PROTECTID

Client Authenticated SSL Server Setup Guide for Microsoft Windows IIS

Document:
MK-UM-01180405-01-ProtectIDclientAuthSSLsetupIIS.doc

SENTRY PM

Trademarks: Microsoft and Windows, Windows 95, Windows NT, Windows 98, Windows 2000, Windows Me and Windows XP are registered trademarks of Microsoft Corporation. Netscape, Netscape Communicator and Netscape Messenger are registered trademarks of Netscape Communications Corporation. Novell Groupwise is a registered trademark of Novell Inc. **protectID** is a registered trademark of Sentry Project Management Pty Ltd.

Before you use the protectID product, you must agree to the following terms.

Any use or distribution of the protectID product requires that either you or your supplier have a licence from Sentry Project Management Pty Ltd. Please contact your supplier or support@sentrypm.com for details.

Neither Sentry Project Management nor any other person who has been involved in the creation, production, or delivery of the Software shall be liable to the user or to any other person for any direct, incidental or consequential damages, even if Sentry Project Management has been advised of the possibility of such damages.

Purpose

This document is intended to provide integration support for use of ProtectID smartcards or tokens (ref www.SENTRYpm.com) with client-authenticated SSL on Microsoft Windows IIS-based webservers.

This document describes setup of the IIS server and use of soft certificates at the client PC. Once this setup is complete and the website access is satisfactory, contact Sentry for further advice on installation of Sentry's protectID smartcard- and USB token-based certificates.

The following procedures assume general familiarity with Microsoft Windows systems.

1 Digital certificate client authentication on IIS 5.0 or later

This document assumed that IIS 5.0 or later has already been installed on your PC.

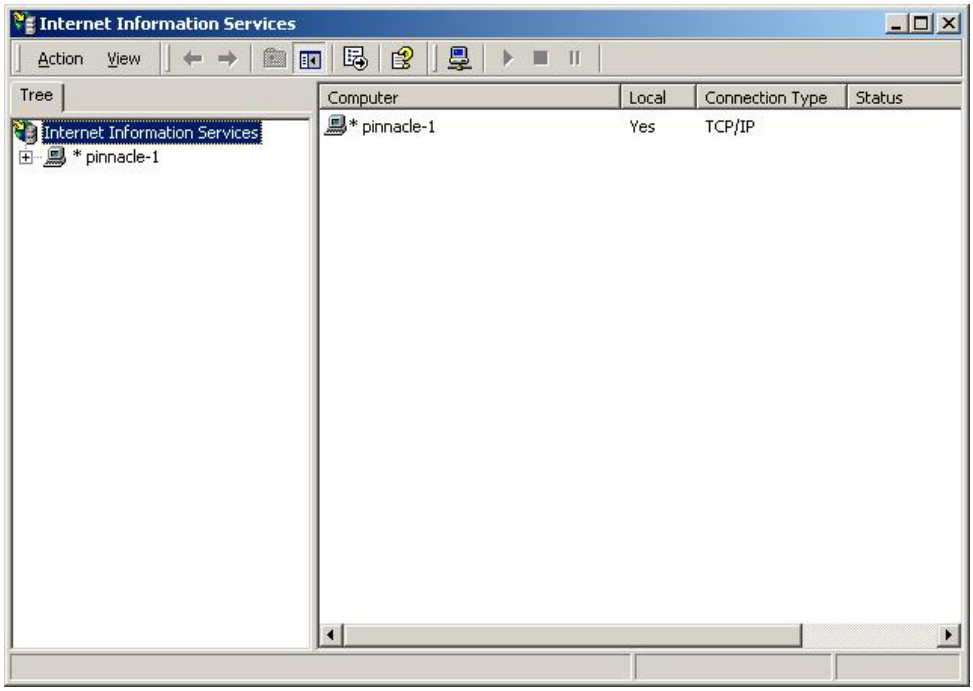
To setup a digital certificate based client authentication on IIS web-server follow the instructions below:

1. Generate a Server Certificate Request
2. Install a server certificate on IIS web-server. You may obtain the certificate from an external Certification Authority or generate one using your own CA[1].
3. Install the CA root certificate used to sign the server certificate.
4. Configure IIS to request a client certificate for authentication.
5. Obtain client certificates from an external CA or generate client certificates using your own CA.
6. Install a root CA certificate used to sign the client certificates.
7. Install user/client certificates on IE 6 web-browser.

Generate a Server Certificate Signing Request

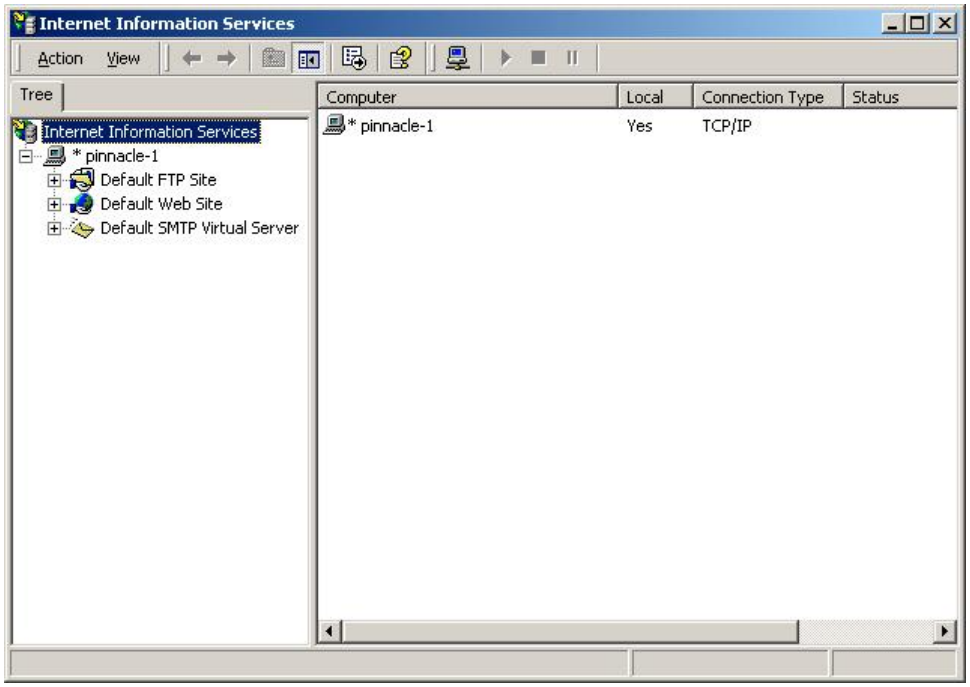
To generate a Server Certificate Signing Request follow the steps below:

1. Click **Start -> Settings** and click **Control Panel**.
2. Double click the **Administrative Tools** applet icon.
3. Double click the **Internet Services Manager**.

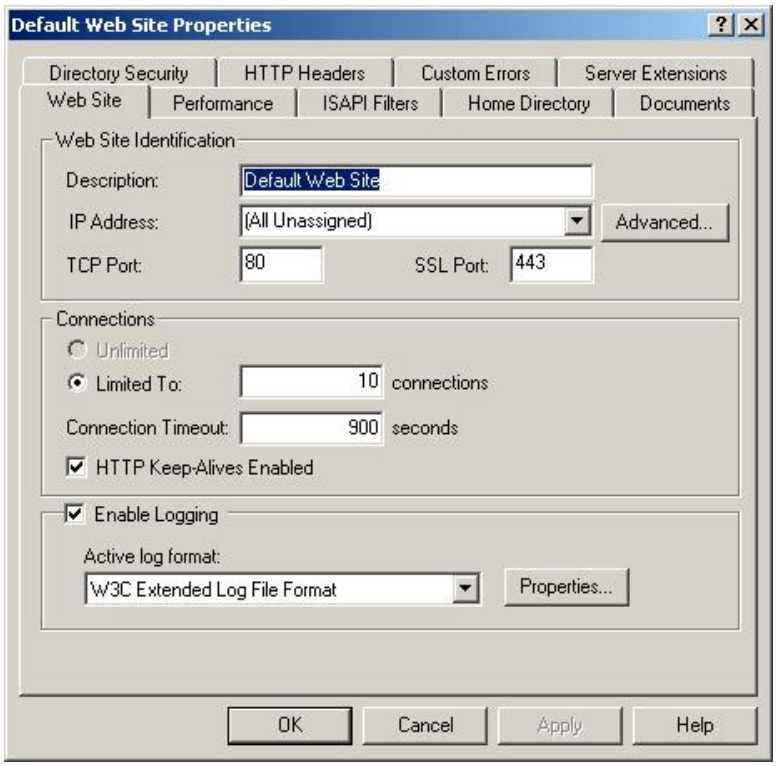


[1] To generate your own certificates you must have a machine with Microsoft Certificate Server installed.

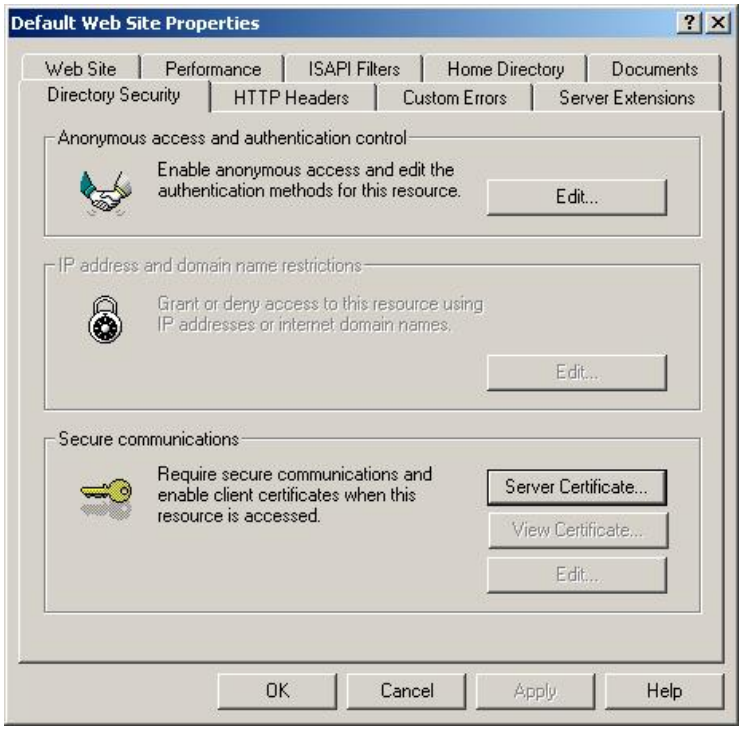
4. Expand your Host name. Right-click the **Default Web site** and then click **Properties**.



5. Click **Directory Security** tab.

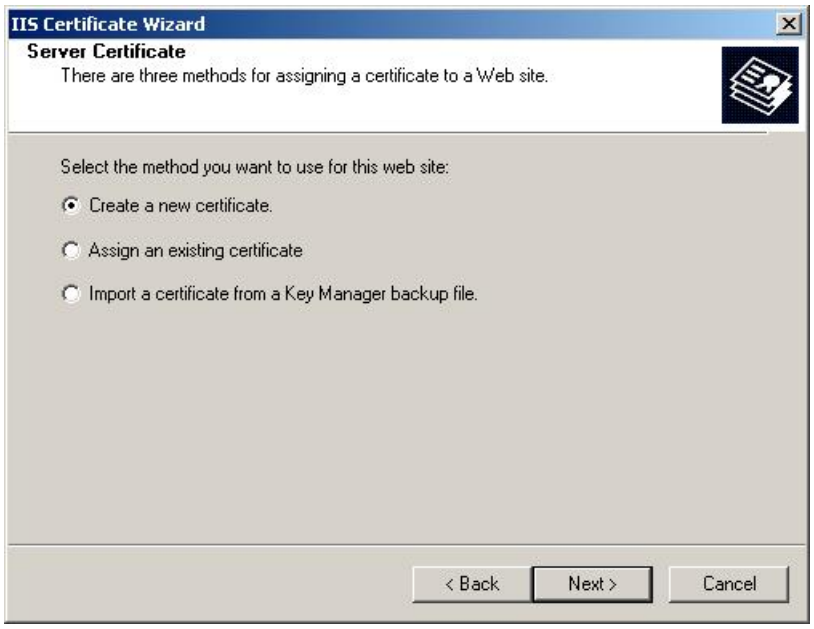


6. Click **Server Certificate** button to launch the Web Server Certificate Wizard.

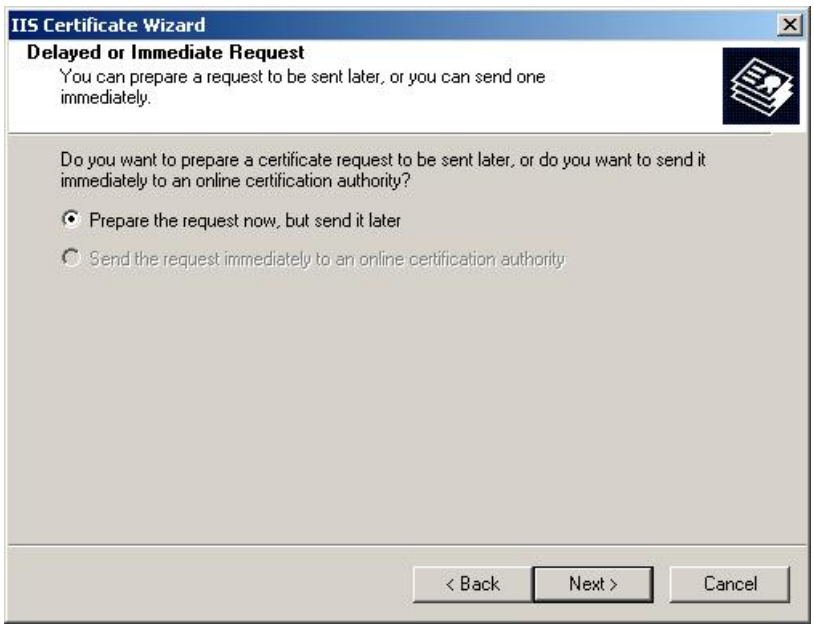


7. Click **Next** to move past the welcome dialog box.

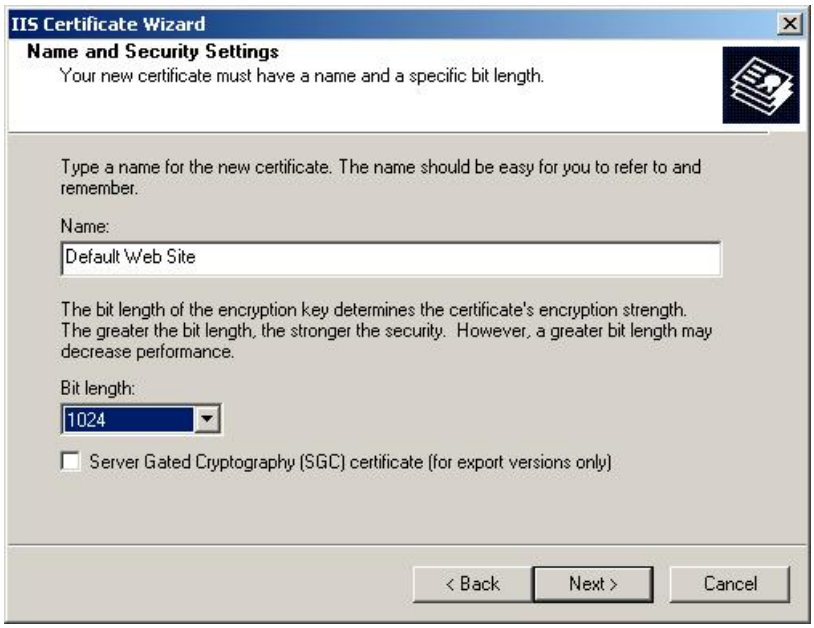
8. Click **Create a New Certificate**, and then click **Next**.



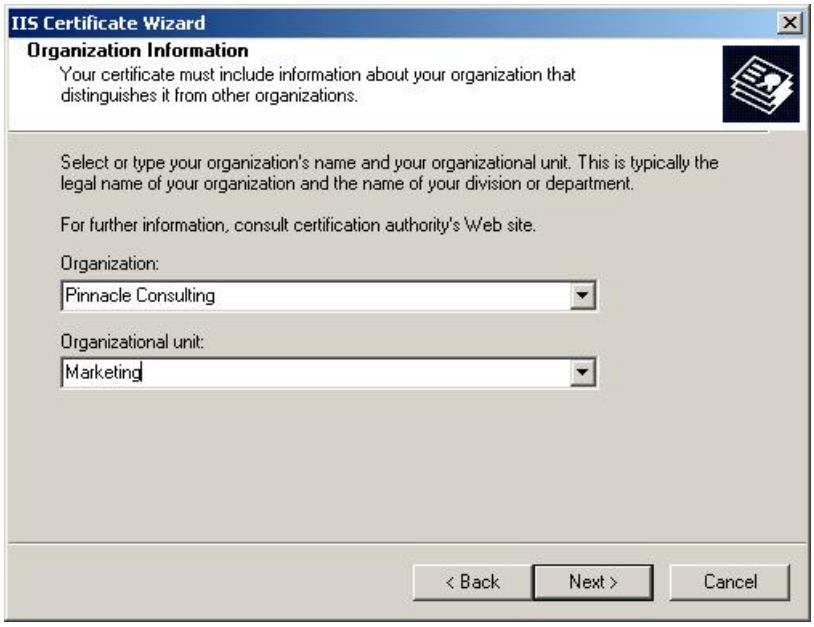
9. Click **Prepare the request now, but send it later**, and then click **Next**.



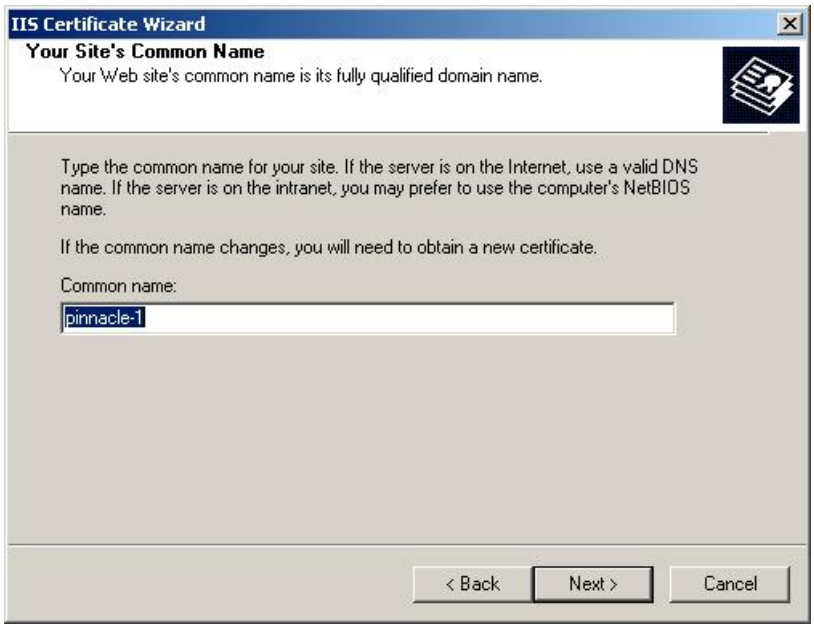
10. Enter the name you wish to appear on the certificate and select 1024 in the **Bit length** drop down list. Click **Next** to continue.



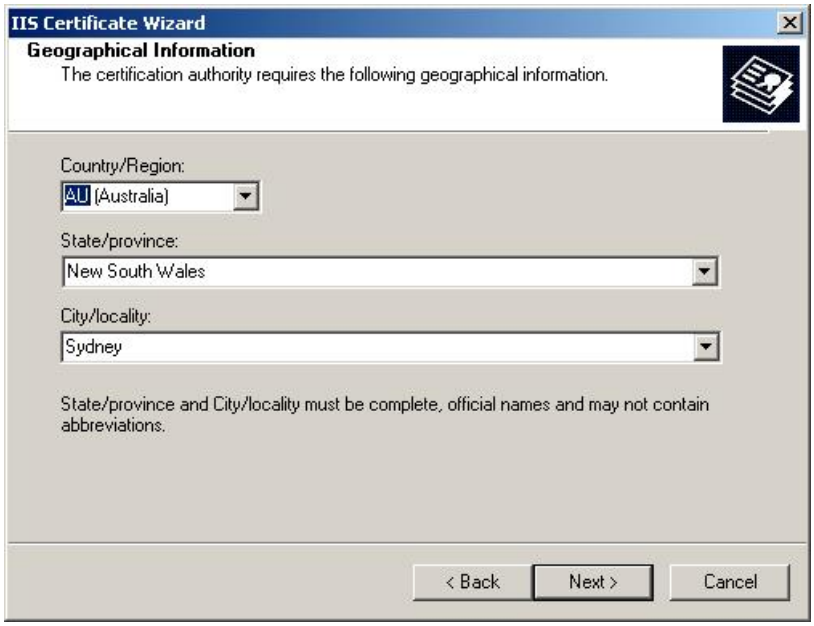
11. Enter the name of your Organisation and the organisational unit and click Next.



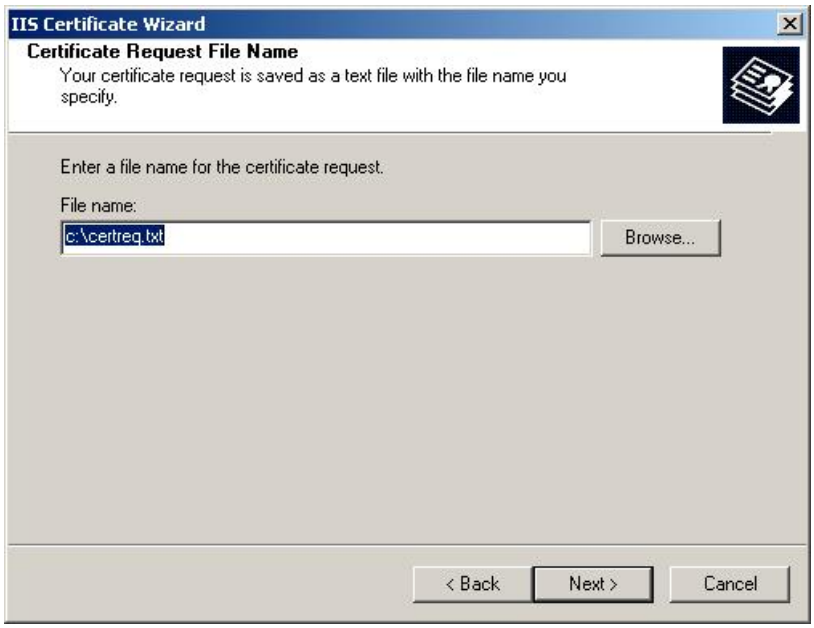
12. Enter the common name you wish to use. For a server certificate this is usually your domain name.



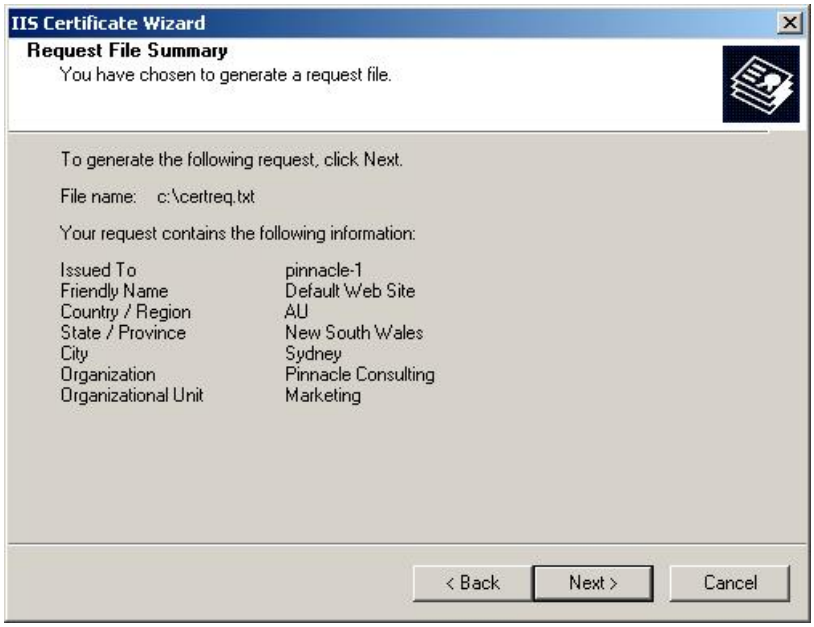
13. Enter the location of your organization and click **Next**.



14. Specify a file name where you want to store the certificate request and click **Next**.



15. The information that will appear on the certificate will be shown for verification. Click **Next**.



16. Click **Finish** to complete the Web Server Certificate Wizard.

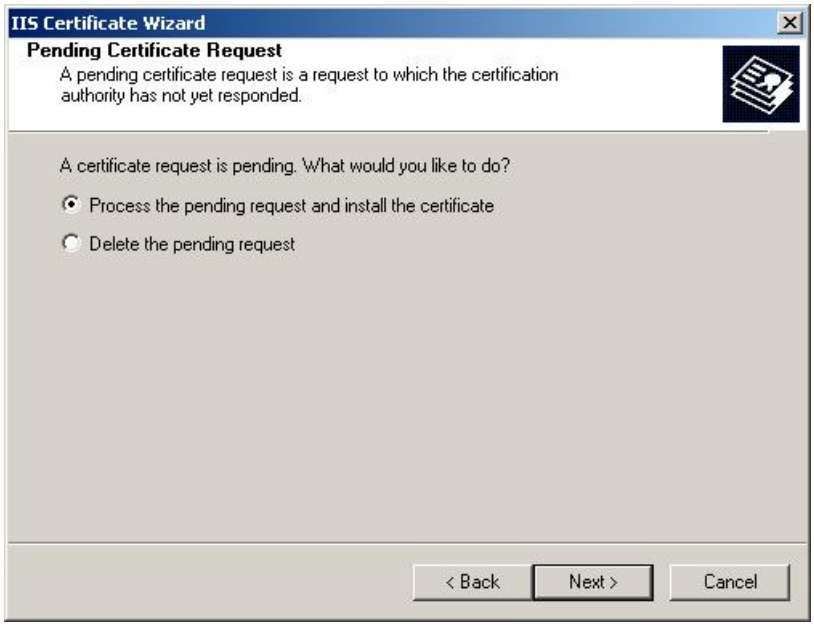
17. Send the generated certificate request file to a CA of your choice for signing.

2 To install the certificate on the Web server

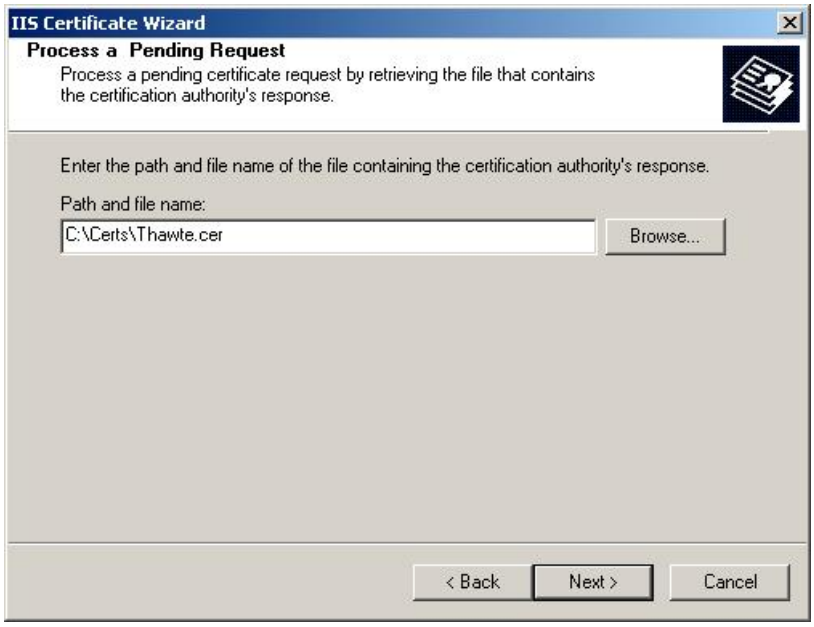
After you received the certificate back from the CA you need to install it on your web-server.

1. Follow step 1 to 7 as described in the previous section.
2. Click **Server Certificate** to launch the Web Server Certificate Wizard. Click **Next** to process the certificate you obtained from the CA.

3. Click **Process the pending request and install the certificate**, and then click **Next**.



4. Enter the path and file name of the file that contains the response from the CA, and then click **Next**. The example below will read the certificate from C:\Certs directory.



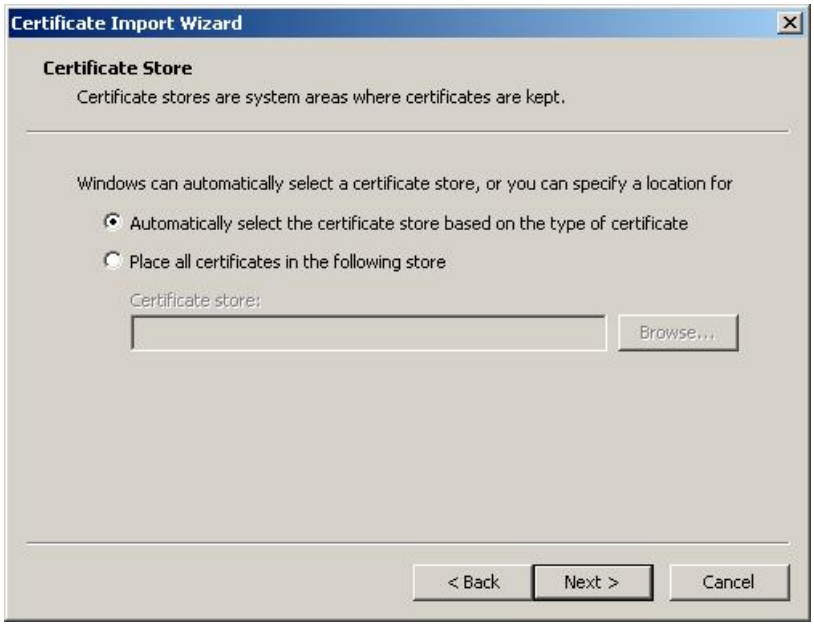
5. Examine the certificate overview, click **Next**, and then click **Finish**.

A certificate is now installed on the web server.

3 Install the CA root certificate used to sign the server certificate

This procedure installs a trusted certificate on IIS 5.0 on Windows 2000 Pro. This section assumed that you already obtained a CA root certificate, which was used to sign the server certificate.

1. Start Windows Explorer
2. Navigate to the directory, where the CA root certificate file is stored.
3. Right click on the certificate file and select **Install Certificate**.
4. It will start the Certificate Import Wizard.
5. Click **Next** to go pass the Welcome screen.
6. Select **Automatically select the certificate store based on the type of certificate** and click **Next**.



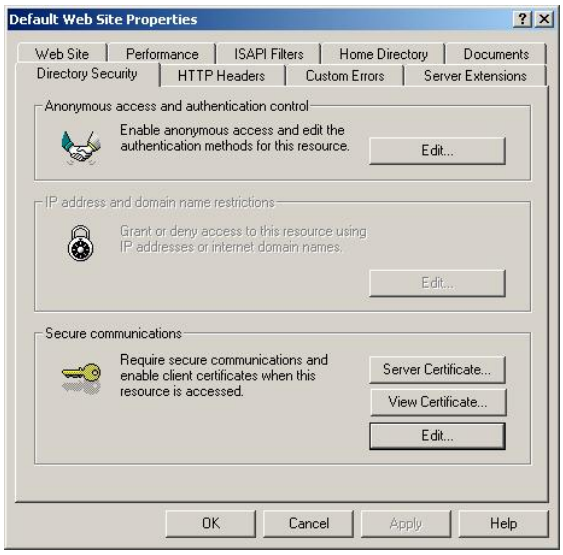
7. On the next screen click **Finish** to complete the installation of CA root certificate.
8. You may be asked, if you trust the certificate issuer. Click Yes, if you are prompted to do so, assuming you received the certificate from a trusted CA.

Tip: To view a certificate, start Windows Explorer, navigate to a .cer file and then double-click it.

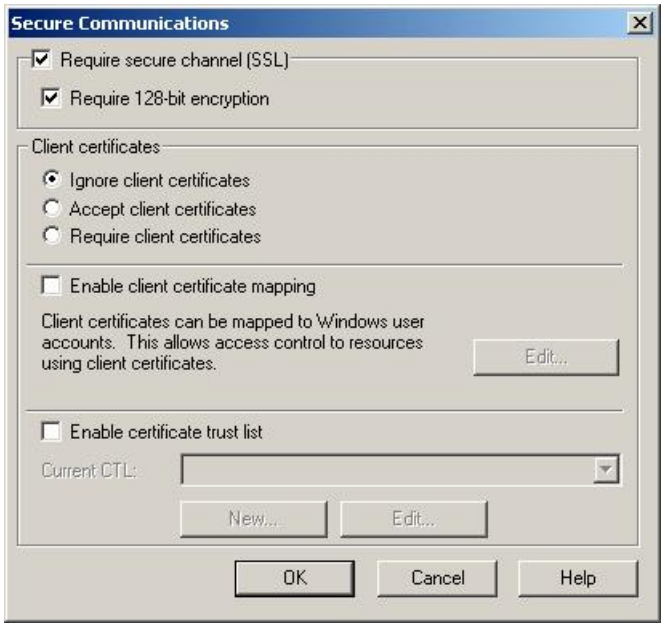
4 Configure IIS Web Server to use SSL

This procedure uses Internet Information Services (IIS) to configure your Web application's virtual directory to require SSL to access it.
This procedure assumed that you have a valid certificate installed on your Web server.

1. Follow steps 1 to 6 as described in section 1.
2. On the **Default Web Site Properties** dialog box, click **Edit**.



3. Select the **Require secure channel (SSL)** check box.



4. If you want to force strong encryption, select the **Require 128-bit encryption** option.
5. Select either **Ignore client certificates** or **Accept client certificates**.
6. Click OK, and then click OK again.

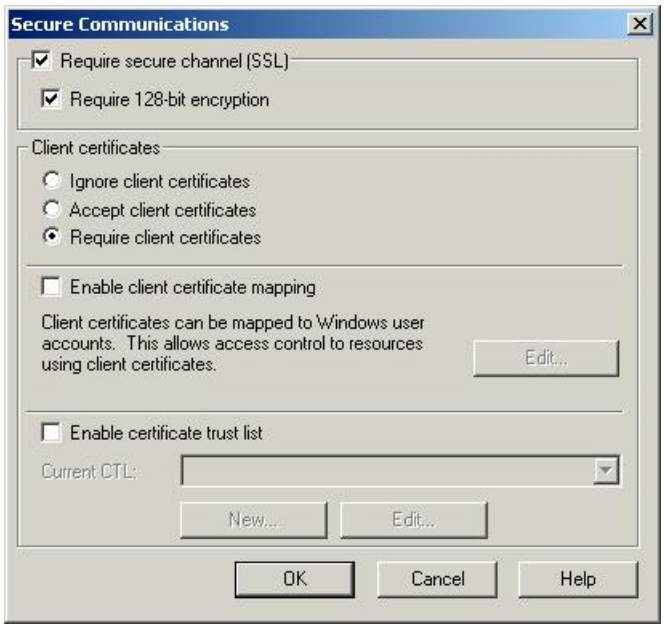
7. In the Inheritance Overrides dialog box, click Select All, and then click OK to close the properties dialog box.

Your IIS web server is now ready to communicate securely using SSL.

5 Configure IIS Web Server to require client certificates

This procedure uses Internet Information Services (IIS) to configure your Web application's virtual directory to require client certificates.
This procedure assumes that you have a valid certificate installed on your Web server.

1. Follow steps 1 – 5 in section 3.
2. To force your web server to ask for client certificates, select the **Require client certificates** option in Client certificates section.



3. Click OK, and then click OK again.
4. In the Inheritance Overrides dialog box, click Select All, and then click OK to close the properties dialog box.

6 Obtain client certificates from an external CA or generate your own client certificates

To obtain a client certificate go to Certification Authority such as Verisign, Thawte, Baltimore, CACert or others.

To generate client certificates from your own CA, you need a machine running Microsoft Certificate Service.

7 Install the CA root certificate

Before you can use a SSL client certificate to access the web-server, which was set up to request client certificate, you must install the root certificate of the CA who signed the client certificate(s).

This procedure installs a trusted certificate on IIS 5.0 on Windows 2000 Pro. This section assumed that you already have a root certificate stored in a .cer file.

Follow instructions in section 3 to install the CA root certificate. The difference is that you must double click the CA root certificate that was used to sign the client certificate(s).

Tip: To view a certificate, start Windows Explorer, navigate to a .cer file and then double-click it.

8 Install a Client Certificate

This procedure installs a client-side certificate. ***You can use a certificate from any certificate authority,*** or you can generate your own certificate using Microsoft Certificate Services. This section assumed that you already have a client certificate from a CA stored in a .cer file

Follow instructions in section 3 to install a client certificate. The difference is you must double click the client certificate file, instead of a CA root certificate file.

Tip: To view a certificate, start Windows Explorer, navigate to a .cer file and then double-click it.

Click Finish to complete the wizard. Dismiss the confirmation message box, and then click OK to close the certificate.