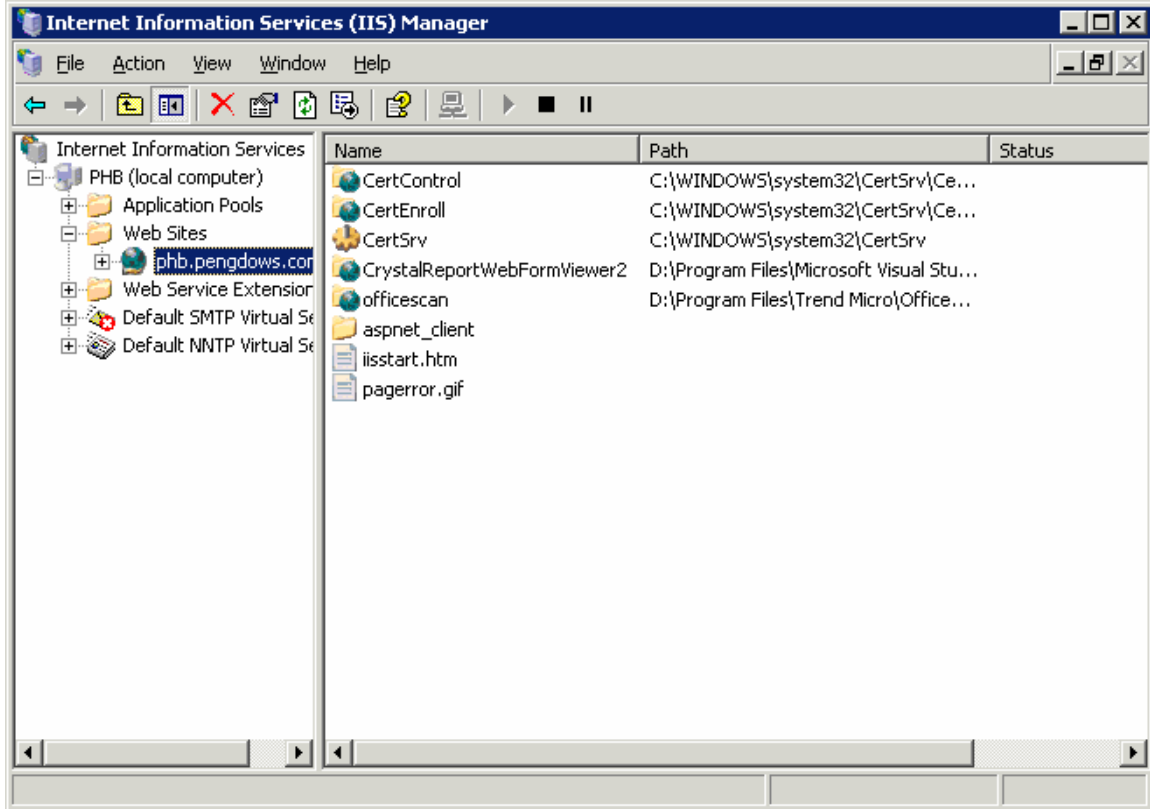
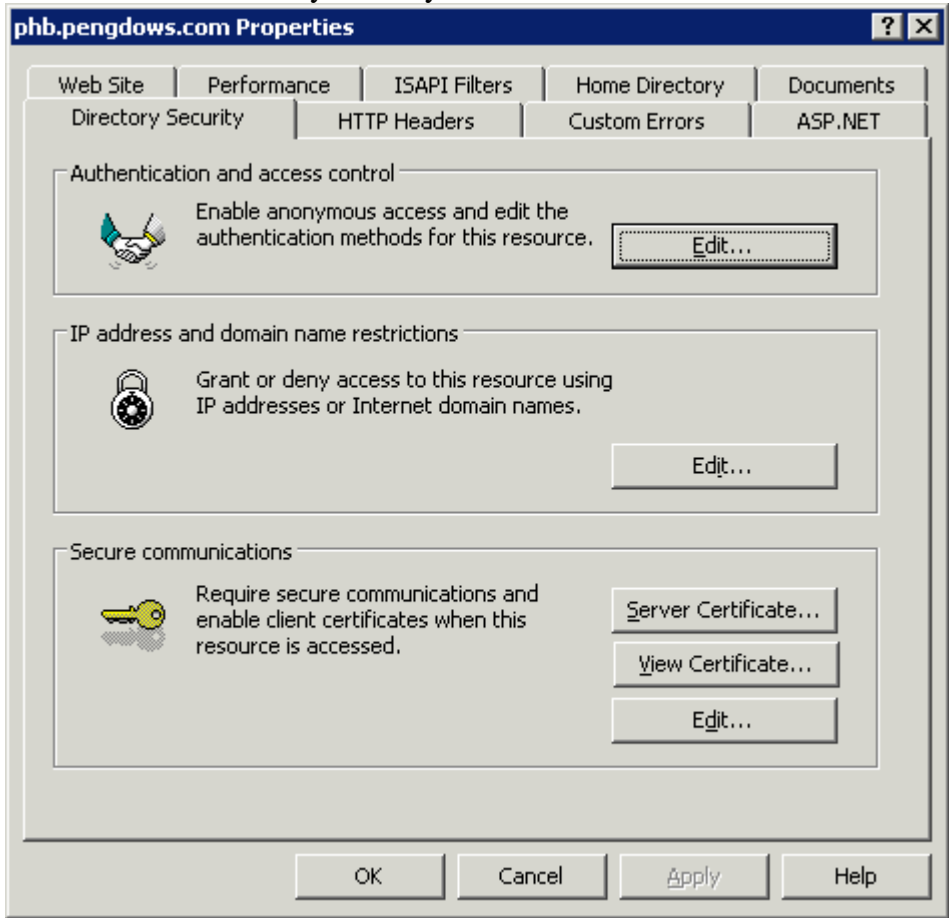


# How to Create a certificate for a website using IIS 6 and CAcert.

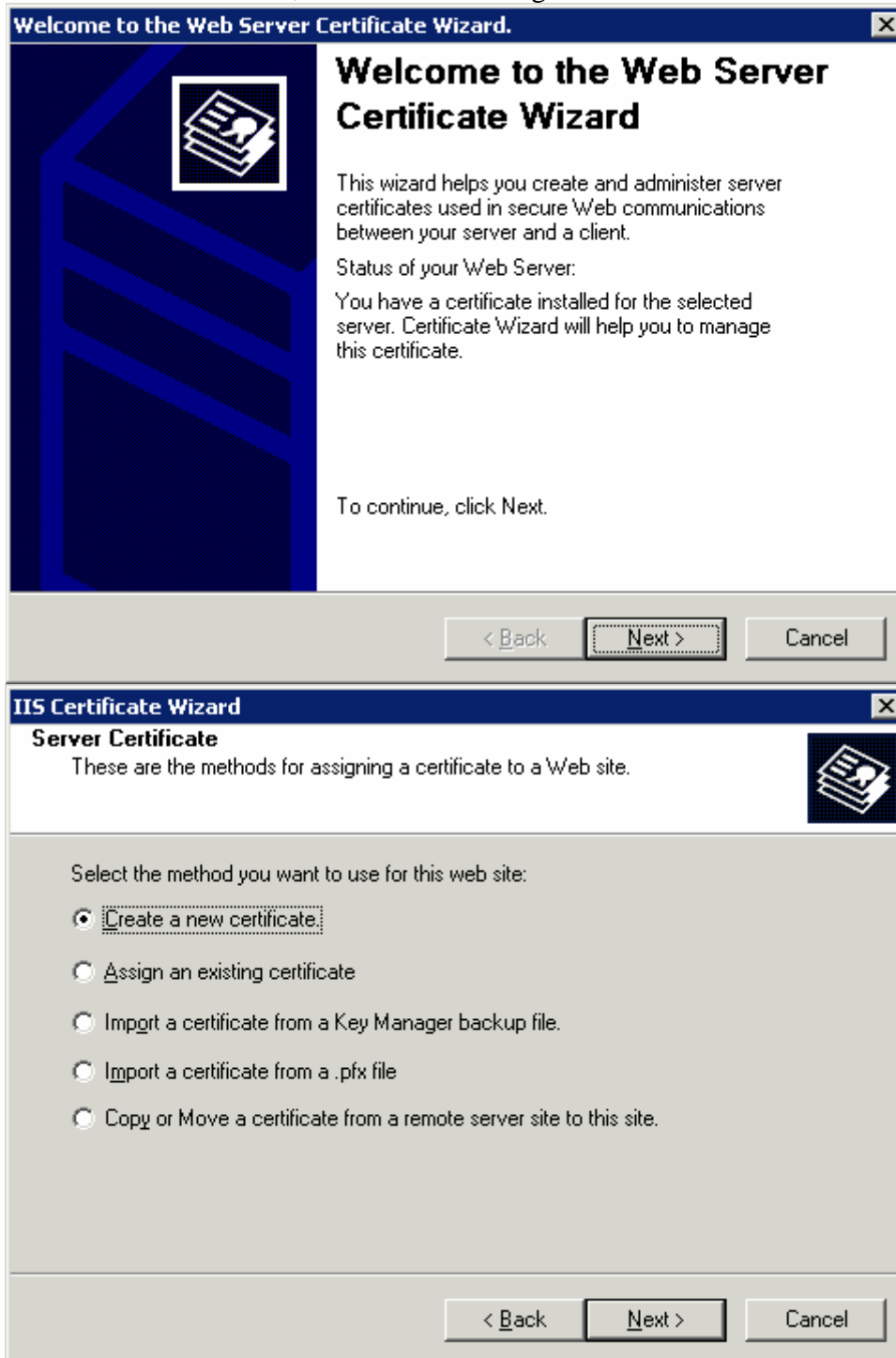
1. Open IIS Manager, then right click on the website you wish to create the cert for.



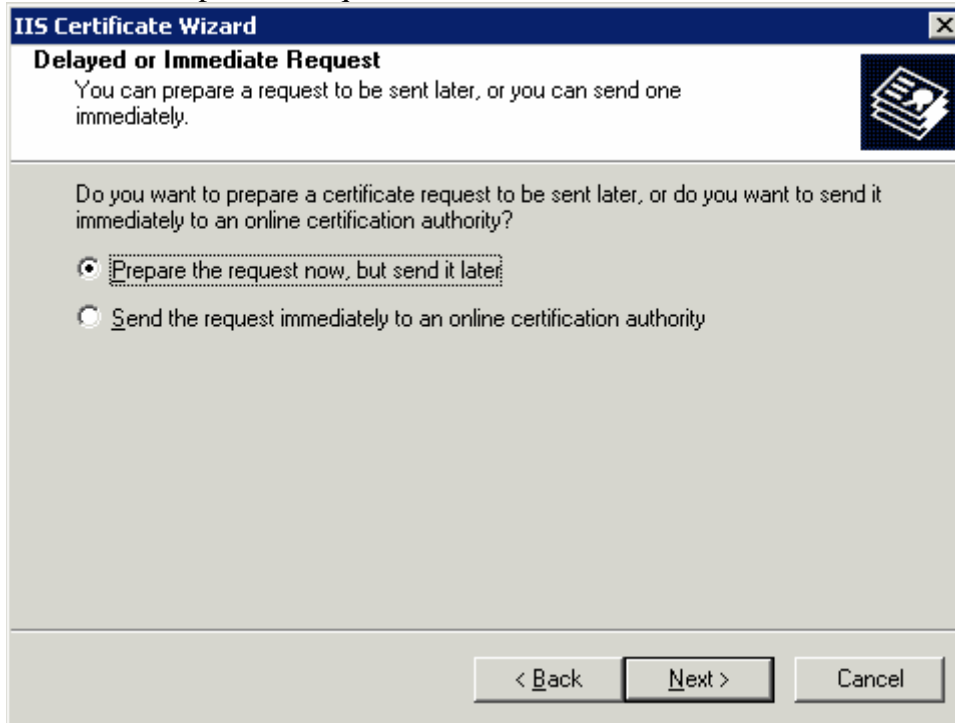
2. Choose the “Directory Security” tab then choose the “Server Certificate” button.



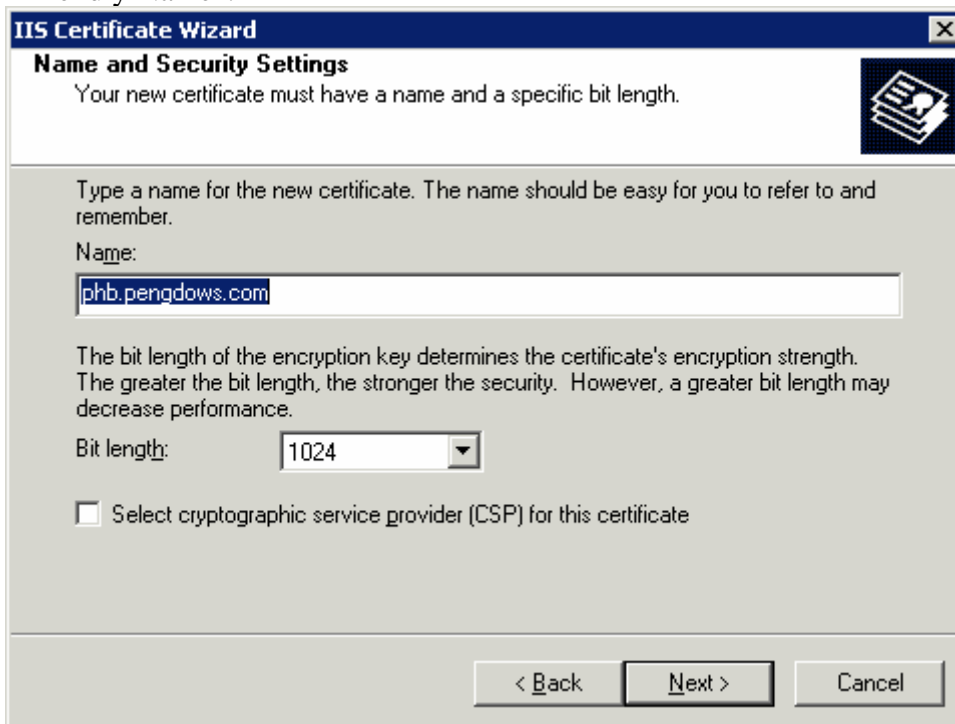
3. Click Next, on the “Welcome” page to the Wizard. Choose the “Create new certificate” radio button, then click “next” again.



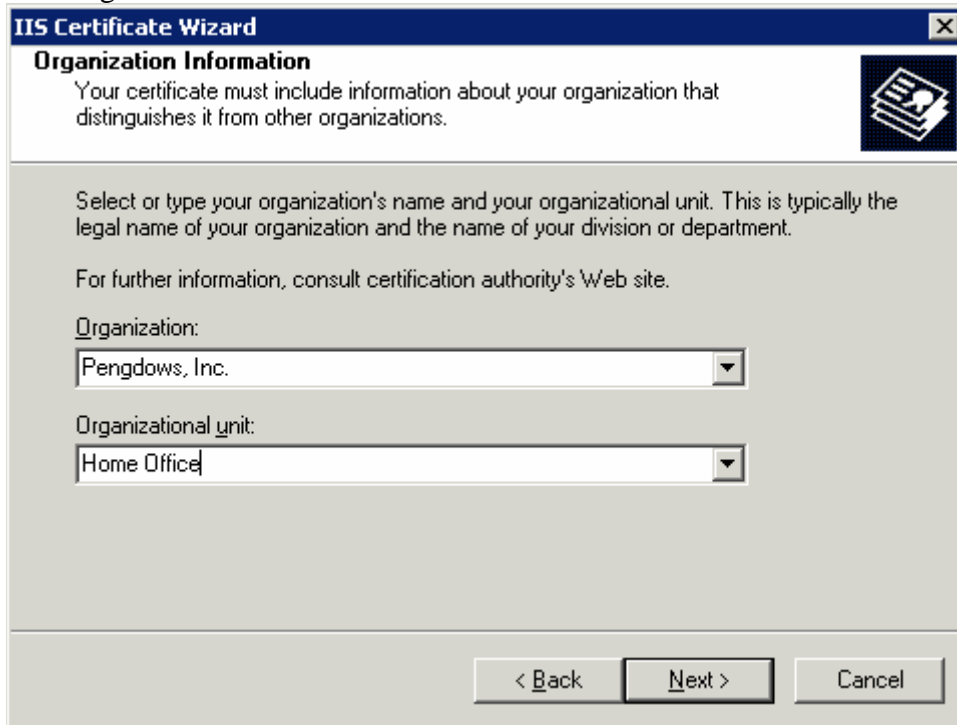
4. Choose “Prepare the request now, but send it later”



5. Enter a name for the cert, this could be anything, Microsoft often refers to this as the “Friendly Name”.

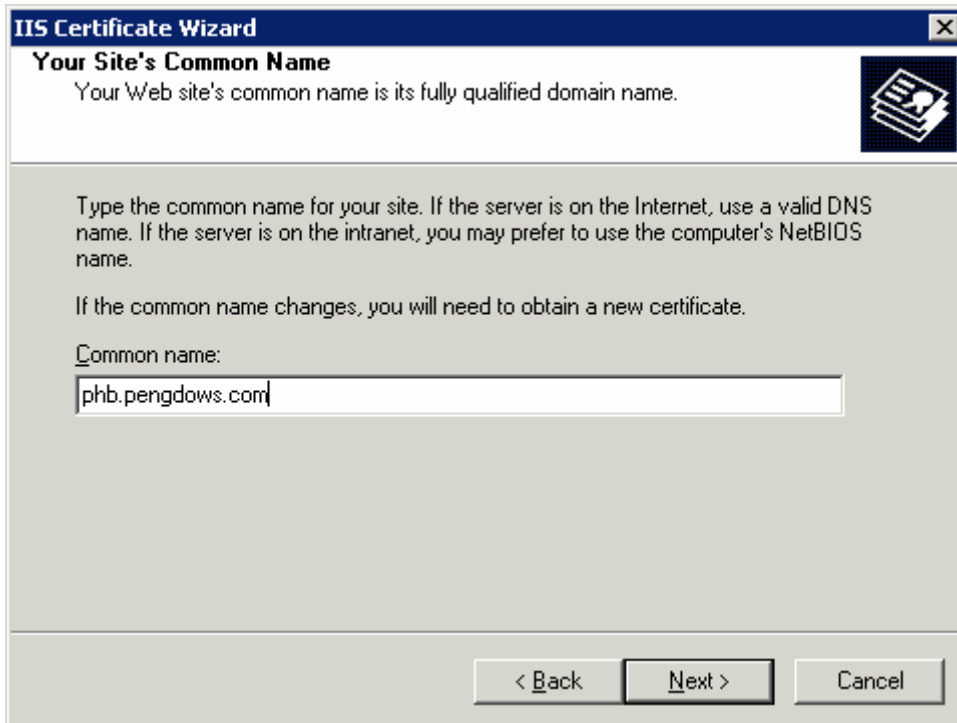


6. Enter something into “Organization” and “Organizational Unit”, these can be anything but are more useful to people who might look at the certificate if you put something meaningful here.



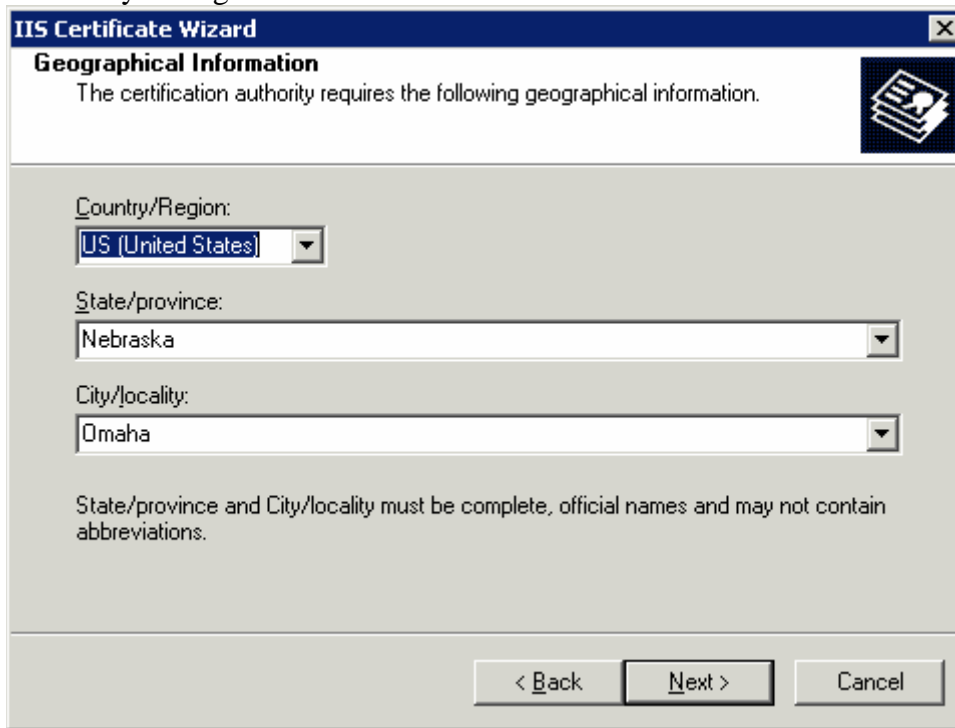
The screenshot shows the 'IIS Certificate Wizard' window at the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Organization Information' with a sub-heading 'Your certificate must include information about your organization that distinguishes it from other organizations.' Below this, there is a text box with instructions: 'Select or type your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.' and a note: 'For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization:' with 'Pengdows, Inc.' selected, and 'Organizational unit:' with 'Home Office' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Enter the common name for your website. (This must be the DNS entry name that the website will be accessed by, at least if you don't to get errors.) Then choose your bit size for the cert.



The screenshot shows the 'IIS Certificate Wizard' window at the 'Your Site's Common Name' step. The title bar reads 'IIS Certificate Wizard'. The main heading is 'Your Site's Common Name' with a sub-heading 'Your Web site's common name is its fully qualified domain name.' Below this, there is a text box with instructions: 'Type the common name for your site. If the server is on the Internet, use a valid DNS name. If the server is on the intranet, you may prefer to use the computer's NetBIOS name.' and a note: 'If the common name changes, you will need to obtain a new certificate.' There is a text input field labeled 'Common name:' containing 'phb.pengdows.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

8. Put in your region info.



**IIS Certificate Wizard**

**Geographical Information**

The certification authority requires the following geographical information.

Country/Region:  
US (United States)

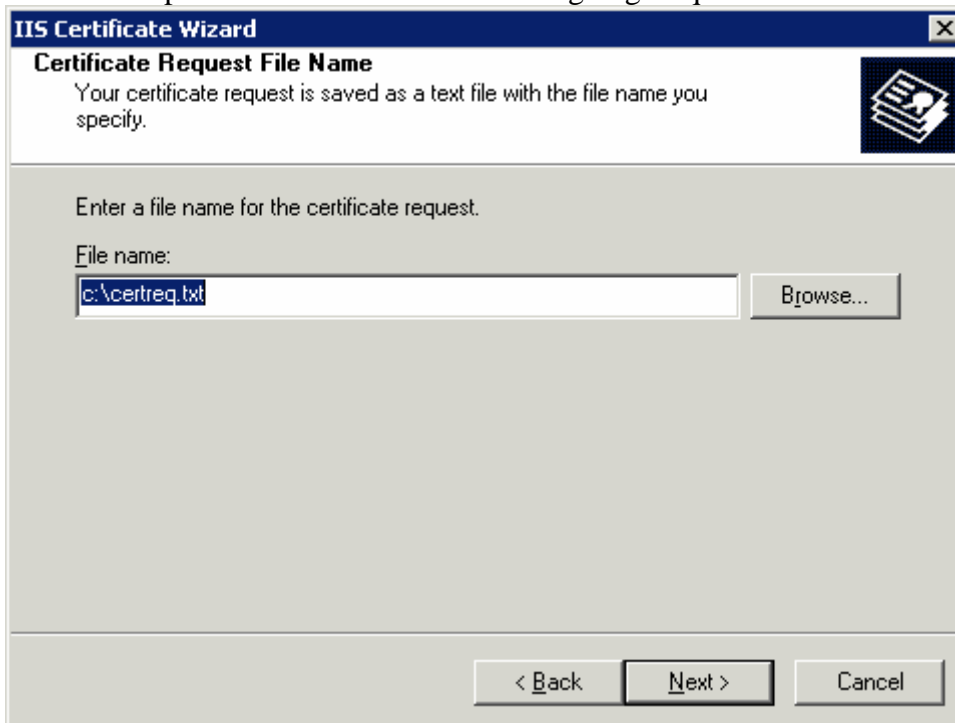
State/province:  
Nebraska

City/locality:  
Omaha

State/province and City/locality must be complete, official names and may not contain abbreviations.

< Back   Next >   Cancel

9. Choose a place to save the “Certificate Signing Request” also known as a CSR.



**IIS Certificate Wizard**

**Certificate Request File Name**

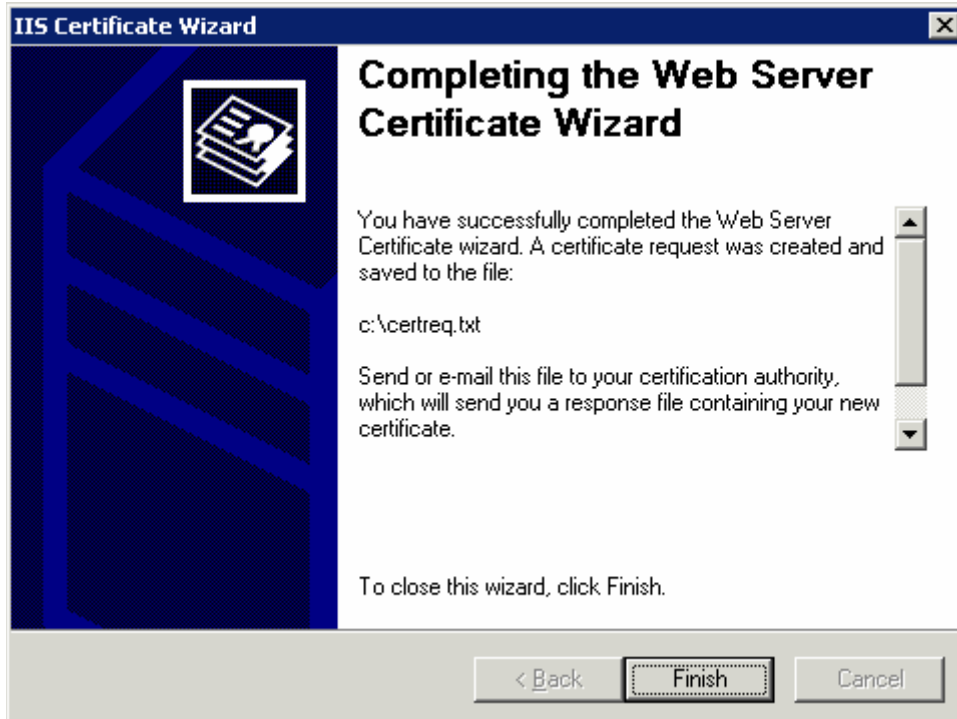
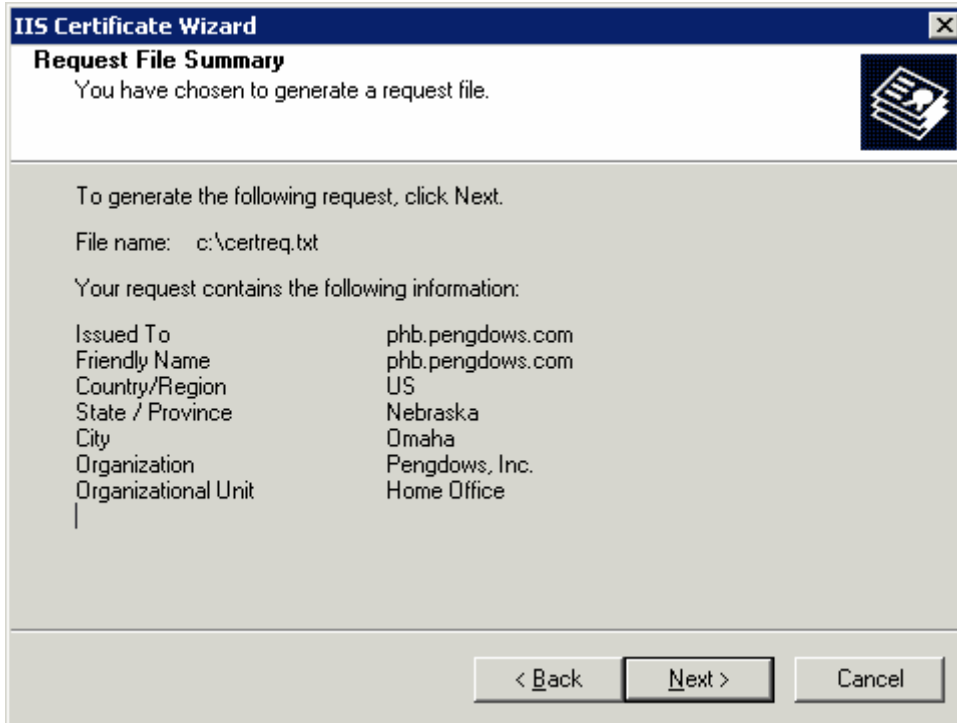
Your certificate request is saved as a text file with the file name you specify.

Enter a file name for the certificate request.

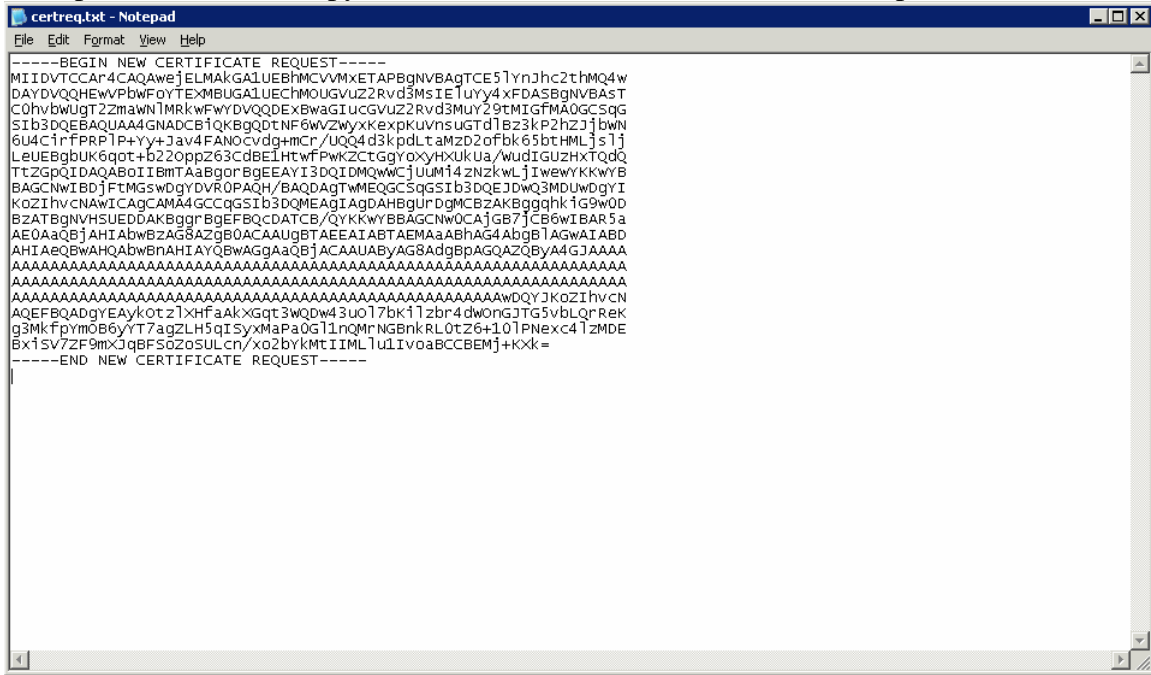
File name:  
c:\certreq.txt   Browse...

< Back   Next >   Cancel

10. Look over the settings, click “back” if anything is wrong to correct it. Otherwise, click “Next” then “Finish”



11. Open the file, then copy the ENTIRE contents of the file to the clipboard.



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVTCCA4CAQAwEjELMAKGA1UEBHMCVVMXETAPBgnVBAgtCE51ynJhc2thM04w
DAYDVQQHEWVpBwF0YTEuMBUgA1UECmOUgVuz2Rvd3MsIE1uyy4xFDA5BgnVBASt
C0hvbwJGT2ZmawNlMRkxwFwydVQQDEXBw3GIucGVUZ2Rvd3Muy29tMIGFMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDENF6wZwYXkexpkUvnsuCTd1Bz3kP2hzj1bwn
6U4C1rFPRP1P+Yy+Jav4FANOCvdg+mcR/UQQ4d3kpdLtaMzD2ofbk65btHMLj31j
LeUEggbUK6qot+b22Oppz63CdBE1HtwfPwKZCTGgyoxyHXkua/wudIGUZHXTQdQ
TTZgpQIDAQABoIIBMTAaBggrBgEEAYI3DQIDMQwCjUUM14zNzkwljIwewyKkwyB
BAGCNwIBDjFTMGswdgyDVR0PAQH/BAQDAgTWMEQGC5qGSIb3DQEJDbQ3MDUwdgyI
KozIhvcnAwICAgCAMAA4GCCqGSIb3DQMEAgIAgDAHBgUrDgMCB2AKBggqhkg9W0D
BZATBgnVHsUEDDAKBgggrBgEFBQcDATCB/QYKkwyBBAGCNw0CAjGB7jEB6wIBAR5a
AEQAAQBJAHIAbwBZAG8AZgB0ACAAUgBTAEAAIABTAEMAaABhAG4AbgB1AGWAIABD
AHIAEQBWAHQAbwBnAHIAYQBWAGgAAQBJACAAUABYAG8AdgBPAQAZQBYA4GJAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAWdQYjKozIhvcn
AQEFBQADgYEAYkOtz1XHfAakXgqt3WQDw43uo17bk11zbr4dwongJTG5vblQrReK
g3MkFpYm0B6yY77agZLH5qISyMaPa0G11nQMNGbnkRL0tZ6+101PnExc41ZMDE
Bx15v7ZF9mxJqBFS0z0SULcn/xo2bykmtIIML1uL1voabCCBEMj+kXk=
-----END NEW CERTIFICATE REQUEST-----
```

12. Login to the CAcert website, choose ‘‘Server Certificates’’ then choose ‘‘New’’, then paste into the text box the copy of the clipboard. Make sure it looks exactly like the file, no extra lines. Then Click Submit.

**CAcert** **Free digital certificates!**

**CAcert Certificate Acceptable Use Policy**

Once you decide to subscribe for an SSL Server Certificate you will need to complete this agreement. Please read it carefully. Your Certificate Request can only be processed with your acceptance and understanding of this agreement.

I hereby represent that I am fully authorized by the owner of the information contained in the CSR sent to CAcert Inc. to apply for an Digital Certificate for secure and authenticated electronic transactions. I understand that a digital certificate serves to identify the Subscriber for the purposes of electronic communication and that the management of the private keys associated with such certificates is the responsibility of the subscriber's technical staff and/or contractors.

CAcert Inc.'s public certification services are governed by a CPS as amended from time to time which is incorporated into this Agreement by reference. The Subscriber will use the SSL Server Certificate in accordance with CAcert Inc.'s CPS and supporting documentation published at <http://www.cacert.org/docs/>

If the Subscriber's name and/or domain name registration change the subscriber will immediately inform CAcert Inc. who shall revoke the digital certificate. When the Digital Certificate expires or is revoked the company will permanently remove the certificate from the server on which it is installed and will not use it for any purpose thereafter. The person responsible for key management and security is fully authorized to install and utilize the certificate to represent this organization's electronic presence.

\*\*\* Please Note. All information on your certificate will be removed except the CommonName field, this is because it's an automated service and cannot automatically verify other details on your certificates are valid or not. If you are a valid organisation and would like more details to appear on certificates, you will need to have at least 50 assurance points and you need to send us a copy of your document of incorporation. Then we can add those details to your certificates. Contact us for more information on our organisational services.\*\*\*

Sign by class 1 root certificate  
 Sign by class 3 root certificate

Please note: The class 3 root certificate needs to be setup in your webserver as a chained certificate, while slightly more complicated to setup, this root certificate is more likely to be trusted by more people.

Paste your CSR below...

```

6U4ClrfrPR1P=YY+Jav4FAN0cvdq+mCz/UQ4d3kpdLtaMzD2ofbk6SbtHMLj_s1j
LeUEBgbUR6qot+b22OppZ63CdBE1HtwfPwKZCtGgYoXyHXKUa/WudIGUzHxTQdQ
T+2GpQIDAQABoIIBmTAABoBQEAAI3DQIDMgWtCjUuM14znzkLjIwevYKkwyB
BACNwIBDjFtMgsvDgYDVR0PAQH/BAQDAgTwMEQCSqGSIlb3DQEJdWQ3MDUwDgYI
KoZlHvcNAwIcAgCAMA4GCCqGSIlb3DQMEAgTAgDAHBgUzDgMCEzAKBggqhkiG9w0D
BzATBgnVHsUEDDARBggrBgEFBQcDQATCB/ QYKkwYBBAGCNw0CaJGB7jCB6wIBAR5a
AE0aQBJAHtbwBzAGSAZG8GACAAUgSTAEFAIABTAEMAaABnAG4AbgSIAgwaIABD
hIIEAQwAHQzWwBzAHIIY0wAgBaQBJACMAUByAGSAZG8GACAAUgSTAEFAIABTAEMA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAWDOYJKoZIhvcN
AQEFBQADgYEAYkCtZlXhfakXGqt3WQDw43u017bKl1zb4dW0nGJT5vblQrReK
g3MKfpYm0B6yYT7agZLH5qISyxMaPa0G11nQMtrNGbnkRLotZ6+10LFFNexc4lzMDE
BxiSV7ZF9mXJgBFS0ZoSULcn/xo2bYkMcIIML1uIv0aBCCBEMj+KXk=
-----END NEW CERTIFICATE REQUEST-----
    
```

Submit

[About Us](#) | [Donations](#) | [Privacy Policy](#) | [Contact Us](#) | ©2002-2005 by CAcert

CAcert.org  
Go Home  
Logout

+ My Details

+ Email Accounts

+ Client Certificates

+ Domains

+ Server Certificates  
New  
View

+ CAcert Web of Trust

+ GPG/PGP Keys

+ Disputes/Abuses

13. Verify the Common name, then click ‘‘submit’’

**CAcert** **Free digital certificates!**

Please make sure the following details are correct before proceeding any further.

CommonName: phb.pengdows.com  
 No additional information will be included on certificates because it can not be automatically checked by the system.

Submit

[About Us](#) | [Donations](#) | [Privacy Policy](#) | [Contact Us](#) | ©2002-2005 by CAcert

CAcert.org  
Go Home  
Logout

+ My Details

+ Email Accounts

+ Client Certificates

+ Domains

+ Server Certificates  
New  
View

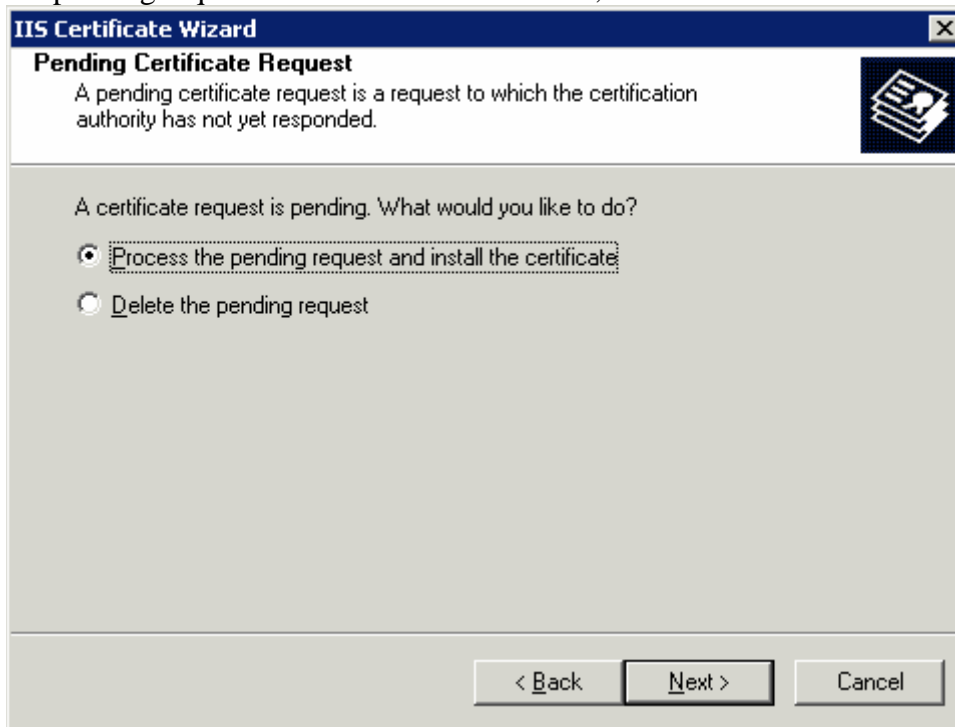
+ CAcert Web of Trust

+ GPG/PGP Keys

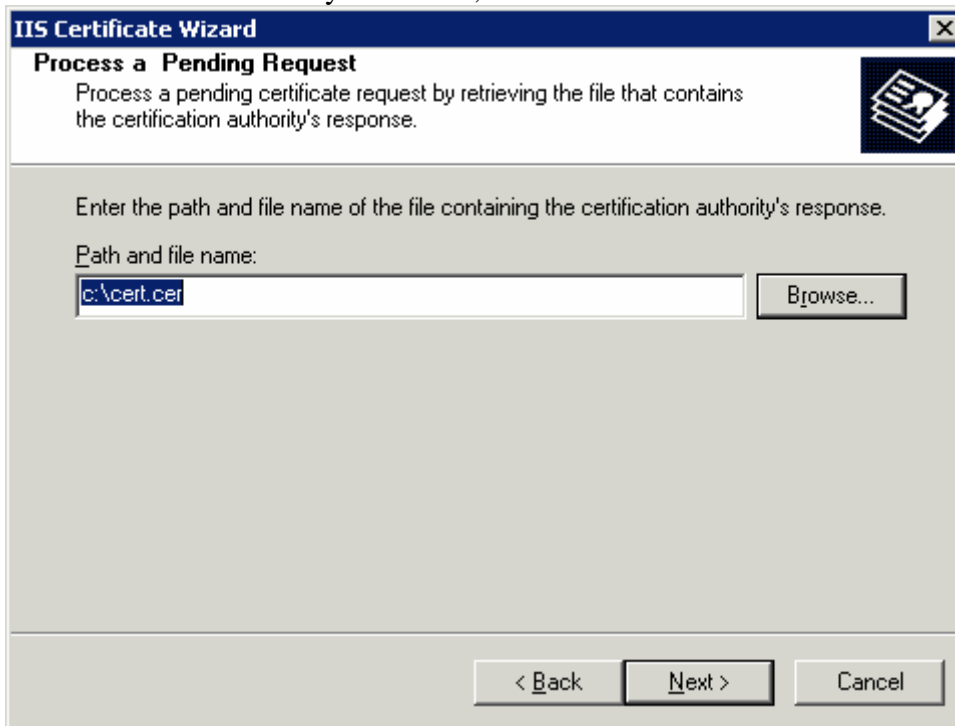
+ Disputes/Abuses



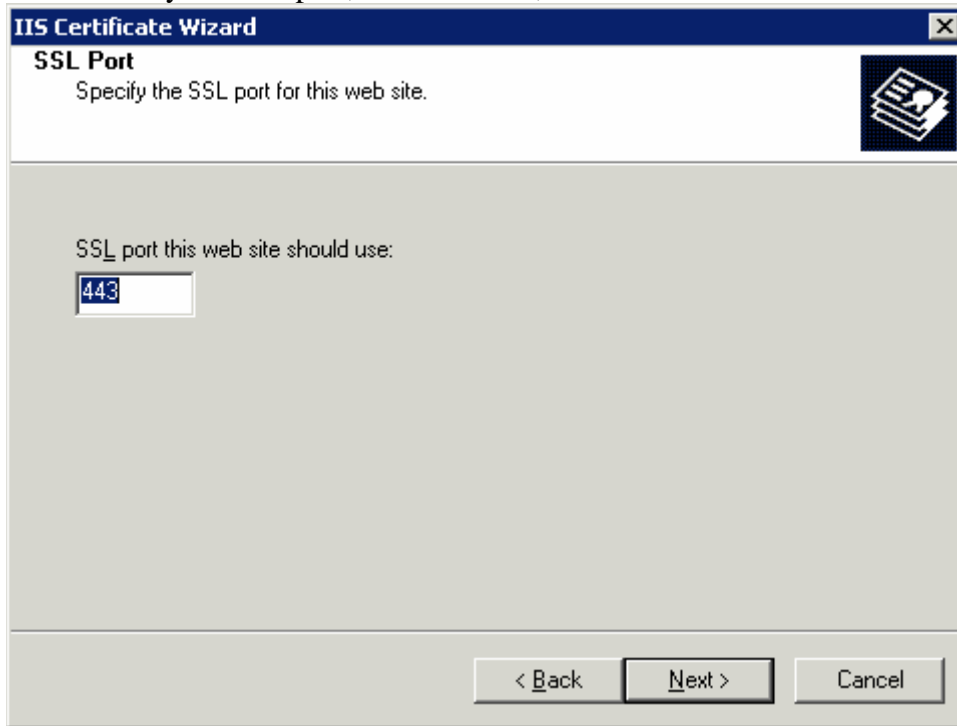
15. Go back to IISAdmin and right click on the website again, going back to the “directory security” tab and, click “Next” on the welcome screen, then choose “Process the pending request and install the certificate”, then click “next”.



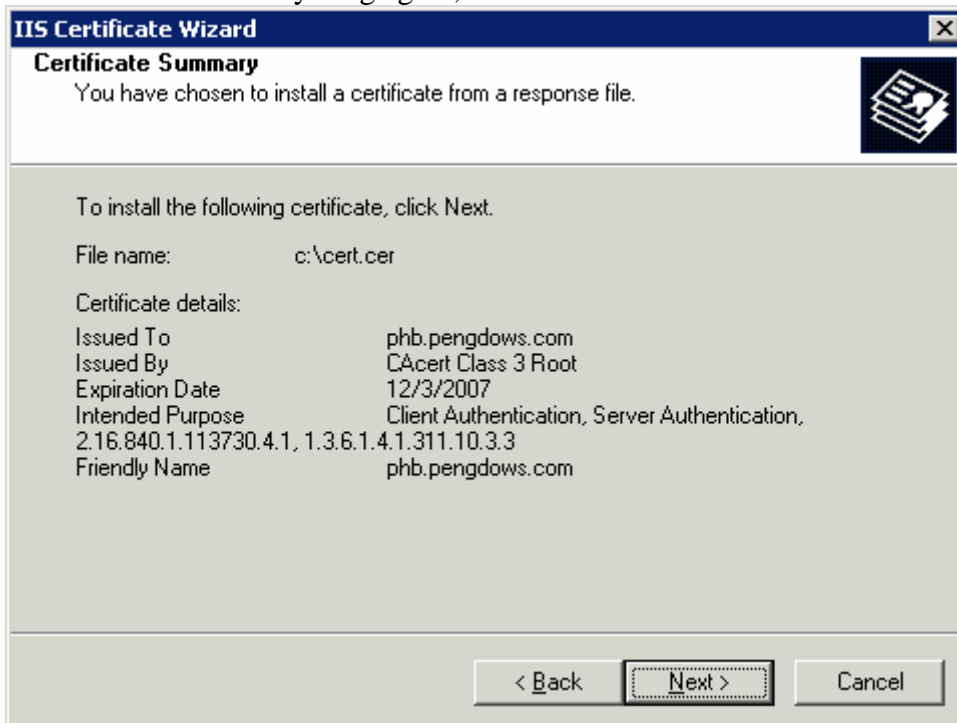
16. Choose the filename you created, then click “next”



17. Choose your SSL port, is the Default, then click “Next”



18. Double check everything again, then click “Next”.



20. Click “Finish”, then close out of IIS Admin.

