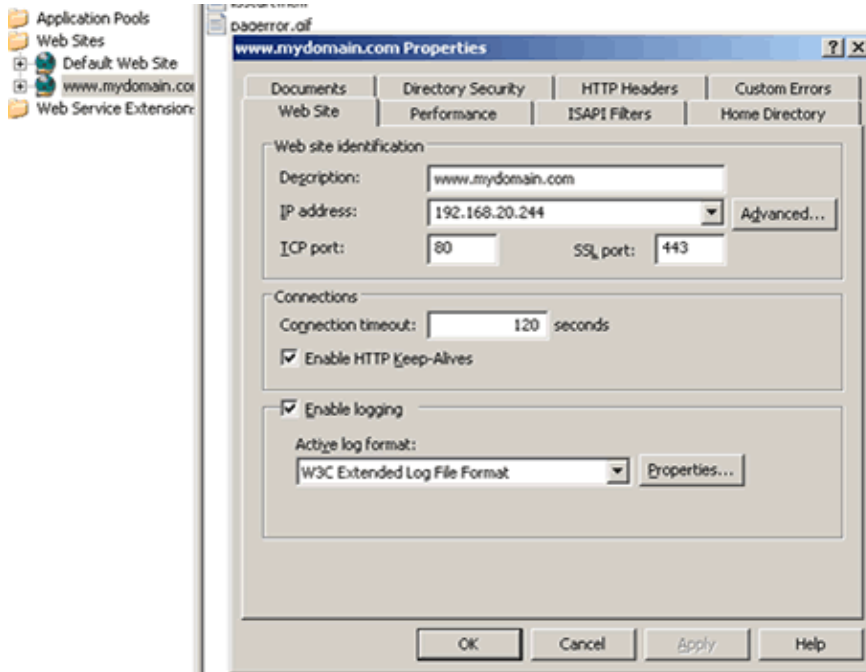


CSR Generation Process

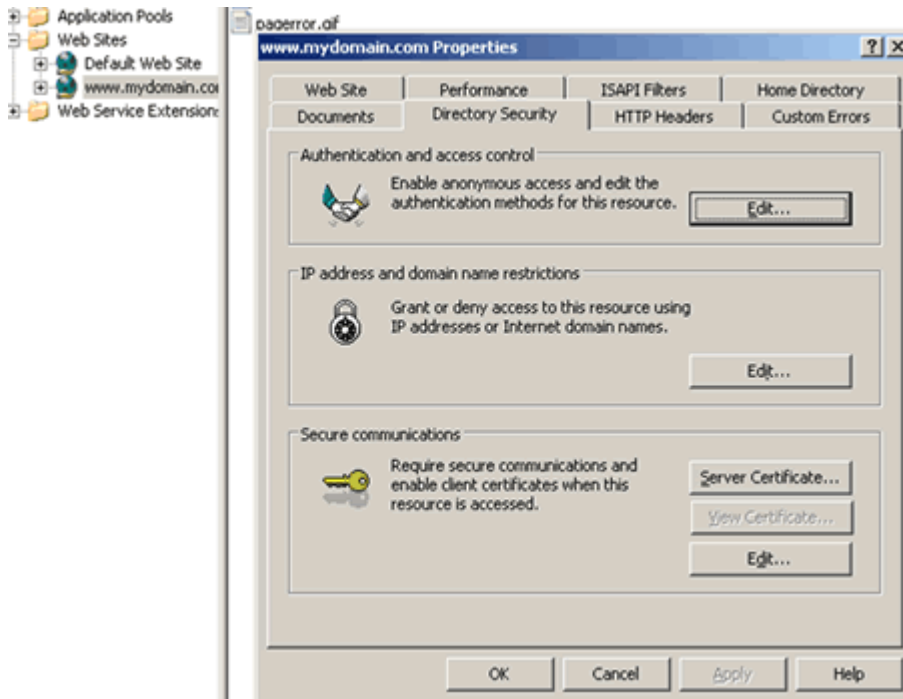
1. Start the Key/CSR Generation Process:

Under Administrative Tools, open the Internet Services Manager. Then open the properties window for the website for which you wish to request the certificate. Right-clicking on the particular website will open up its properties.



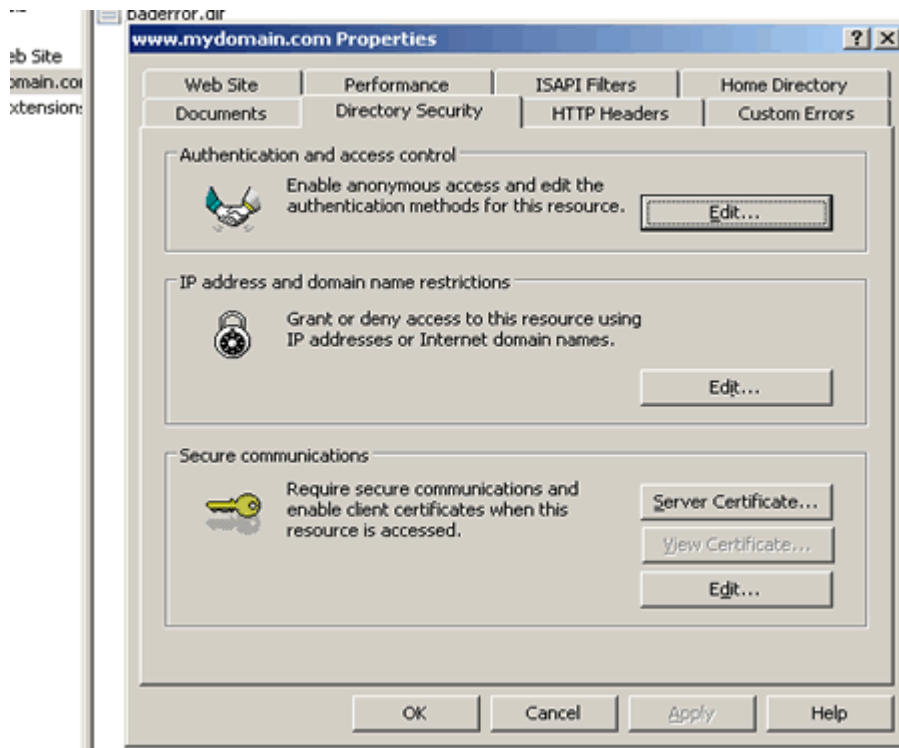
2. Click the Directory Security tab

Click the Directory Security tab and then click on the "Server Certificate" button in the Secure communications section. This will start the Web Site Certificate Wizard.



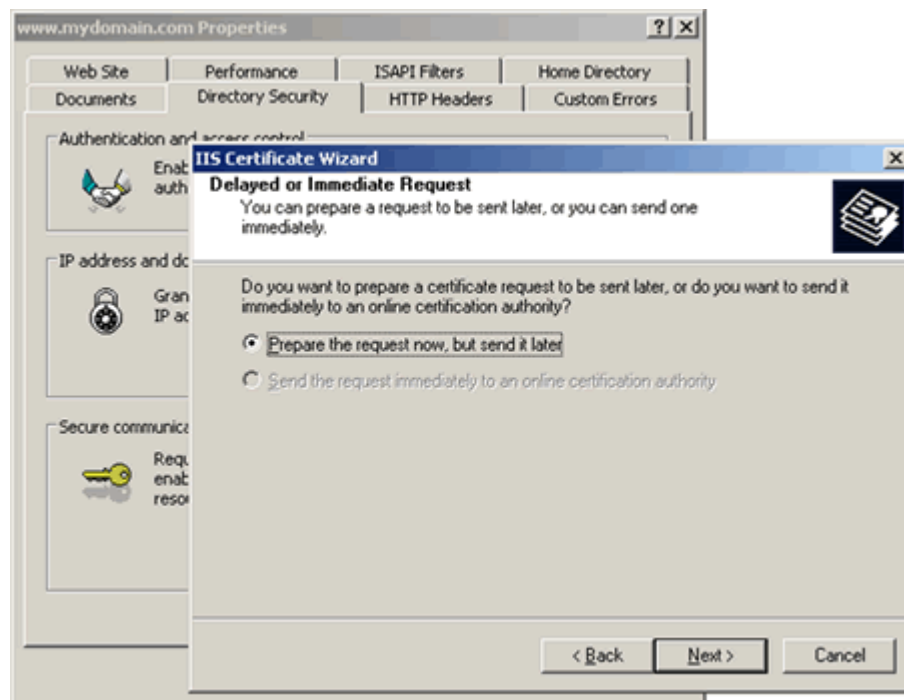
3. Select "Create a new certificate"

From the Web Site Certificate Wizard, select the "Create a new Certificate" option.



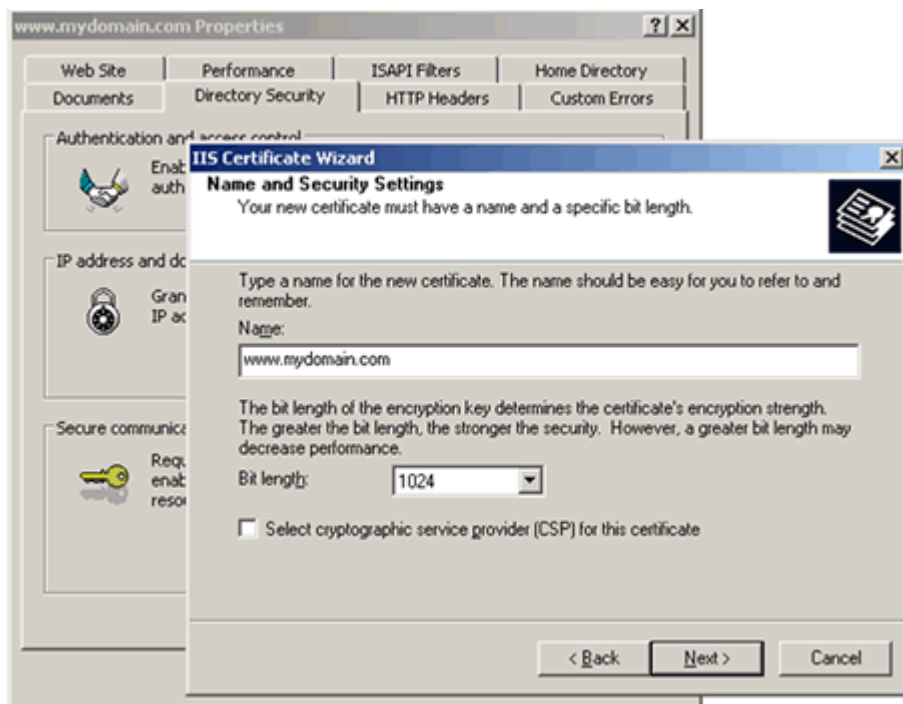
4. Prepare the request

Select the "Prepare the request now, but send it later" option from the list. You will need to prepare the request now but will only submit the request (CSR) via our online request forms. We do not accept CSR's via email.



5. Enter a certificate name and the certificate strength

At this point you will decide what encryption strength your private Key and CSR will be set at. It is advised to choose a 1024-bit key size. Please note that you can choose a larger key size although some browsers may have difficulty making a session with a bigger key size. Do not check the option 'Select cryptographic service provider (CSP) for this certificate'.

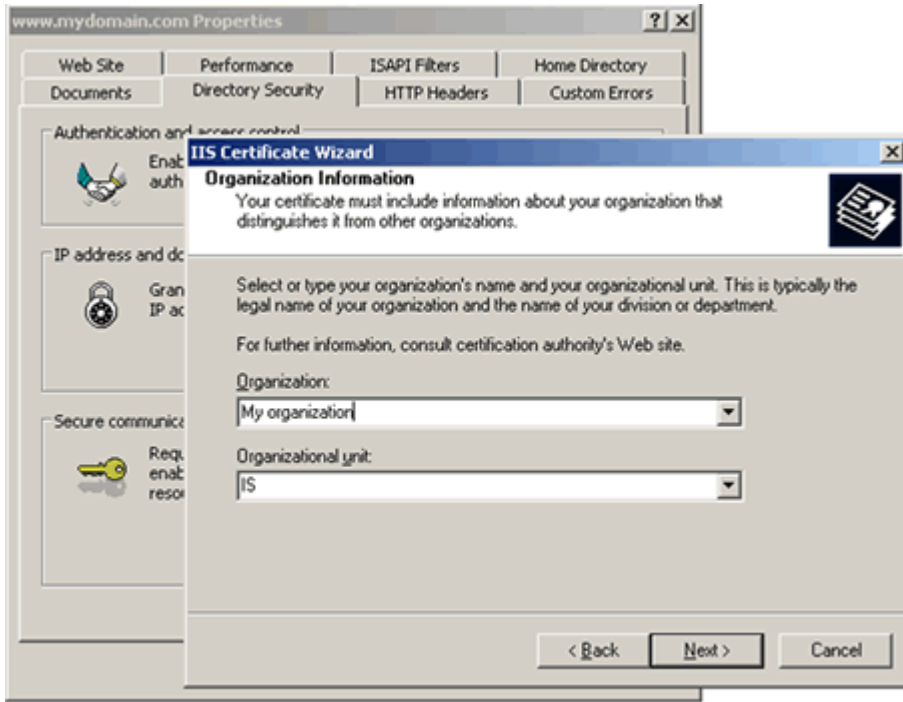


You have now created a public/private key pair. The private key is stored locally on your machine in the MMC, and is used for decryption. The public portion is sent to thawte in the form of a Certificate Signing Request (CSR), and will be used by your users to encrypt the data they send to your site.

You will now create a Certificate Signing Request (CSR). This information will be displayed on your certificate, and identifies the owner of the key to users. The CSR is only used to request the certificate. Certain characters must be excluded from your CSR fields, or your certificate may not work.

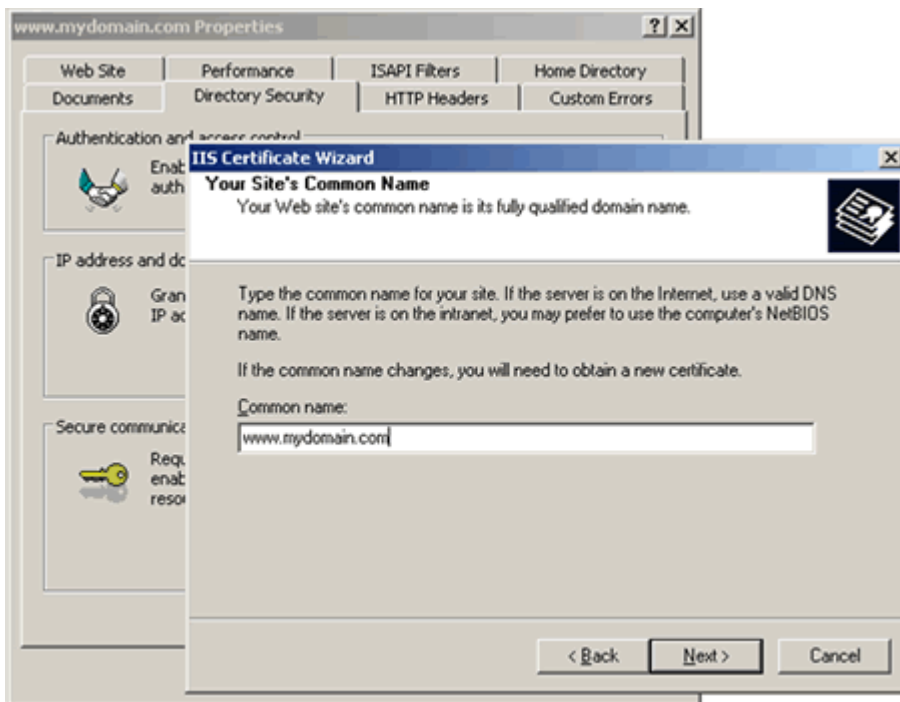
6. Enter your Organization Information

You should enter the company name as it appears on your official company registration documents. The organization unit is optional but IIS 6.0 makes this field compulsory therefore please specify an organization unit.



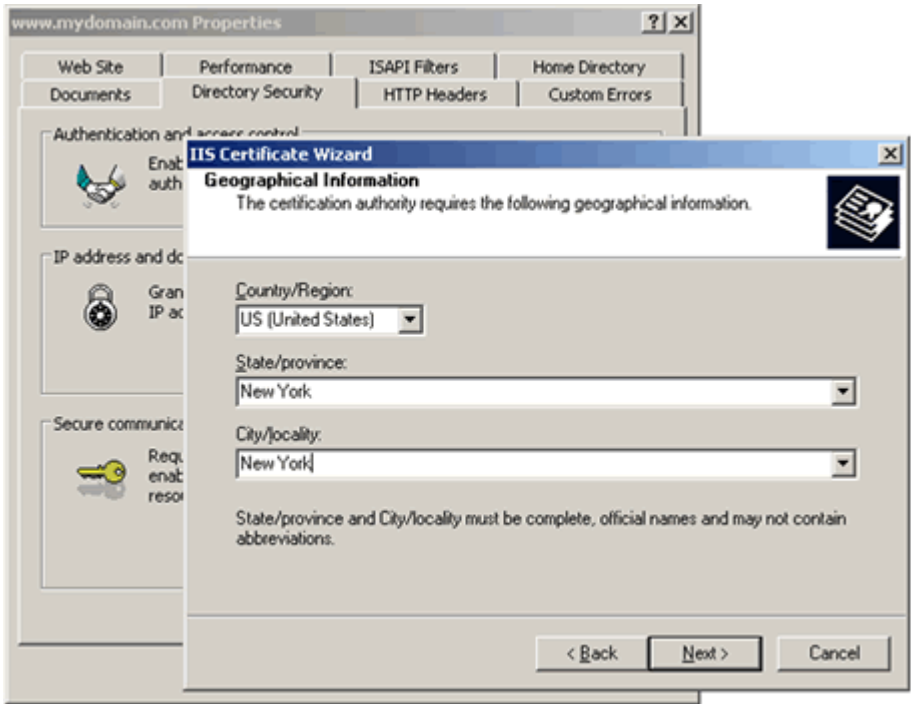
7. Enter your common name

The term "common name" is X.509 speak for the name that distinguishes the certificate best, and ties it to your Organization. Enter your exact host and domain name that you wish to secure. Example: If you wish to secure `www.mydomain.com`, then you will need to enter the exact host (`www`) and domain name (`mydomain.com`) in this field. If you enter `mydomain.com` then the certificate issued to you will only work error free on `https://mydomain.com`. It will cause a certificate mismatch error when you or your users access the domain via `https:// www.mydomain.com`.



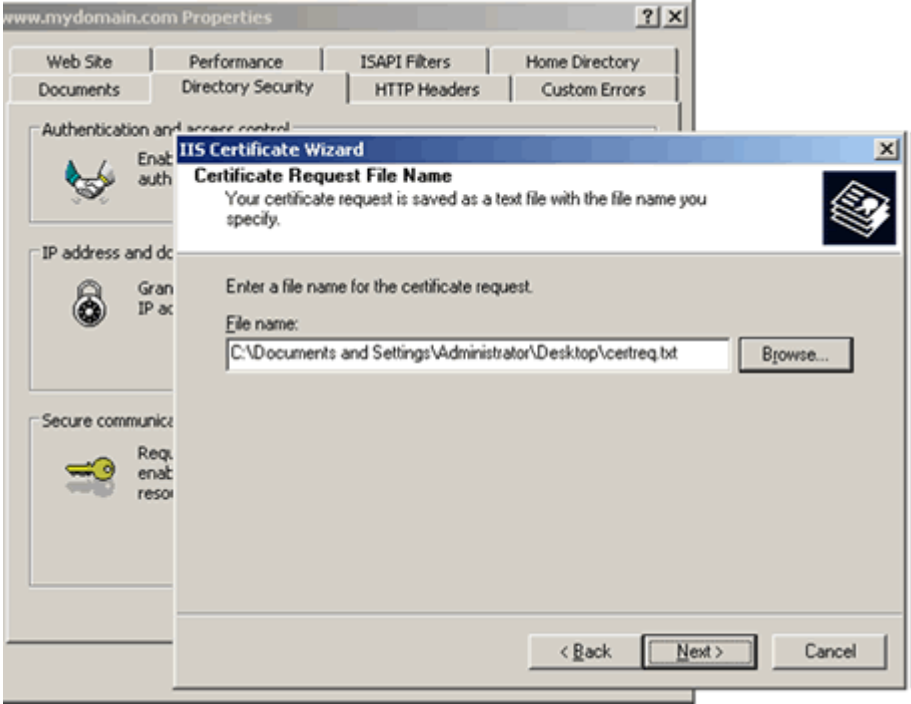
8. Enter the geographical details of your Organization

Enter your country, state or province and locality or city.



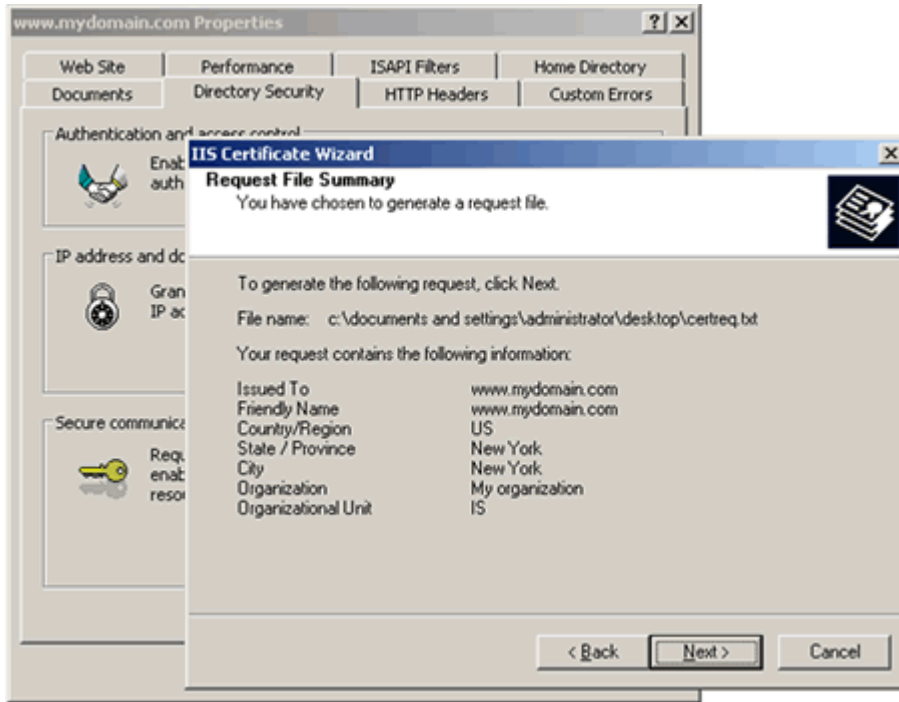
9. Choose a filename to save the request to

Enter the file name for the certificate request (CSR) and the location of where you would like to save the file (we recommend you click the 'browse' button and select a location to save the CSR file to). Then click "Next".



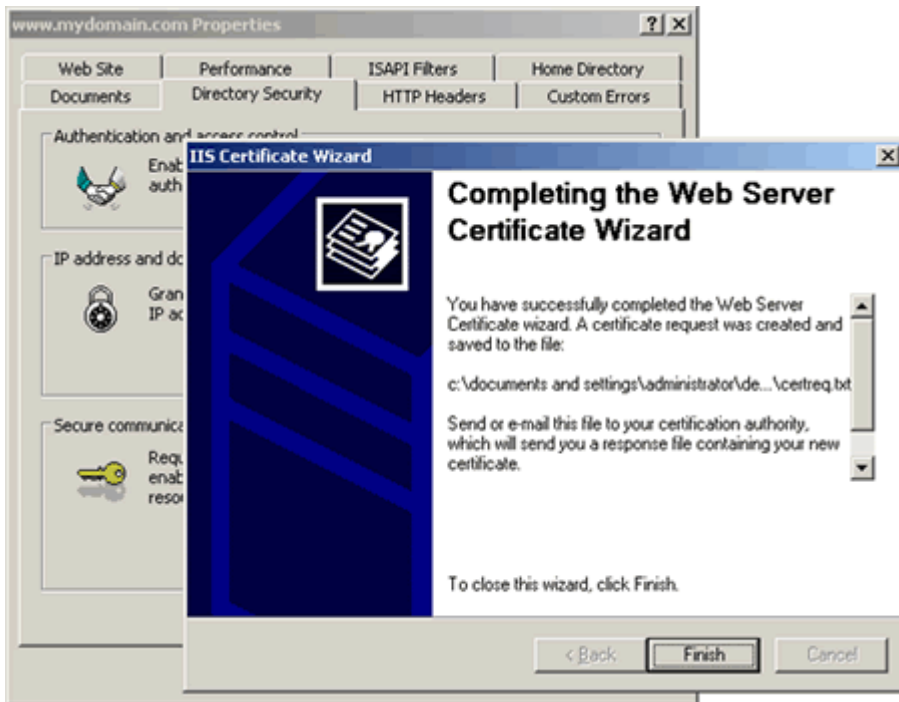
10. Confirm your request details

The next page will display the summary of the certificate request.



11. Finish and exit the IIS Certificate Wizard

Click on 'Finish' to complete the "Web Server Certificate wizard".



12. Backup your private key

If you create a new CSR, or new Key for the same web site, you will overwrite the ones you used to request your certificate. If that happens, you cannot use the certificate we issue you and will need to request a reissue. Please ensure you have a backup of your private key in case it is lost or overwritten.

13. Start the thawte certificate request process

