Microsoft IIS 5/6– Guide to Installing Root Certificates, Generating CSR and Installing certificate

Trustis Limited

Building 273 New Greenham Park Greenham Common Thatcham RG19 6HN

E: info@trustis.com W: www.trustis.com

Registered in England No: 03613613

Table of Contents

1 Introduction

This document specifies instructions for Installing the Root and Intermediate certificates, generating your Certificate Signing Request (CSR), and Installing your SSL certificate. The images in the instructions may differ slightly from your configuration depending on whether you have IIS 5.x or 6.x installed. However, the process is the same.

2 Installing the Root & Intermediate Certificates:

Firstly, you need to download the CA certificates (both Root CA certificate and Issuing CA certificate) as individual files

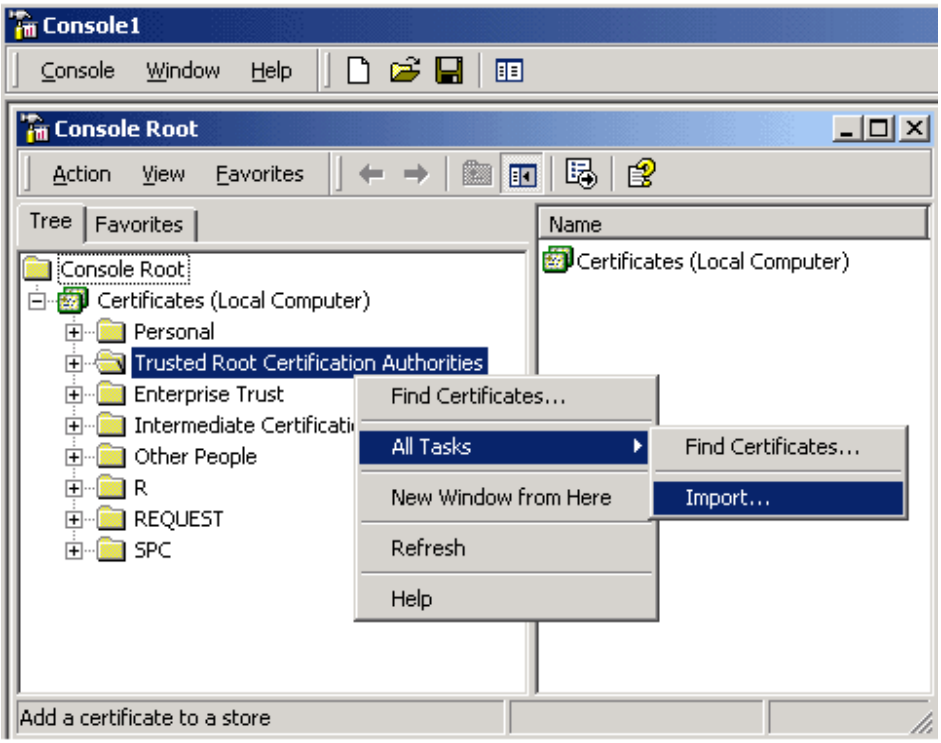
- DER format Root CA certificate – found at http://www.trustis.com/pki/healthcare/ops/fpsroot-der.crt
- DER format Healthcare TT Issuing Authority certificate – found at http://www.trustis.com/pki/healthcare/ops/healthcarett-der.crt

To install these certificates, you must first enable the Certificates Snap-in for the Microsoft Management Console (mmc)

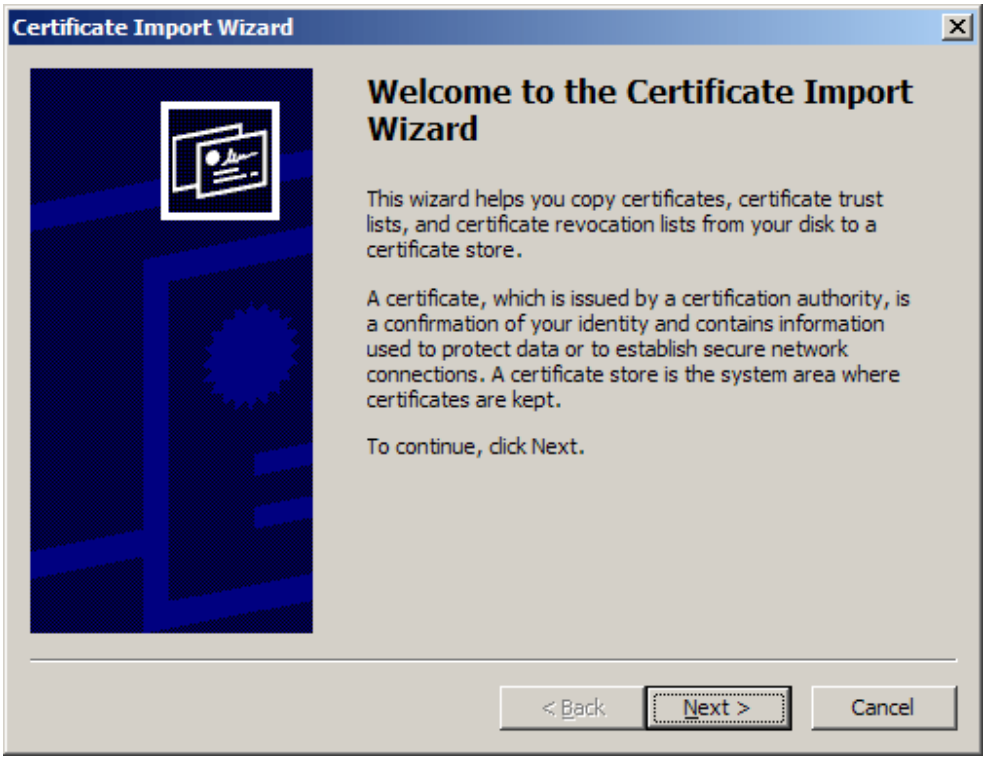
1. Click the **Start Button** then select **Run** and type *mmc*
2. Click **File** and select **Add/Remove Snap in**
3. Select **Add**, select **Certificates** from the **Add Standalone Snap-in** box and click **Add**
4. Select **Computer Account** and click **Next**
5. Select **Local Computer** and click **Finish**
6. **Close** the **Add Standalone Snap-in** box, click **OK** in the Add/Remove Snap in
7. Return to the MMC

2.1 Installing the Root CA Certificate

1. Right click the *Trusted Root Certification Authorities.* Select **All Tasks**, select **Import**.

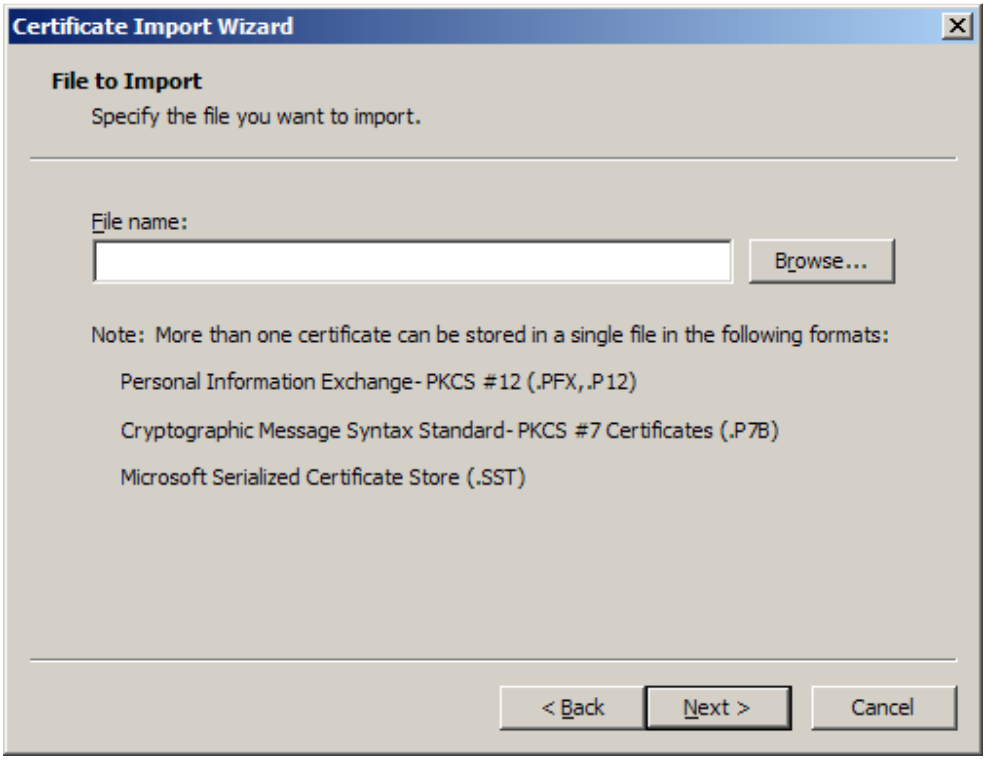


This starts the certificate import wizard



Click **Next**.

2. The File to Import dialog is shown

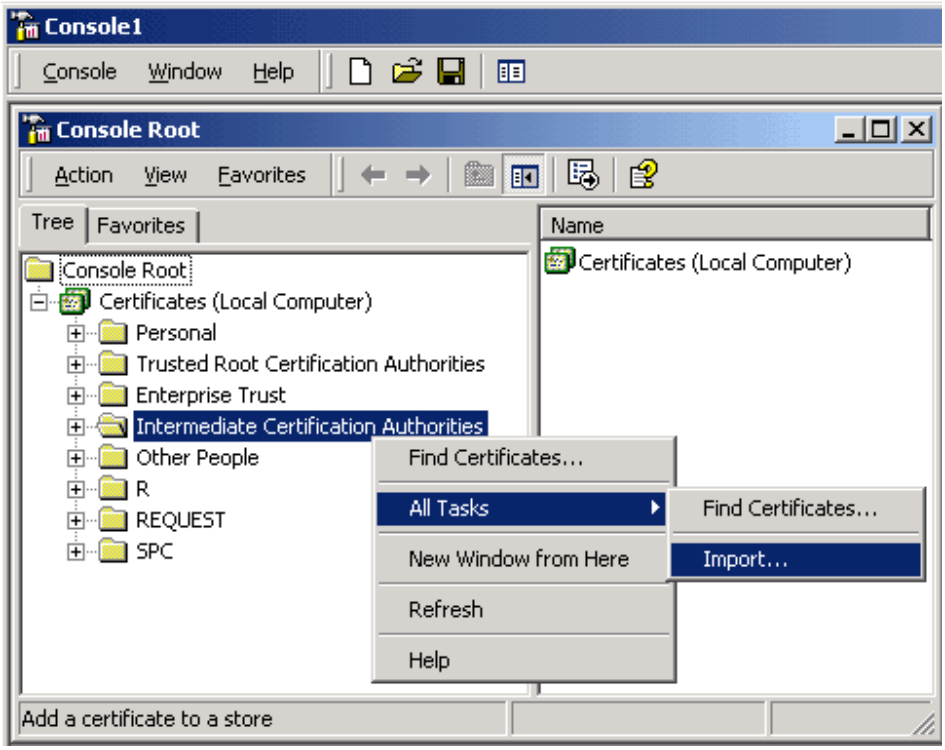


Locate the **Root CA** Certificate file you downloaded earlier and click **Next**.

3. When the wizard is completed, click **Finish**.

2.2 *Installing the Issuing CA* Certificate

1. Right click the *Intermediate Certification Authorities.* Select **All Tasks**, select **Import**.



2. Complete the import wizard again, but this time locating the **Issuing CA Certificate** when prompted for the Certificate file.

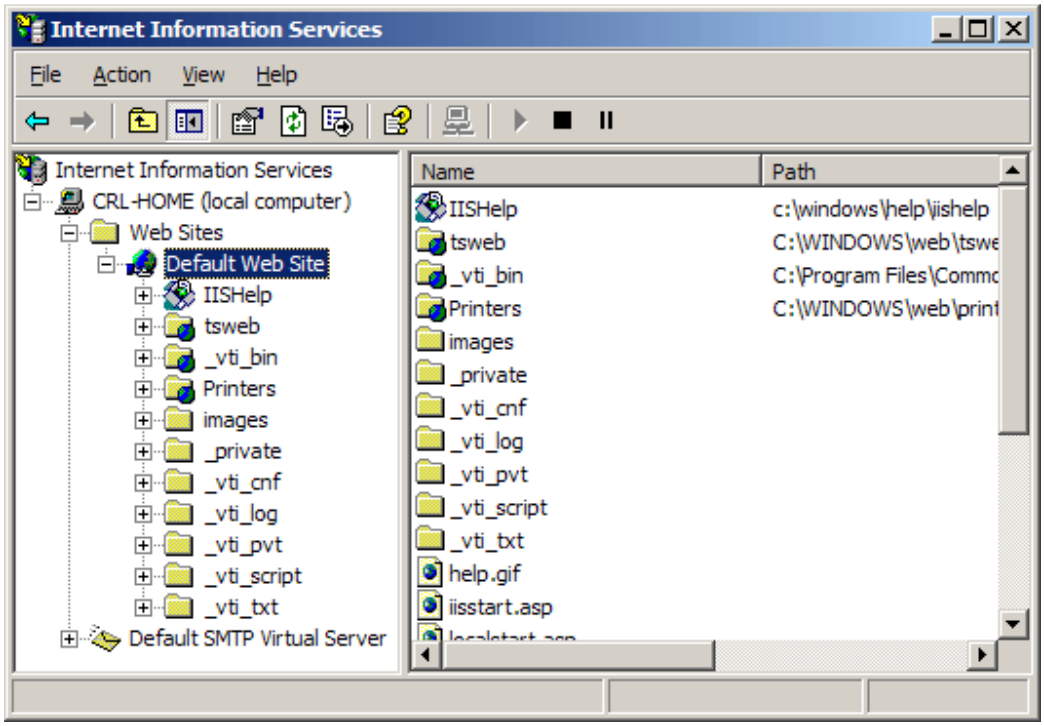
When both certificates have been installed:

- Ensure that the **Root CA** certificate appears under **Trusted Root Certification Authorities**
- Ensure that the **Issuing CA** certificate appears under **Intermediate Certification Authorities**

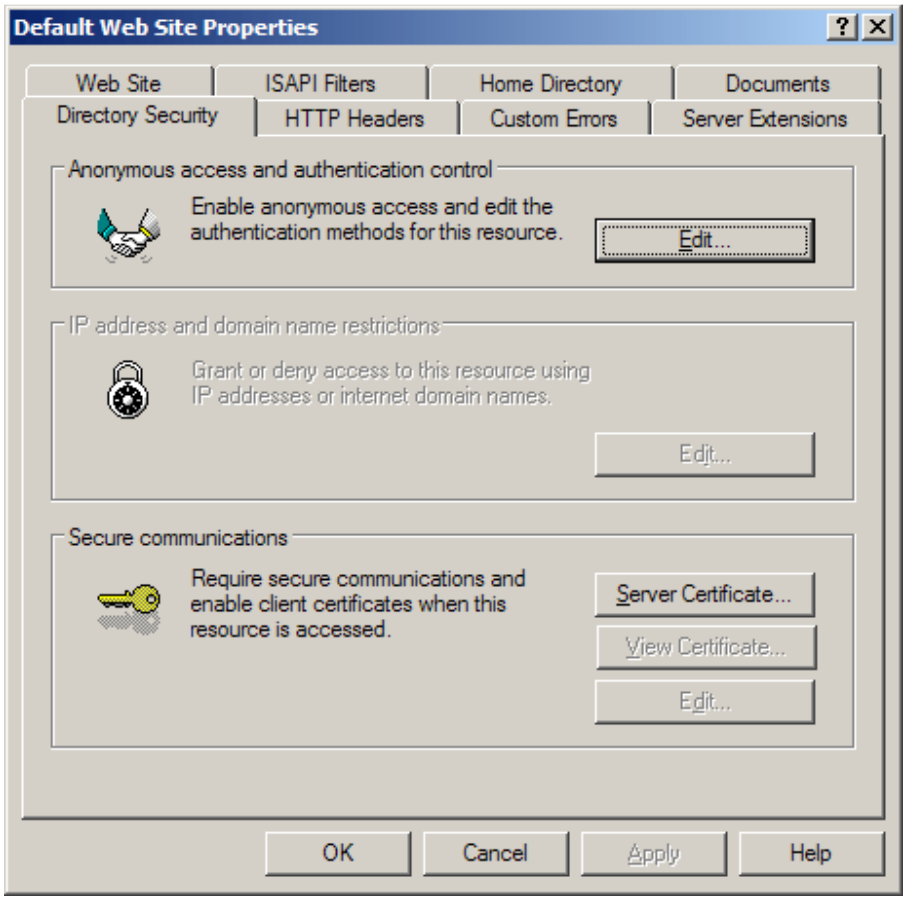
3 Certificate Signing Request (CSR) Generation

A CSR is a file containing your IIS SSL certificate application information, including your Public Key. Generate your CSR and then copy and paste the CSR file into the webform in the enrolment process:

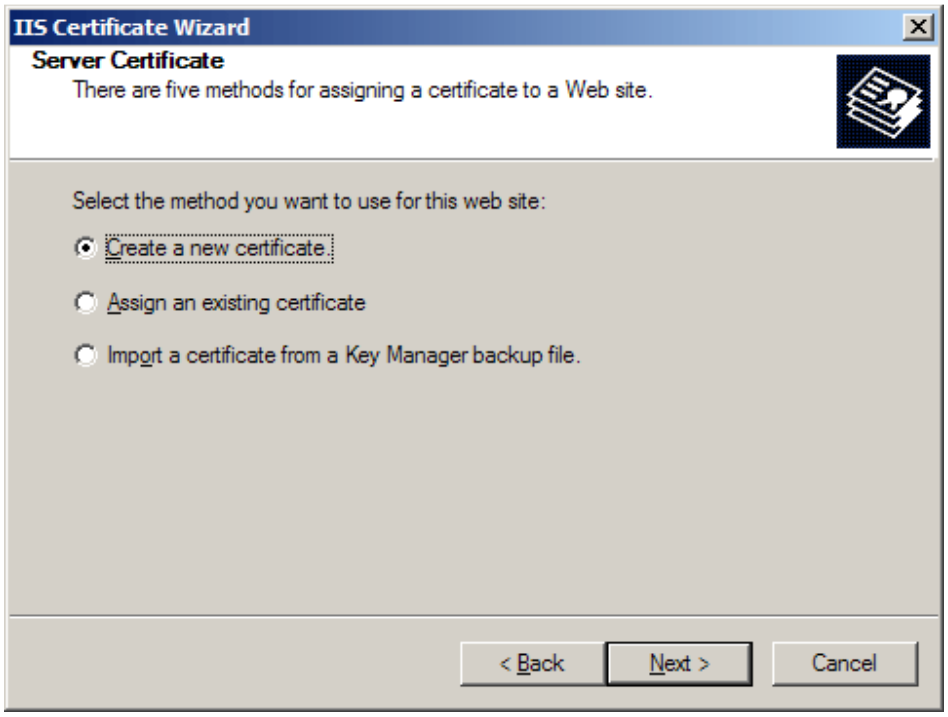
1. Select **Administrative Tools**
2. Start **Internet Information Services (IIS) Manager**



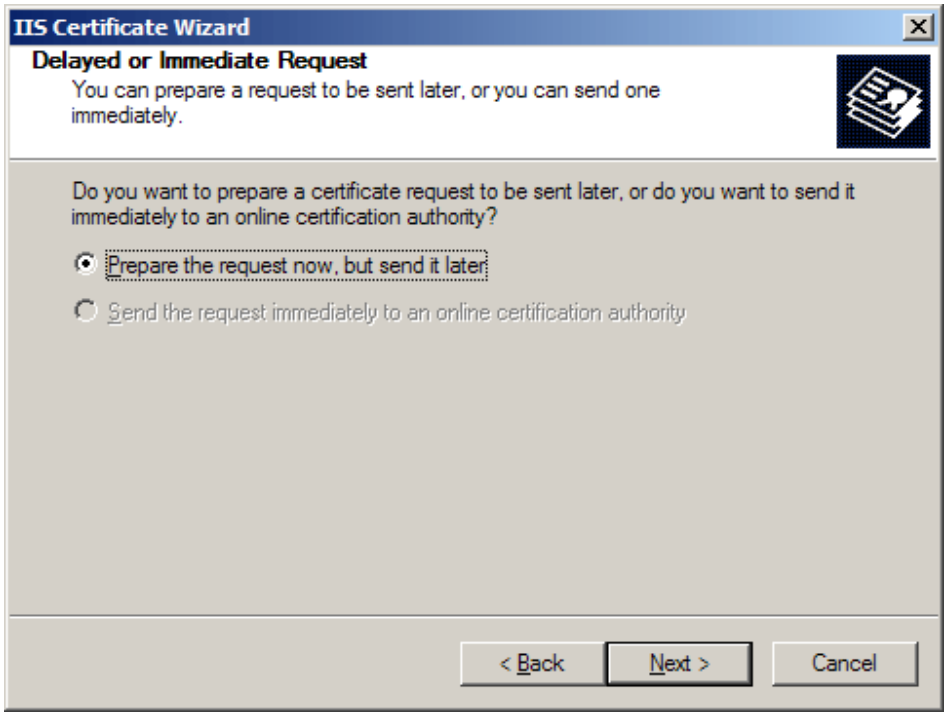
3. Open the properties window for the website the CSR is for. You can do this by right clicking on the Default Website and selecting Properties from the menu
4. Open **Directory Security** by right clicking on the Directory Security tab



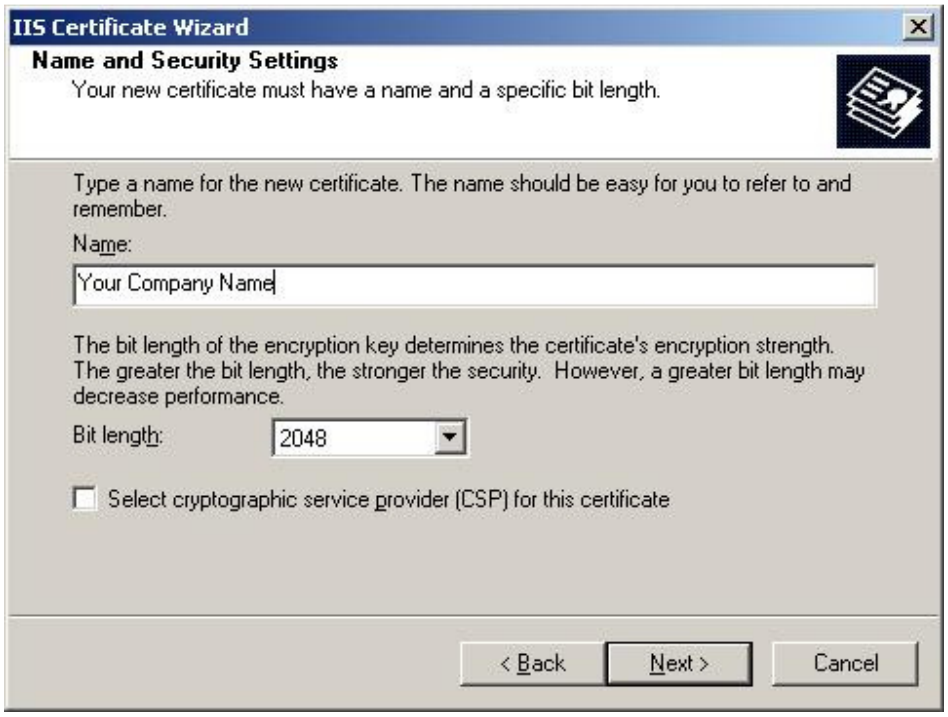
5. Click **Server Certificate**. The following Wizard will appear:



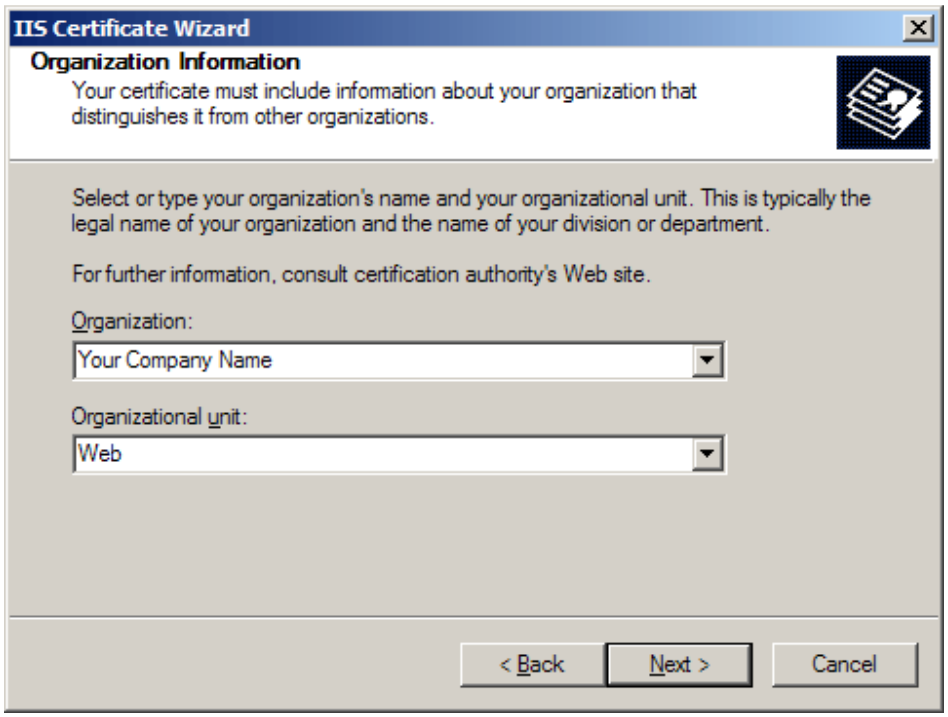
6. Click **Create a new certificate** and click **Next**.



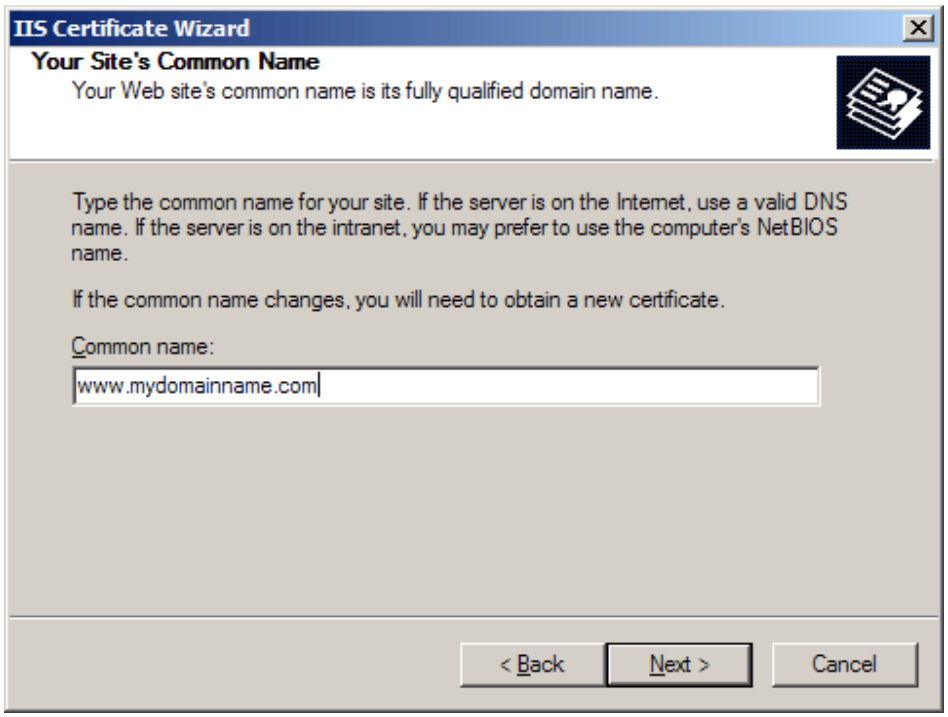
7. Select **Prepare the request** and click **Next**.



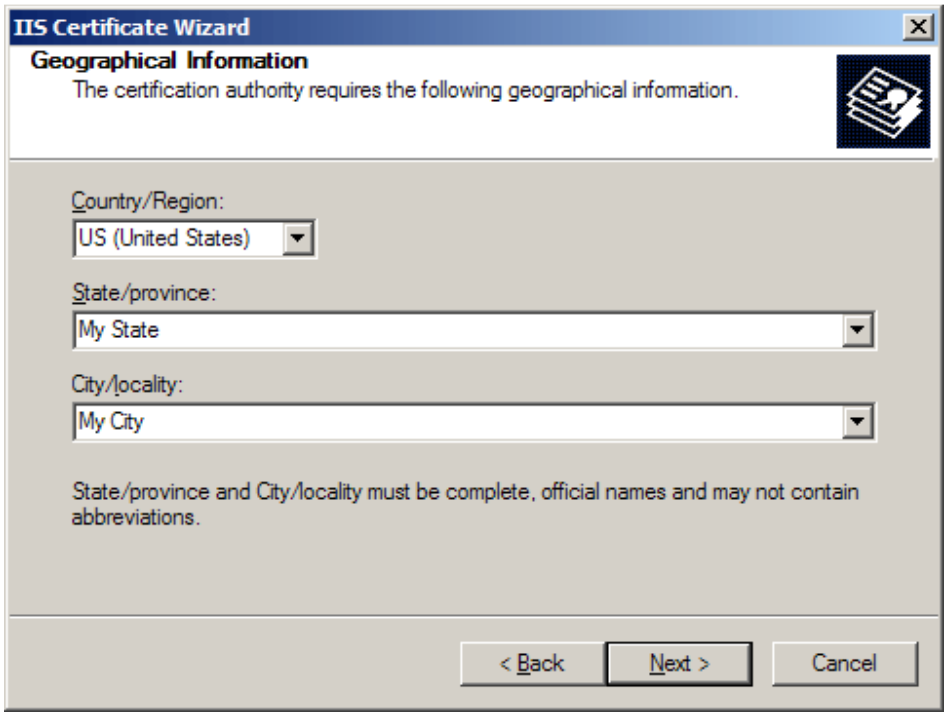
8. Provide a name for the certificate, this needs to be easily identifiable if you are working with multiple domains. This is for your records only.
9. Choose 2048 bit length. If this is not available, you will need to check the cipher strength of your server. Visit www.microsoft.com for more details. ONLY 2048 bit keys are accepted. Click **Next**



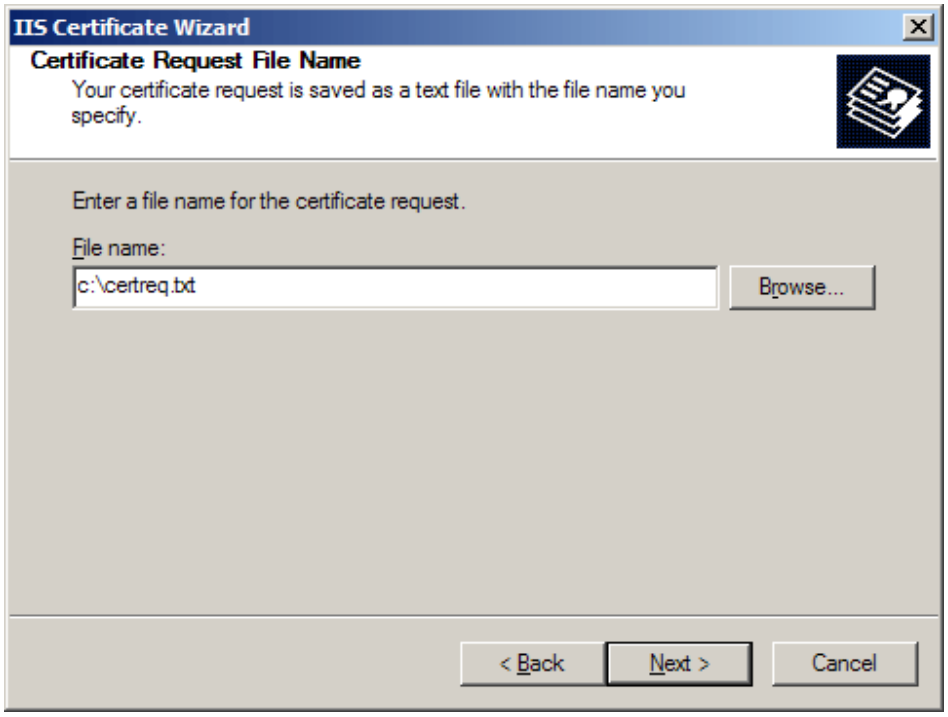
10. Enter **Organisation** and **Organisation Unit**, these are your company name and department respectively. Click **Next**.



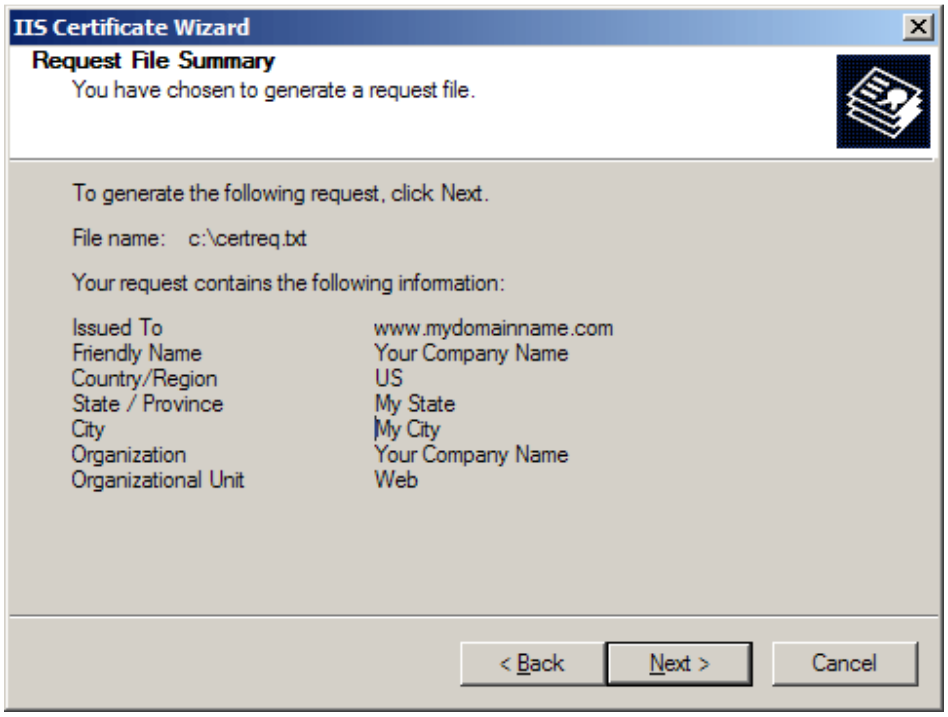
11. The Common Name field should be the **Fully Qualified Domain Name** (FQDN) or the web address for which you plan to use your IIS SSL Certificate, e.g. the area of your site you wish customers to connect to using SSL. For example, an Instant SSL Certificate issued for **trustis.com** will not be valid for **www.trustis.com**. If the web address to be used for SSL is **www.trustis.com**, ensure that the common name submitted in the CSR is www.trustis.com. Click **Next**.



12. Enter your **country**, **state** and **city**. Click **Next**.



13. Enter a filename and location to save your CSR. You will need this CSR to enrol for your IIS SSL Certificate. Click **Next**.



14. Check the details you have entered. If you have made a mistake click **Back** and amend the details. Be especially sure to check the domain name the Certificate is to be "Issued To". Your IIS SSL Certificate will only work on this domain. Click **Next** when you are happy the details are absolutely correct.
15. When you make your application, make sure you include the CSR in its entirety into the appropriate section of the enrolment form - including **-----BEGIN CERTIFICATE REQUEST-----to-----END CERTIFICATE REQUEST-----**
16. Click **Next**
17. Confirm your details in the enrolment form
18. Finish

4 Installing your SSL Server Certificate

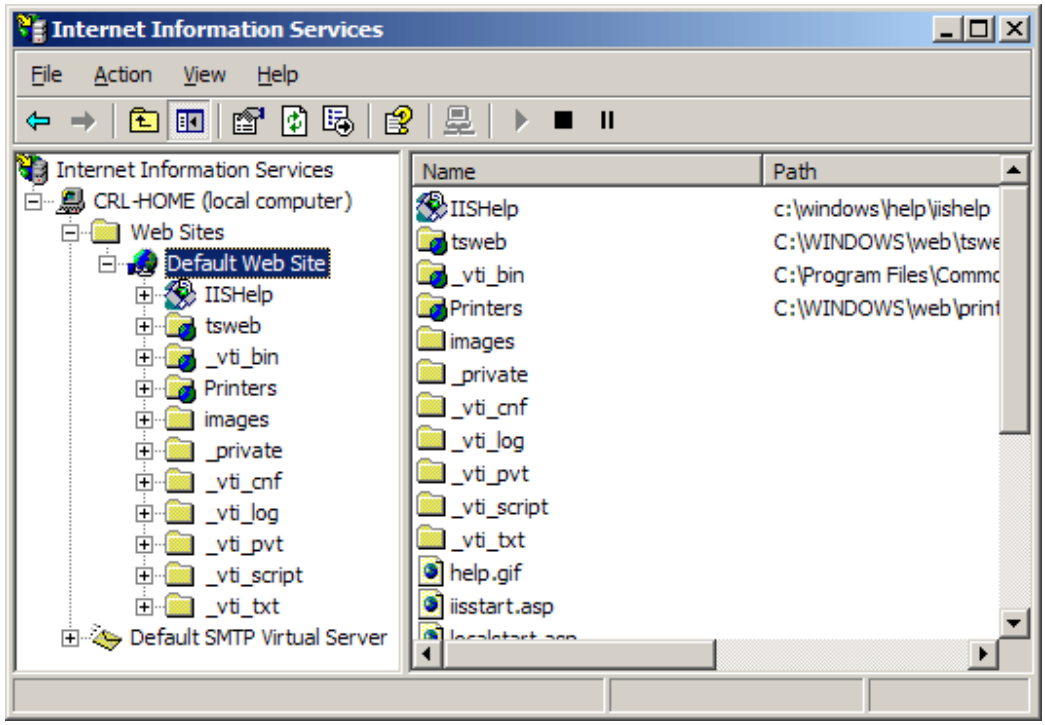
You will receive an email from the Registration Authority when your certificate request has been approved that contains a link to a location where your certificate may be obtained. Clicking on this link will bring up a browser window that contains the details of your issued certificate and includes a section that looks something like the following:

-----BEGIN CERTIFICATE-----
MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BBwGggDCCAmowggHXA
hAF
UbM77e50M63v1Z2A/5O5MA0GCSqGSIb3DQEOBAUAMF8xCzAJBgNVBAYTAIVTMS
Aw
(.....)
E+cFEpf0WForA+eRP6XraWw8rTN8102zGrcJgg4P6XVS4l39+l5aCEGGbauLP5W6
K99c42ku3QrlX2+KeDi+xBG2cEIsdSiXeQS/16S36ITclu4AADEAAAAAAAAA
-----END CERTIFICATE-----

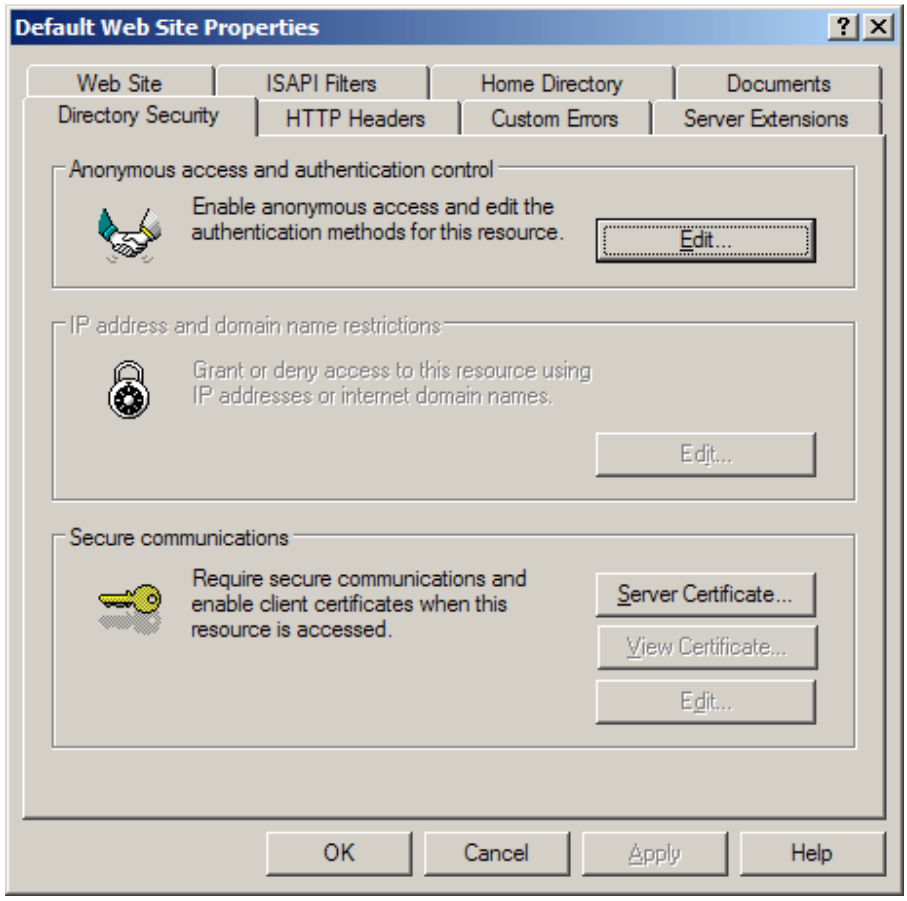
Copy everything you see **between and including** the lines that look like
-----BEGIN CERTIFICATE-----
and
-----END CERTIFICATE-----

Paste the CSR into an appropriately named text file e.g. myserver.crt

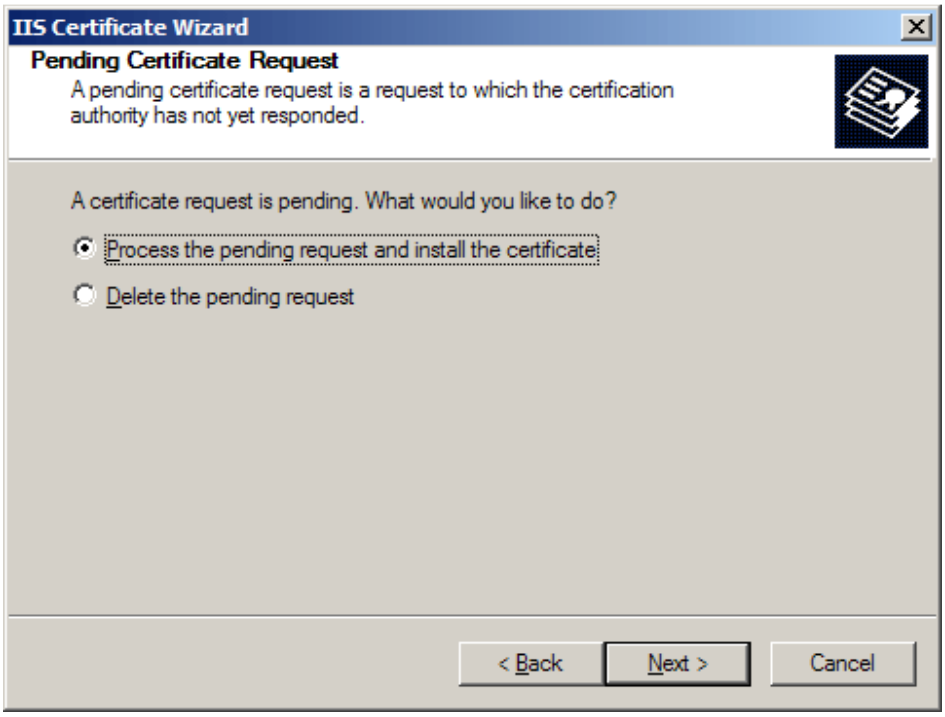
1. Select **Administrative Tools**
2. Start **Internet Services Manager**



3. Open the properties window for the website. You can do this by right clicking on the Default Website and selecting Properties from the menu.
4. Open **Directory Security** by right clicking on the Directory Security tab



5. Click **Server Certificate**. The following Wizard will appear:



6. Choose to **Process the Pending Request and Install the Certificate**. Click **Next**.
7. Enter the location of your IIS SSL certificate that you obtained earlier (e.g. myserver.crt)
   (you may also browse to locate your IIS SSL certificate), and then click **Next**.
8. Read the summary screen to be sure that you are processing the correct certificate, and then click **Next**.
9. You will see a confirmation screen. When you have read this information, click **Next**.
10. You now have an IIS SSL server certificate installed.

Important: You must now restart the computer to complete the install

You may want to test the Web site to ensure that everything is working correctly. Be sure to use when you test connectivity to the site.

5 Using a Wildcard certificate on multiple Webservers

The following advice is from Microsoft's website:

In IIS 5.0 - to use the wildcard certificate you have just installed in the original server that made the certificate request - in other servers, you must:

1. **Export** the certificate and private key from the original IIS server to a Personal Information Exchange - PKCS #12 (PFX) file
2. **Import** the certificate and private key from the Personal Information Exchange - PKCS #12 (PFX) file - into the new server

In IIS 5.0, you can export the private key in PKCS #12 format (*.pfx), using the certificate export wizard.

1. Start the Internet Information Service
2. Display the properties of the Web site.
3. Click the **Direct Security** tab.
4. Click **View Certificate** button.
   Certificate is displayed.
5. Click **Details** tab.
6. Click **Copy to File...** button.
   Certificate Export Wizard starts.
7. Click the Next button.
   Export Private Key page appears.
8. Select **Yes, export the private key**, and click the **Next** button.
   Export File Format page appears.
9. Select **Personal Information Exchange - PKCS #12 (PFX)**
10. Select **Include all certificates in the certification path if possible**
    IMPORTANT: ensure all other check boxes are **NOT checked** (especially the one marked - Delete the private key if the export is successful),
    (if the private key is deleted from this server, SSL operations on this server will cease)
    and click the **Next** button.
11. **Password** page appears.
    Enter the password if necessary, and click the **Next** button.
12. **File to Export** page appears.
    Enter the file name, and click the **Next** button.
13. **Completing the Certificate Export Wizard** page appears.
    Click the **Finish** button.
    The certificate is exported to the file, and "The export was successful" message appears.

To import a certificate from a pfx file, you will need the Microsoft Management Console (MMC) & the certificates snap-in
To add Local Computer Certificate Management to a new MMC console for a local computer

1. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
2. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.

3. Under **Snap-in**, select the **Certificates** snap-in and click on **Add**
4. **Select** "this snap-in will always manage certificates for" **Computer Account**:
5. **Select** "this snap-in will always manage" **Local Computer** (the computer this console is running on), and then click **Finish**.
6. Choose "**Close**" in the "Available Snap-ins" window
7. Click on **OK** in the Add/Remove Snap-in window

Now that you have access to the Certificates snap-in, you can import the server certificate into your computer's certificate store by following these steps:

1. Open the **Certificates (Local Computer) snap-in** and navigate to **Personal**, and then **Certificates**.
2. Right-click **Certificates** (or Personal if that option does not exist.)
3. Choose **All Tasks**, and then click **Import**.
4. When the wizard starts, click **Next**. Browse to the pfx file you created containing your server certificate and private key. Click **Next**.
5. Enter the password you gave the pfx file when you created it. Be sure the Mark the key as exportable option is selected if you want to be able to export the key pair again from this computer. As an added security measure, you may want to leave this option unchecked to ensure that no one can make a backup of your private key.
6. Click **Next**, and then choose the Certificate Store you want to save the certificate to. You should select Personal because it is a Web server certificate. If you included the certificates in the certification hierarchy, it will also be added to this store.
7. Click **Next**. You should see a summary of screen showing what the wizard is about to do. If this information is correct, click **Finish**.
8. You will now see the server certificate for your Web server in the list of Personal Certificates. It will be denoted by the common name of the server (found in the subject section of the certificate).

To enable Internet Information Services 5.0 to use the imported certificate (and the corresponding private key) perform the following steps:

1. Open the Internet Services Manager (under Administrative Tools) and navigate to the Web site you want to enable secure communications (SSL/TLS) on.
2. Right-click on the site and click **Properties**.
3. You should now see the properties screen for the Web site. Click the **Directory Security** tab.
4. Under the **Secure Communications** section, click **Server Certificate**.
5. This will start the Web Site Certificate Wizard. Click **Next**.
6. Choose the **Assign an existing certificate** option and click **Next**.
7. You will now see a screen showing that contents of your computer's personal certificate store. Highlight your Web server certificate (denoted by the common name), and then click **Next**.
8. You will now see a summary screen showing you all the details about the certificate you are installing. Be sure that this information is correct or you may have problems using SSL or TLS in HTTP communications.
9. Click **Next**, and then click **OK** to exit the wizard.

You should now have an SSL/TLS-enabled Web server. Be sure to protect your pfx files from any unauthorised personnel.