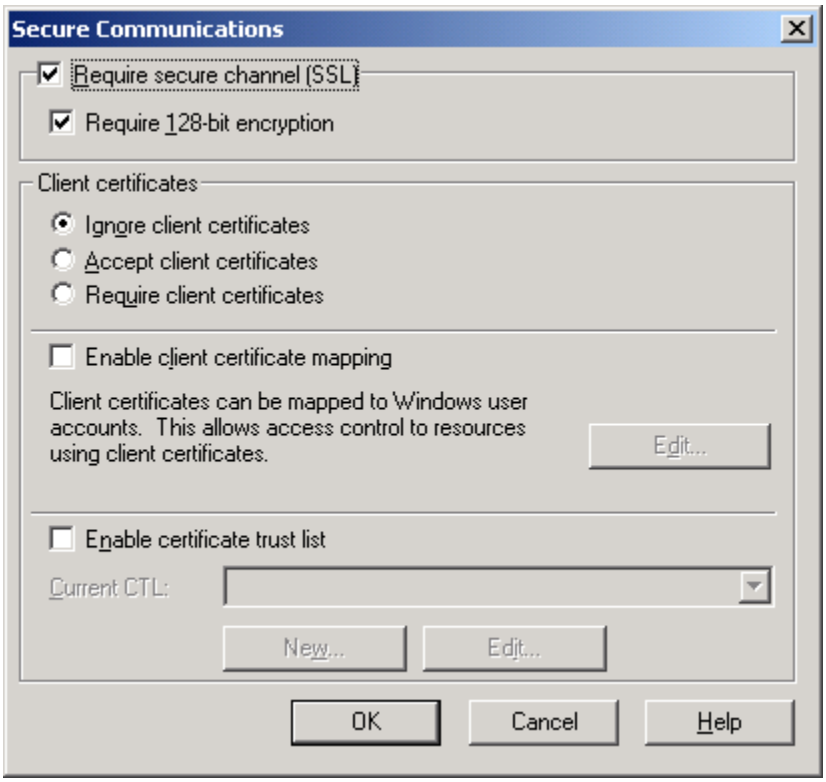
2.11 Enabling SSL Communications

- Click the **Require Secure Channel (SSL)** box.
- Click **Require 128-bit encryption**.

Note: Depending on your requirement you may need to require client certificates. Only select this option if you wish to restrict access to your web server to clients who have their own Identity Certificates.

- Click **OK** to return to the Web site properties screen.

Figure 4-10. The Secure Communications Screen

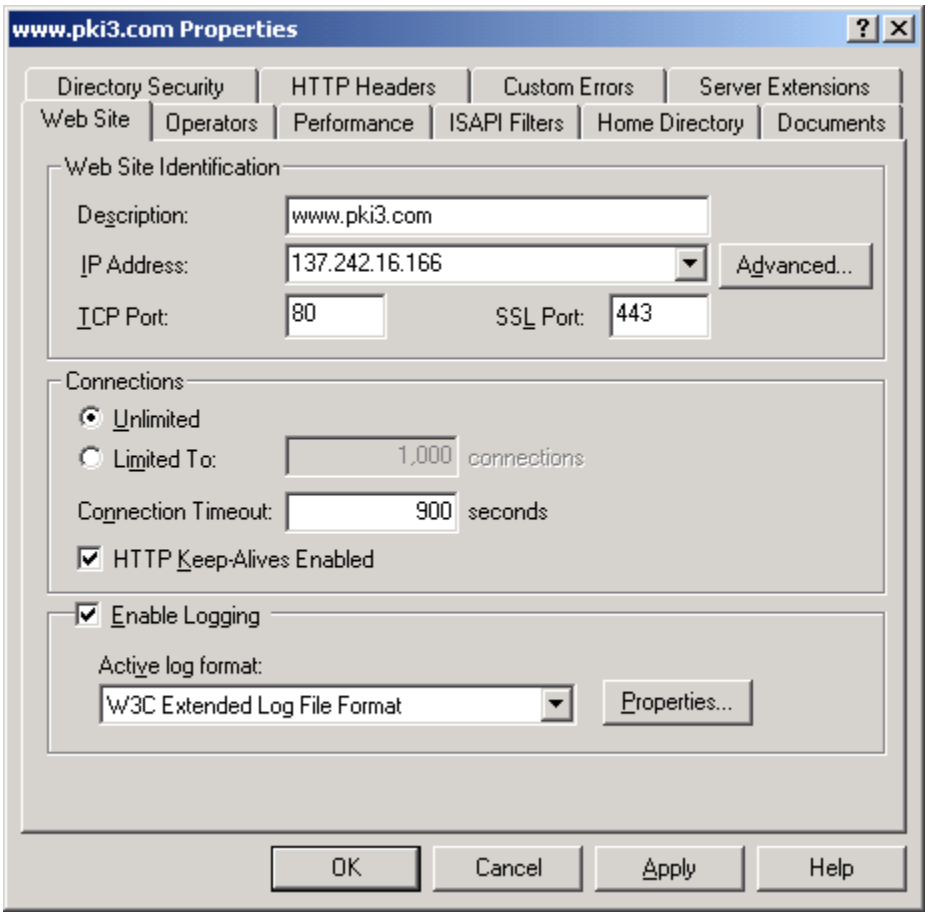


Note: The DoD PKI and by extension the ECA PKI requires that 128-bit encryption algorithms be used.

2.12 Setting the SSL Properties

On the **Administration Web Site Properties** dialog box, click the **Web Site** tab. In the **SSL Port** field, make sure the number **443** is displayed. If not present, enter 443. This is the default port number for SSL communications.

Figure 4-11. Assigning the SSL Port Screen



Click **OK**. Close the *Internet Information Manager* and save all settings.

At this point, the Web server is SSL enabled.

3. Obtaining and installing the ECA Root Certificate Chain

3.1 Trusted CA installation using the Windows Certificate Manager Import Wizard.

Note: Use this process only if procedure at section 5.1 does not work OR you simply prefer this method in lieu of section 5.1

Step 1. Download the Base 64 encoded certificate chain from the following URL:
https://afpki.lackland.af.mil/assets/files/DoDcert_chainB64.zip

This file contains the DoD Class 3 Root and all the appropriate Intermediate CAs. It is updated as new CAs are added to the infrastructure.

Step 2. Use WinZIP to extract the Base 64 encoded certificate files.

The current list of CAs in the DoD PKI Trust Chain can be found at:
https://afpki.lackland.af.mil/html/rootchaininstallation.asp

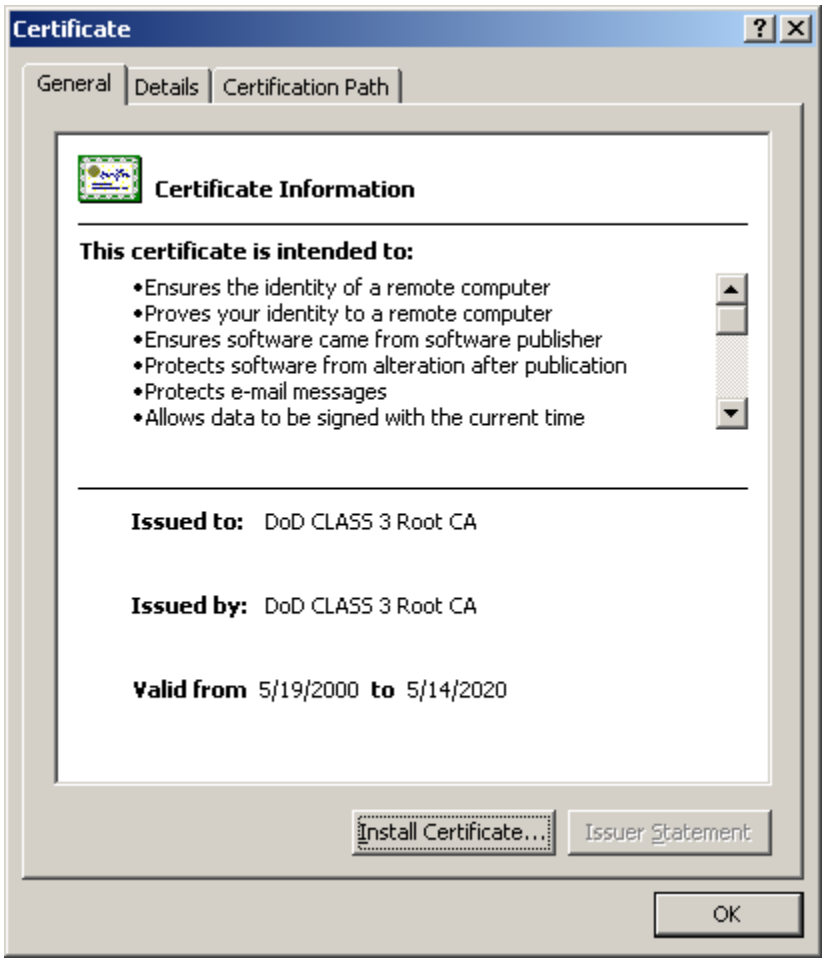
- Certificates identified as Root are installed as Trusted Root Certification Authorities in the Web server.
- Certificates identified with numbers such as CA-5, EMAIL CA-5, etc. are installed as Intermediate or Chaining CAs
- All certificates are placed in the Local Computer store to make them usable by all processes and users running on the computer.

Step 3. Start *Windows Explorer* and locate the Class3_Root_B64.cer file.

Note: This process must be performed as the Administrator.

Step 4. Double click on the .cer file to start the **Microsoft Certificate Wizard** process

Figure 5-1. The Certificate Information Screen



Click **Install Certificate** to display the **Certificate Manager Import Wizard**.

Step 5. The Certificate Import Wizard Screen

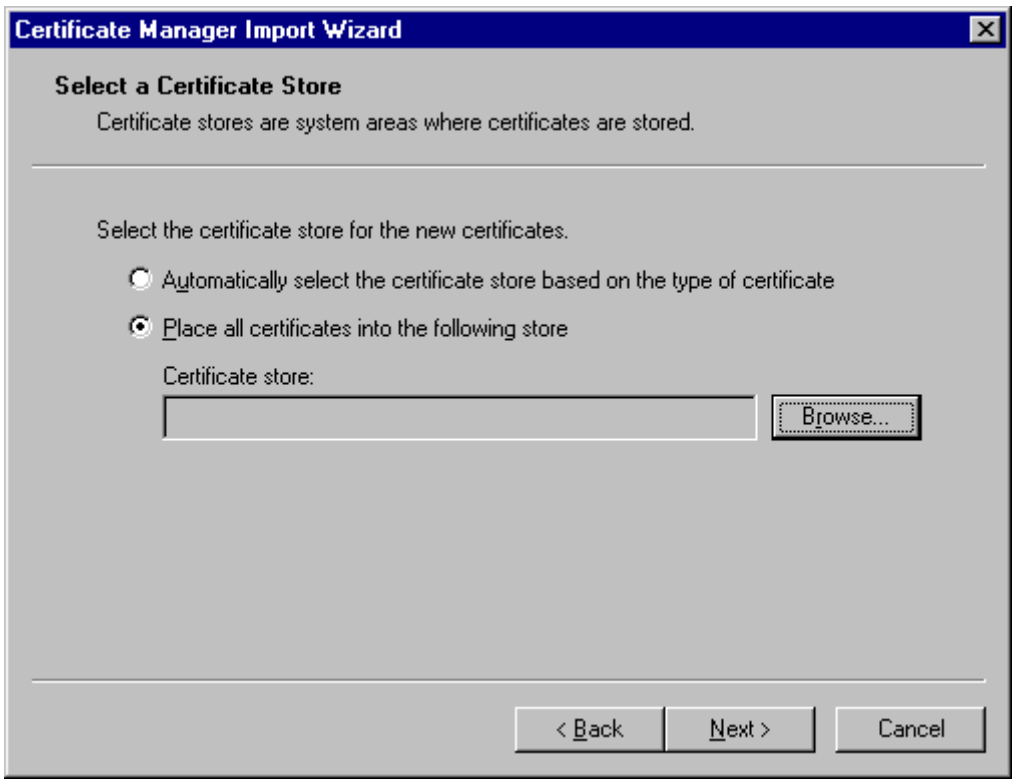
Figure 5-2. The Welcome to the Certificate Manager Import Wizard Screen

After reading the information on this screen, click **Next** to display the **Select the Certificate Store** screen.

Step 6. Select the Certificate Store Screen

Click **Place all certificates into the following store** and then click **Browse** to display the **Select a Certificate Store** screen.

Figure 5-3. The Select a Certificate Store Screen



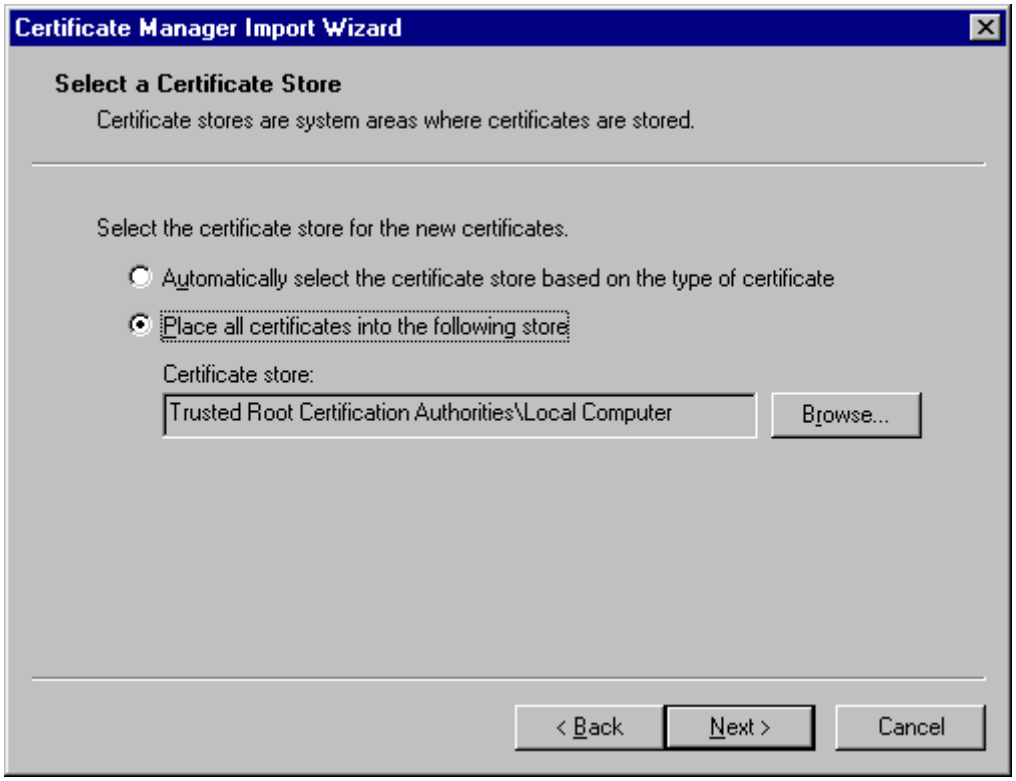
- Select Trusted Root Certification Authorities / local computer for ROOT CA only.
- Select Intermediate Certificate Authorities / local computer for all other certificates such as CA-5, EMAIL CA-5, CA-6, EMAIL CA-6 etc.

Step 7. Select the Certificate Store Screen

Figure 5-4. The Select Certificate Store Screen

Click to place a checkmark in the **Show Physical Stores** box and expand the **Trusted Root Certification Authorities** list as shown and click **Local Computer**. Click **OK** to return to the **Select a Certificate Store** screen. The screen should look like the following:

Figure 5-5. The Select a Certificate Store after Selecting the Local Computer



Click **Next** to display the **Completing the Certificate Wizard Import** screen.

Step 8. Completing the Certificate Wizard Import Screen

Click **Finish** to complete the import process.

Figure 5-6. The Completing the Certificate Manager Import Wizard Screen

You will see the **Certificate Manager Import Wizard** confirmation screen reporting that the import process was successful. Click **OK**.

Figure 5-7. The Import Successful Screen

Note: You must repeat this process (Steps 4 through 8) for the remaining Certificate Authority Certificates identified in Step 2

After all certificates have been installed, the server must be shut down and restarted.

This completes the installation process for the server.

4. Installing the DoD Root Certificate Chain in the Browser

All prospective users of your SSL-enabled Web site must accept the **DoD PKI Root Certificate Chain** in their browsers. These browsers must be U.S. High Encryption-capable (128-bit).

4.1 Using Internet Explorer

If you are using Microsoft Internet Explorer, you may install the root certificate chain by using the executable file found at https://afpki.lackland.af.mil/html/rootchaininstallation.asp . This file may also be used for pushing the root certificate chain out across the entire domain using tools such as System Management Server (SMS).

4.2 Using Netscape Communicator

If you use a *Netscape* browser (4.06 or newer), follow the directions at https://afpki.lackland.af.mil/html/import_netscape.asp

Appendix A

Acronyms

CA	Certificate Authority
COMSEC	Communications Security
CRL	Certificate Revocation Lists
DoD	Department of Defense
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
IA	Information Assurance
ID	Identification
IIS	Internet Information Services
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authority
MMC	Microsoft Management Console
NIPRNet	Non-Classified Internet Protocol Router Network
OS	Operating System
OU	Organizational Unit
PKCS	Public Key Cryptography Standard
PKE	Public Key Enabling
PKI	Public Key Infrastructure
RA	Registration Authority
SIPRNet	Secret Internet Protocol Network
SMS	System Management Server
SPO	System Program Office
SSL	Secure Sockets Layer

TA	Trusted Agent
URL	Uniform Resource Locator
USAF	United States Air Force