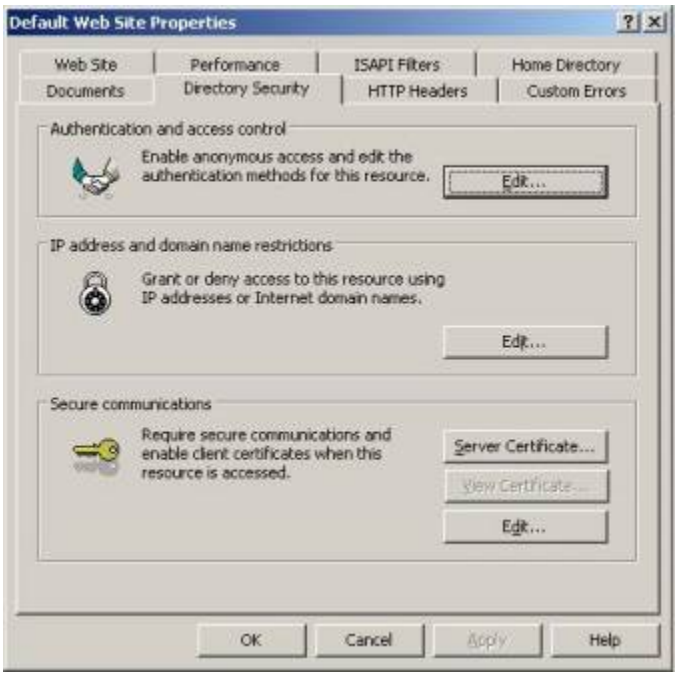
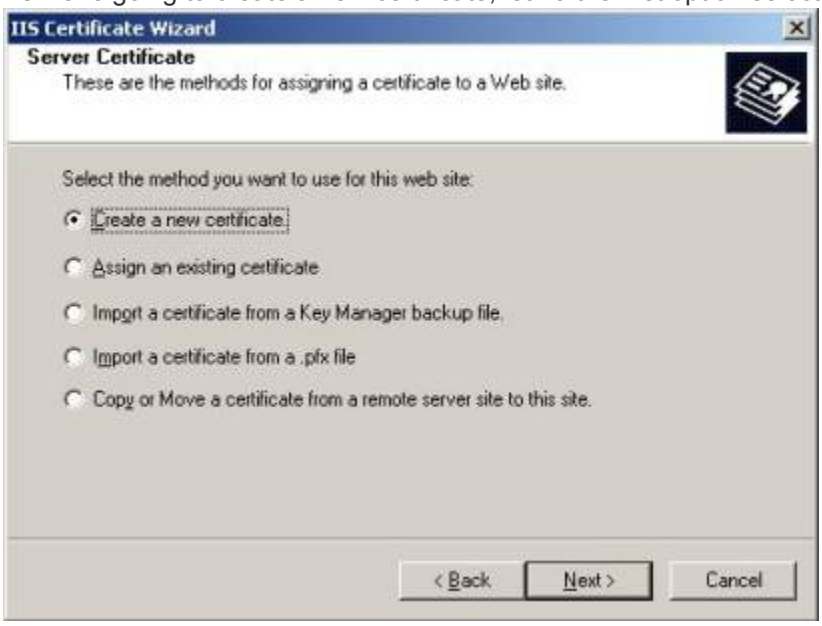
Creating the Certificate Request

Now that we have installed the Certificate Services component, it's time to create the **Certificate Request** for our**Default Website**. We should therefore do the following:

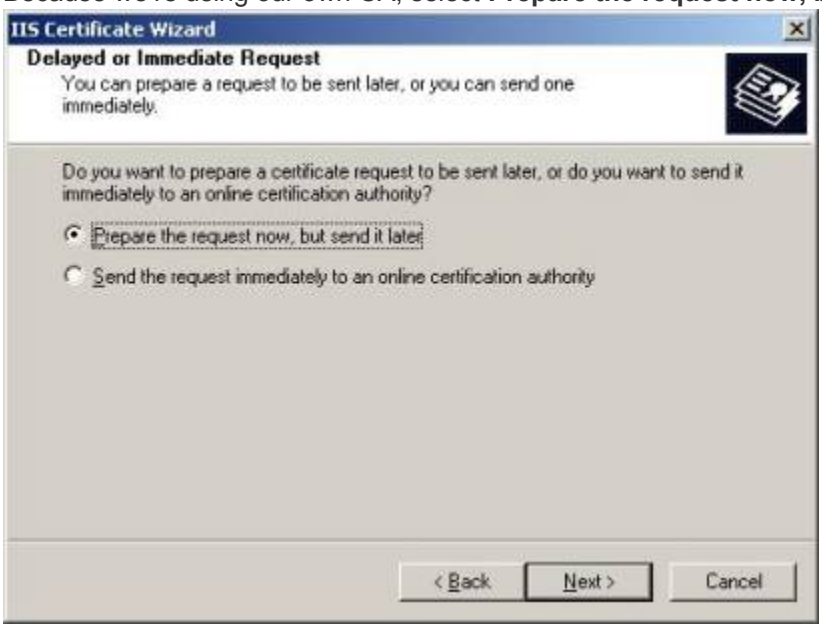
- Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**
- Expand **Websites** > Right-click **Default Website** then select **Properties**
- Now hit the **Directory Security** tab
- Under **Secure Communications** click **Server Certificate…**



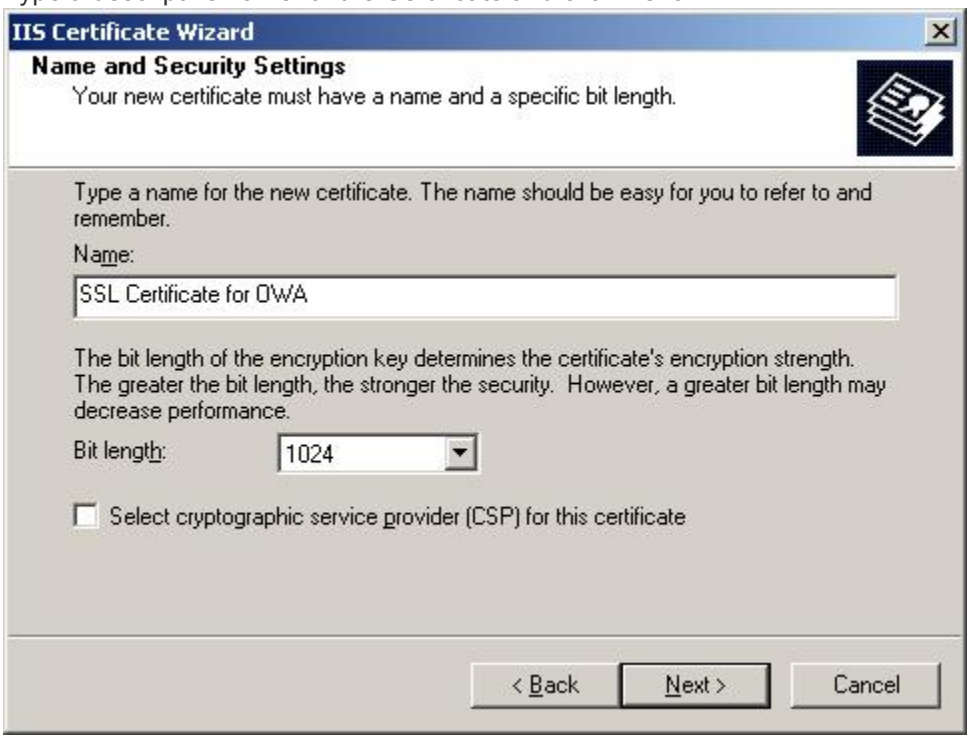
As we're going to create a new certificate, leave the first option selected and click **Next >**



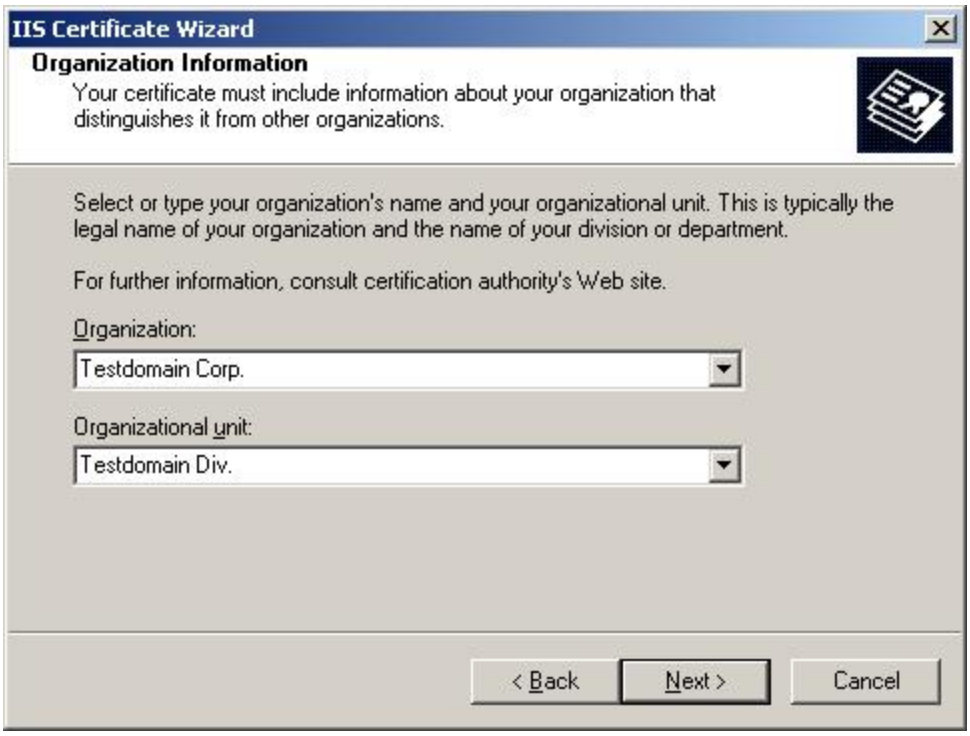
Because we're using our own CA, select **Prepare the request now, but send it later**, then click **Next >**



Type a descriptive name for the Certificate and click **Next >**



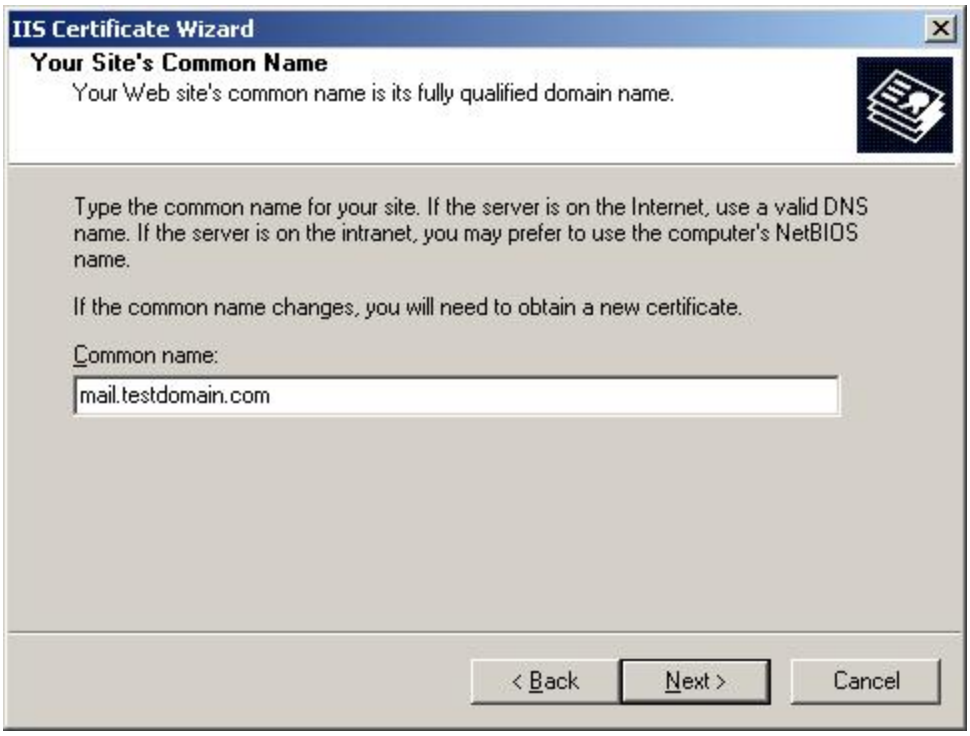
We now need to enter our **organization name** and the **organizational unit** (which should be pretty self-explanatory), then click **Next >**



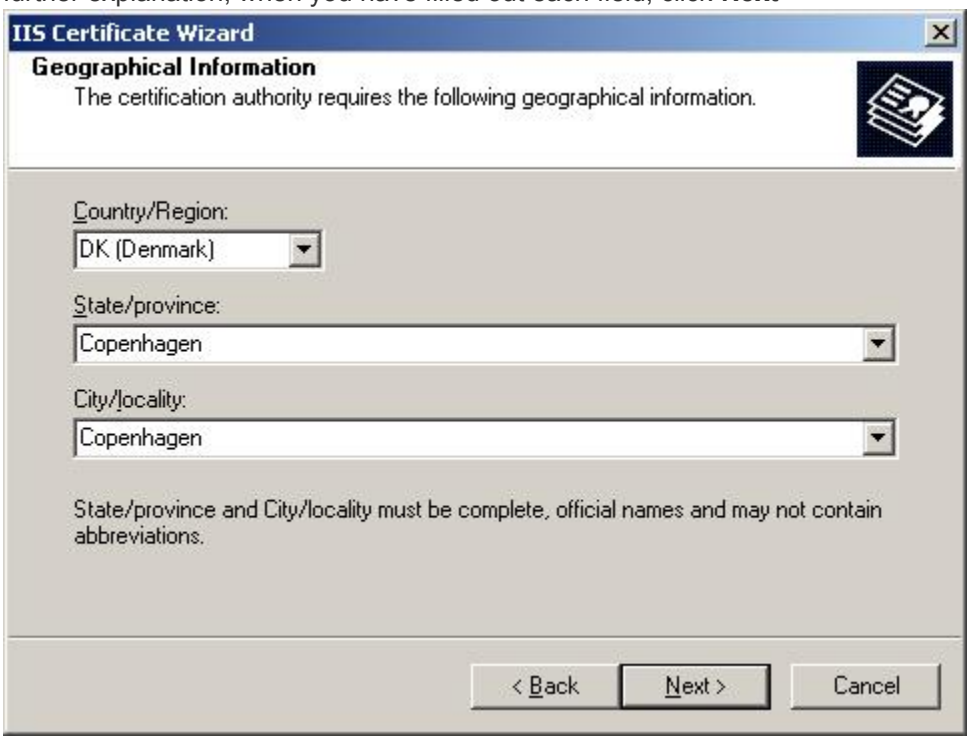
In the next screen we need to pay extra attention, as the common name reflects the external FQDN (Fully Qualified Domain Name), to spell it out, this is the address external users have to type in their browsers in order to access OWA from the Internet.

Note: *As many (especially small to midsized) companies don't publish their Exchange servers directly to the Internet, but instead runs the Exchange server on a private IP address, they let their ISP's handle their external DNS settings. In most cases the ISP creates a so called* ***A record*** *named* ***mail.domain.com*** *pointing to the company's public IP address, which then forwards the appropriate port (443) to the Exchange servers internal IP address.*

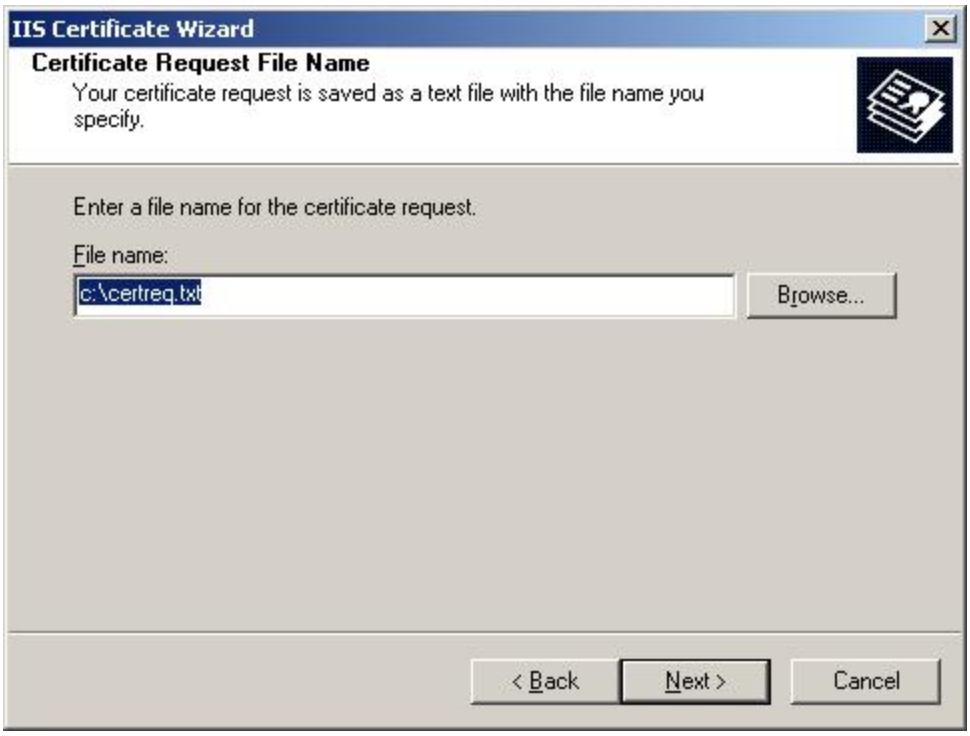
When your have entered a **Common Name** click **Next >**



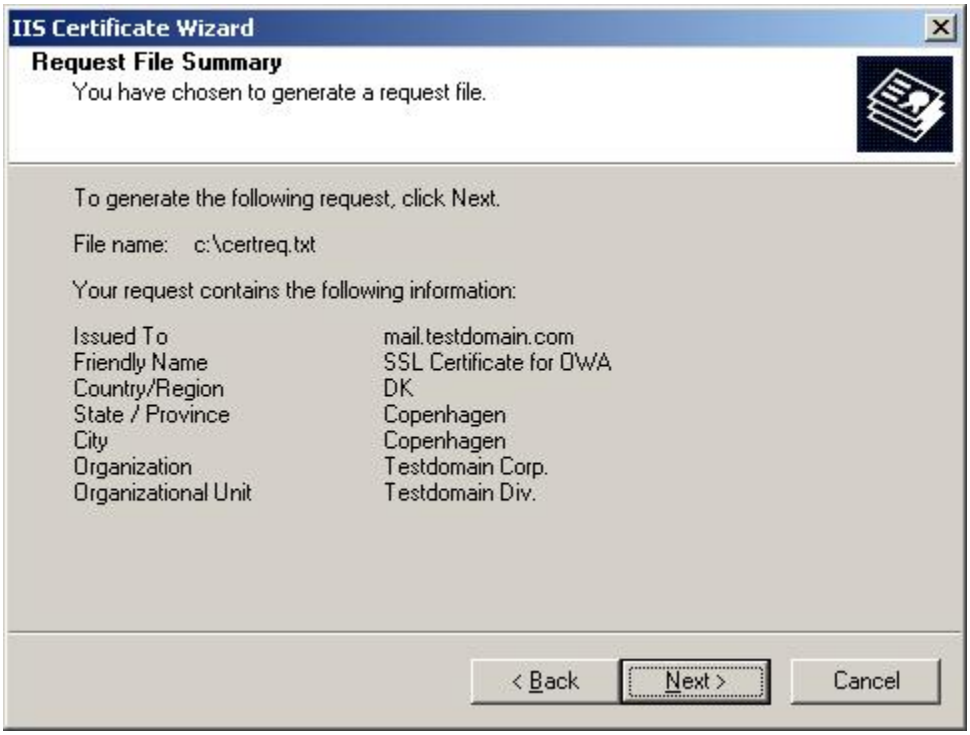
Now it's time to specify the **Country/Region, State/Province and City/locality**, this shouldn't need any further explanation, when you have filled out each field, click **Next >**



In the below screen we have to enter the name of the certificate request we're creating, the default is just fine, click**Next >**



In this screen we can see all the information we filled in during the previous IIS Certificate Wizard screens, if you should have made a mistake, this is your last chance to correct it. If everything looks fine click **Next >**



And finally we can click **Finish**.

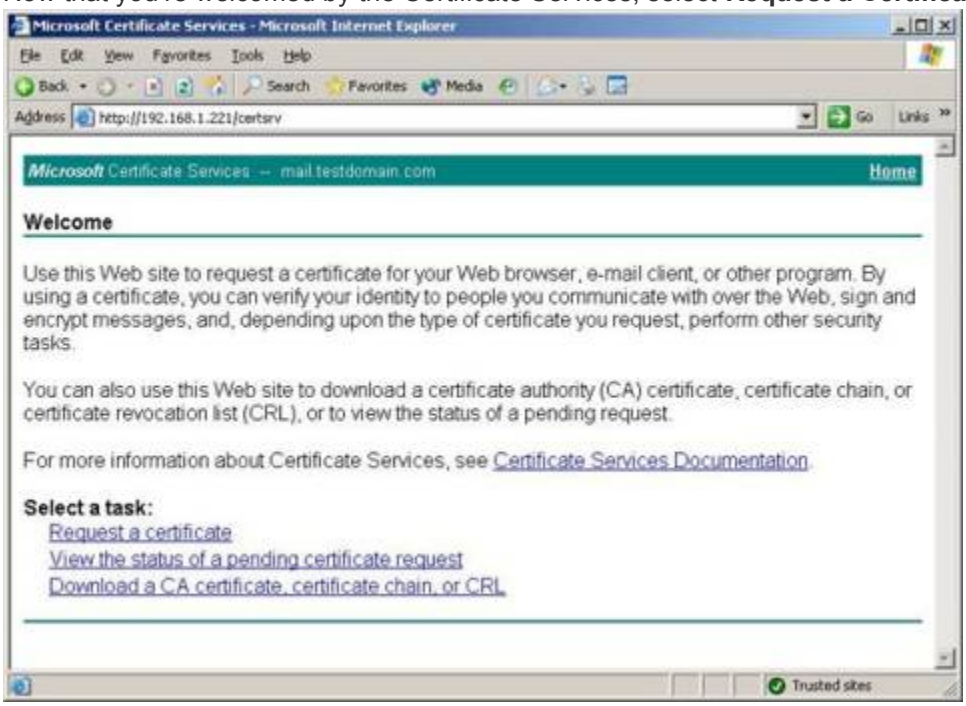
Getting the Pending Request accepted by our Certificate Authority

Now that we have a pending Certificate Request, we need to have it accepted by our CA, which is done the following way:

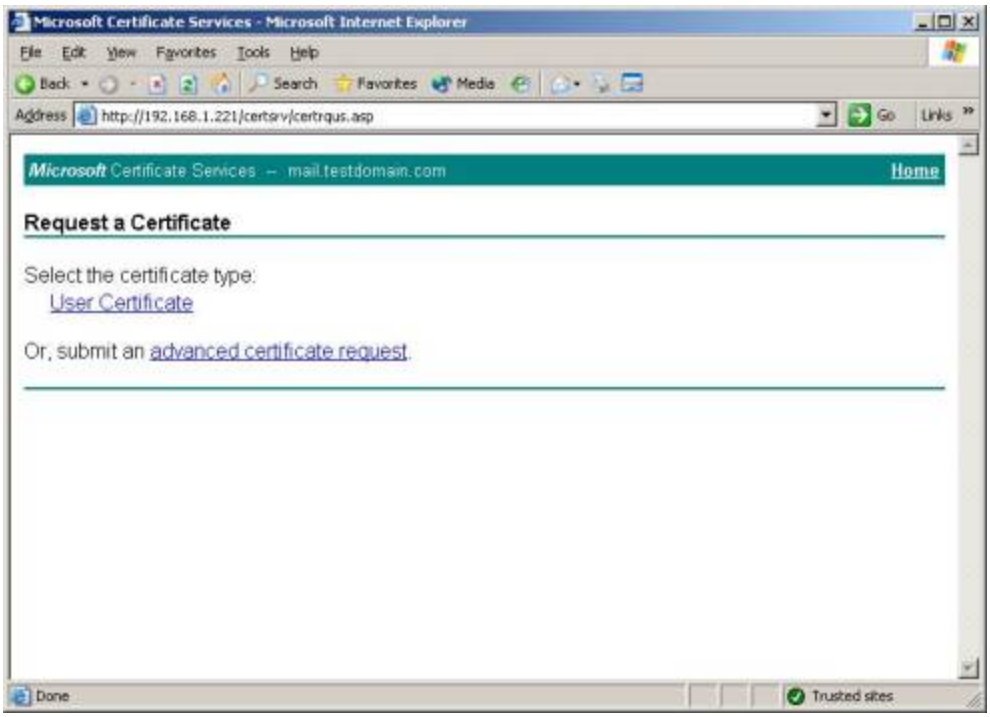
- On the server open **Internet Explorer**
- Type **http://server/certsrv**

Note: *In order to access the **Certsvr virtual folder**, you may be prompted to enter a valid username/ password, if this is the case use the Administrator account. When you have been validated the Windows 2003 Server will most probably block the content of the CertSrv virtual folder, which means you wil have to add it to your trusted sites in order to continue.*

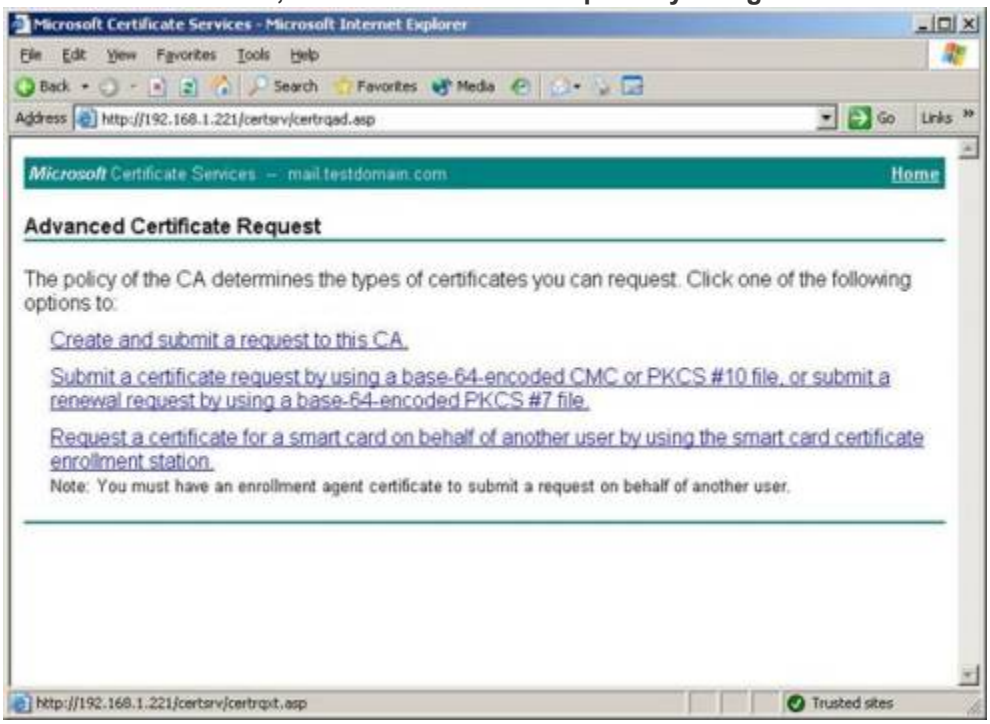
Now that you're welcomed by the Certificate Services, select **Request a Certificate**



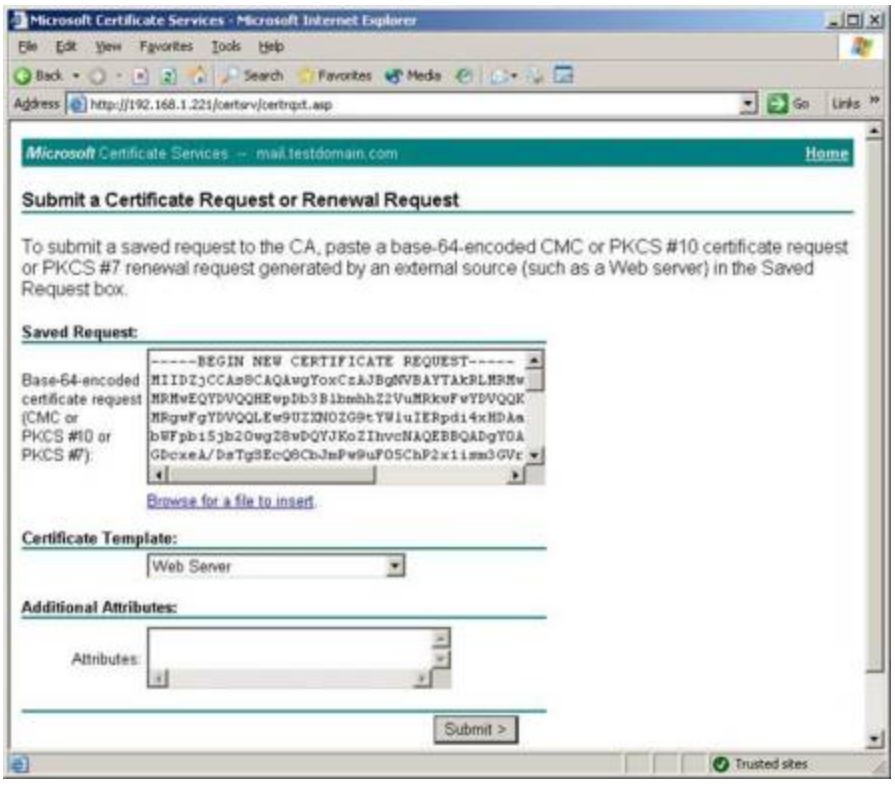
Click **advanced certificate request**



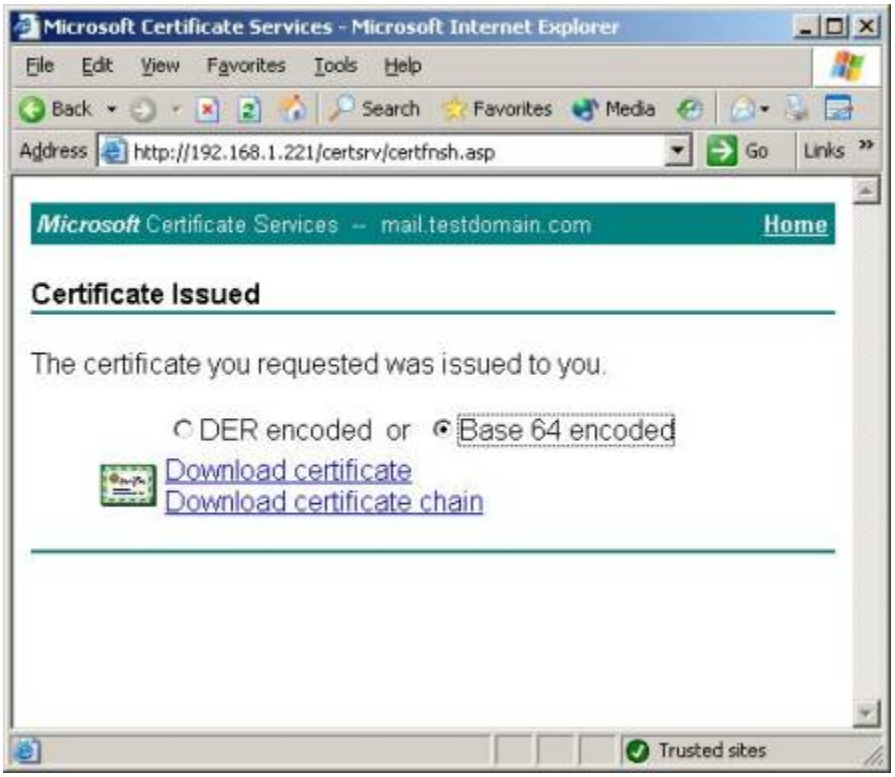
Under **Advanced Certificate Request** click **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**



Now we need to insert the content of the **certreq.txt** file we created earlier, you can do this by clicking the **Browse for a file to insert** or by opening the **certreq.txt** file in notepad, then copy/paste the content as shown in the screen below, then click **Submit >**



Now select **Base 64 encoded** then click **Download certificate**



Click **Save**

Choose to save the **certnew.cer** on the **C: drive** > then click **Save**

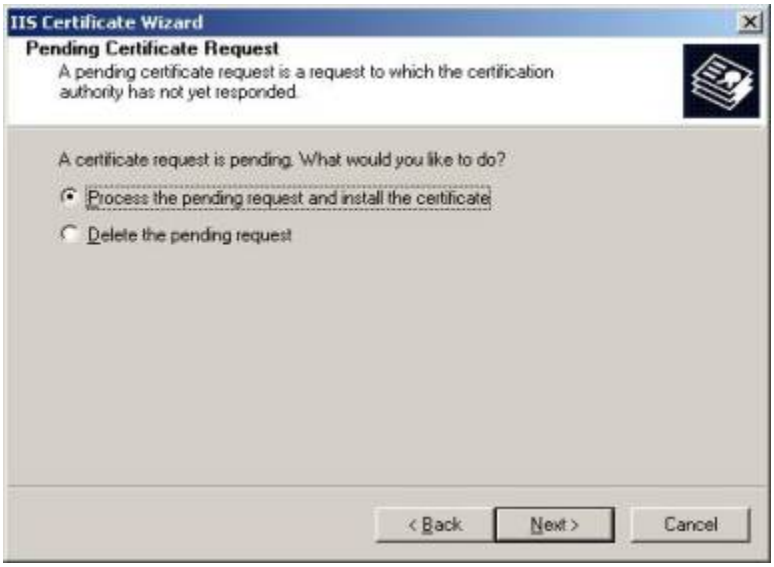
Close the **Microsoft Certificate Services IE window**.

Appending the Certificate to the Default Website

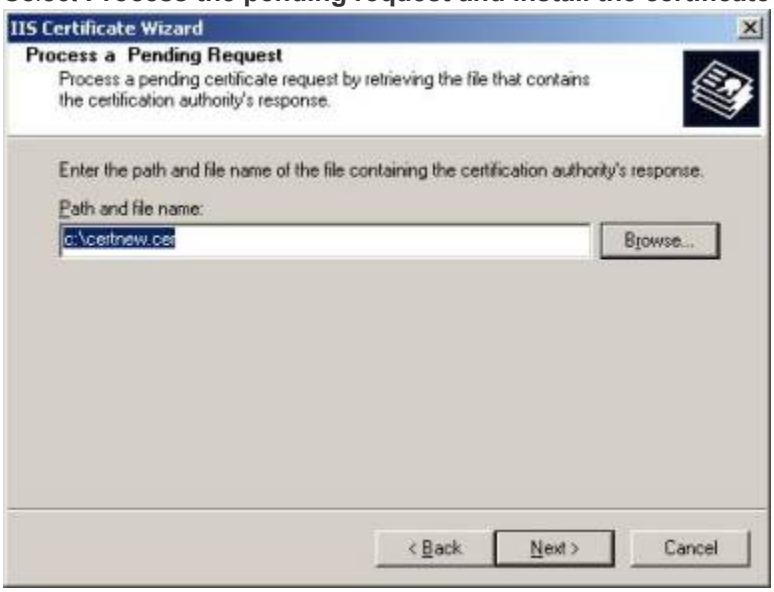
Okay it's time to append the approved Certificate to our Default Website, to accomplish this we need to do the following:

- Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**

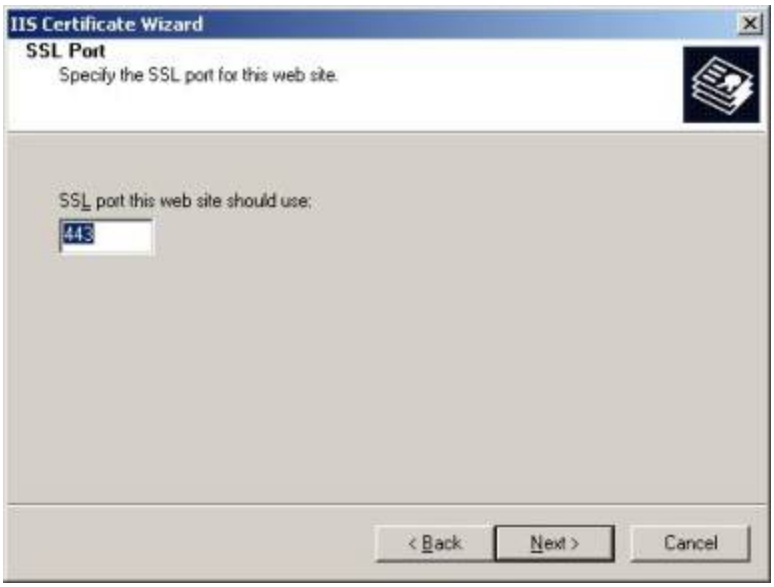
- Expand **Websites** > Right-click **Default Website** then select **Properties**
- Now select the **Directory Security** tab
- Under **Secure Communications** click **Server Certificate…** > then **Next**



Select **Process the pending request and install the certificate** > click **Next >**



Unless you have any specific requirements to what port SSL should run at, leave the default (443) untouched, then click **Next >**



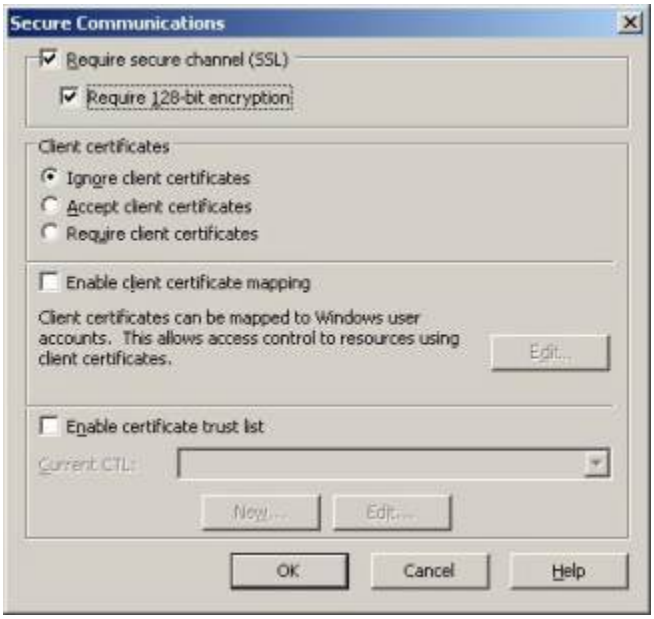
You will now see a summary of the Certificate, again if you should have made any mistakes during the previous wizard screens, this is the final chance to correct them, otherwise just click **Next >**

The Certificate has now been successfully installed and you can click **Finish**

Enabling SSL on the Default Website

We have now appended the Certificate to our Default Website, but before the data transmitted between the clients and the server is encrypted, we need to click the Edit… button under Secure Communications.

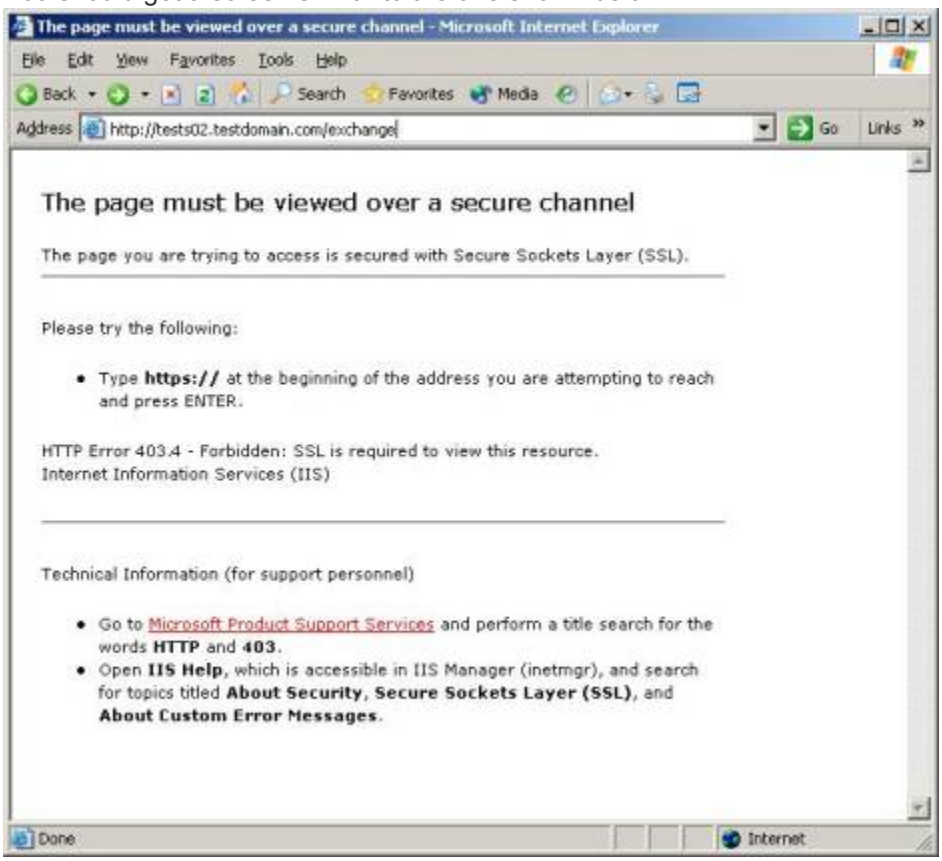
Here we should put a checkmark in Require Secure Channel (SSL) and Require 128-bit encryption just like below:



Now click **OK**.

Testing our SSL enabled Default Website

Now that we have gone through all the configuration steps necessary to enable SSL on our Default Website, it's time to test if our configuration actually works.
From the server (or a client) open Internet Explorer, then type:
http://exchange_server/exchange
You should get a screen similar to the one shown below:



This is absolutely fine, as we shouldn't be allowed to access the Default Website (and any virtual folders below) through an unsecure connection. Instead we should make a secure connetion which is done by typing **https**, therefore type below URL instead:
https://exchange_server/exchange
The following box should appear:

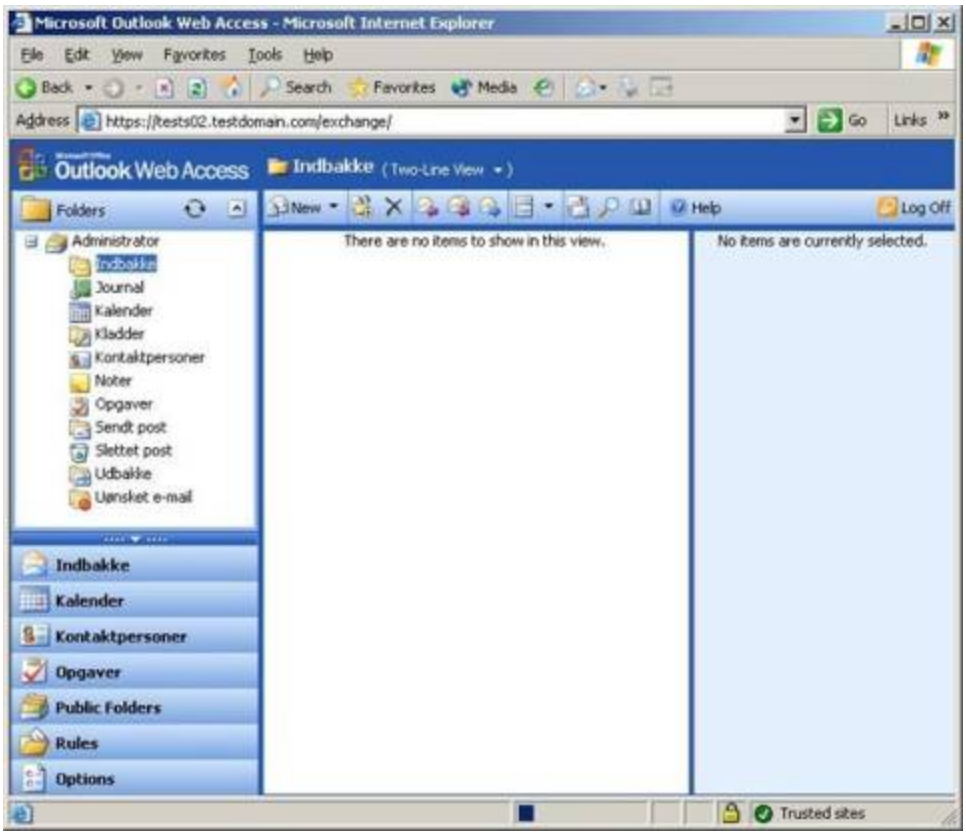
Note: *You may have noticed the yellow warning sign, this informs us* ***The name on the security certificate is invalid or does not match the name of the site****. Don't worry there's nothing wrong with this, the reason why it appears is because we aren't accessing OWA through the common name, which we specified when the certificate was created. When you access OWA from an external client through* ***mail.testdomain.com/exchange****, this warning will disappear.*

Click **Yes**

You will now be prompted for a valid username/password in order to enter your mailbox, for testing purposes just use the administrator account, like shown below:

Now click **OK**

We should now see the Administrator mailbox.



Notice the yellow padlock in the lower right corner, a locked padlock indicates a secure connection, which means OWA now uses SSL.