e-Cert (Server) User Guide

For Microsoft IIS 5.0 / 6.0
For SHA-1 e-Cert(Server) Only

Revision Date: Dec 2014

Table of Content

A. Guidelines for e-Cert (Server) Applicant

After receipt and approval of an e-Cert (Server) application, Hongkong Post Certification Authority will send an e-mail with subject "Submission of Certificate Signing Request (CSR)" to request the applicant (i.e. the Authorized Representative) to submit the CSR at the Hongkong Post CA web site.

This user guide is for reference by applicants of e-Cert (Server) in generating their key pair and Certificate Signing Request (CSR) using Microsoft IIS 5.0 / 6.0 on Windows 2000 / 2003. The CSR containing the public key will then be submitted to Hongkong Post Certification Authority for certificate signing.

If you lose the private key after the certificate is issued, you will be unable to install or use the certificate. Therefore, it is strongly recommended that you should backup the private key **before the submission of the Certificate Signing Request (CSR)** and **after the installation of the server certificate**. To learn the backup and restore procedures of the private key, please follow the instructions as described in the following sections:

New Application

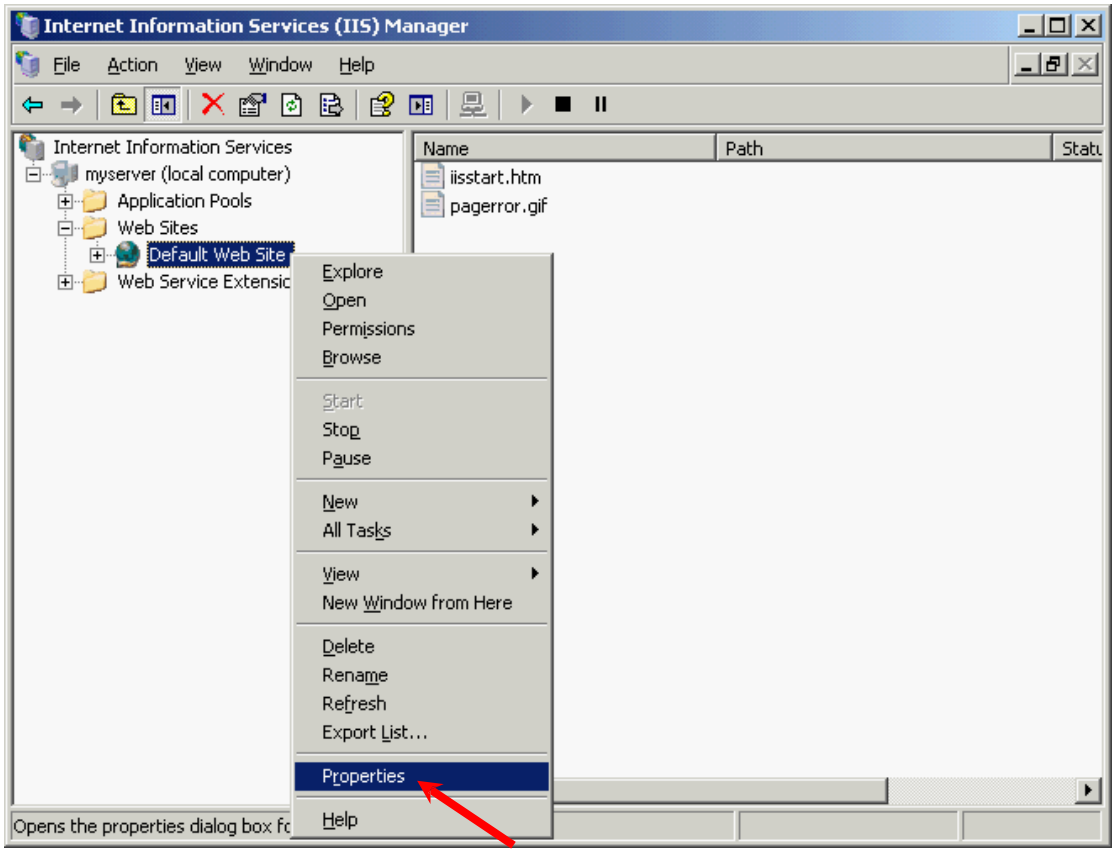
If this is the first time you apply for e-Cert (Server), please follow the instructions as described in the following sections:

Renewal Application

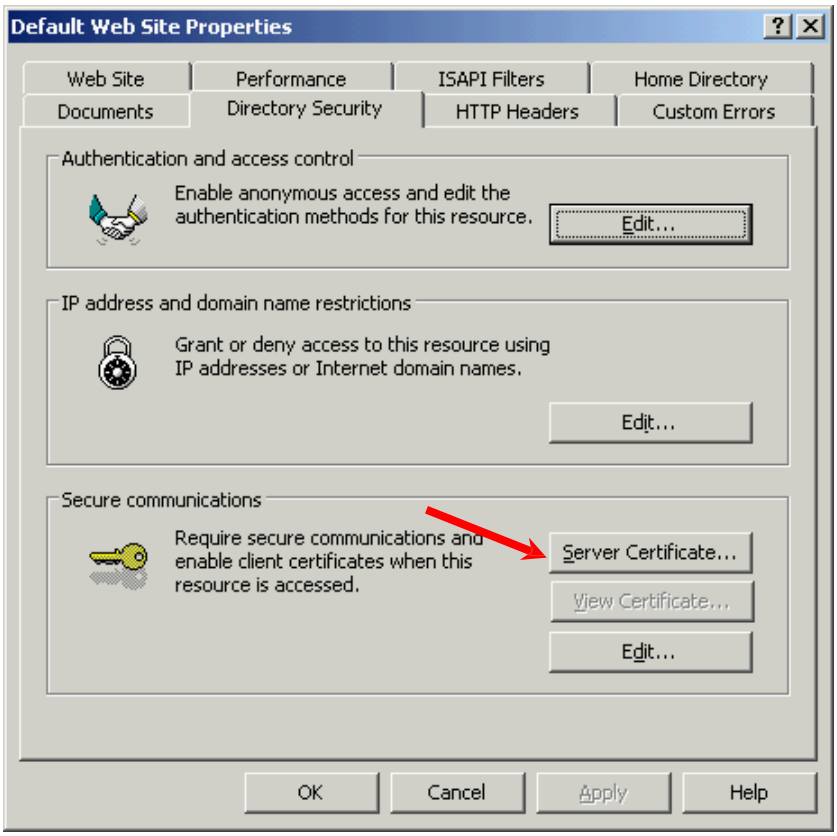
If you are renewing your current e-Cert (Server) on your server, please follow the instructions as described in the following sections:

B. Generating Certificate Signing Request (CSR)

1. Start Internet Information Services (IIS) Manager by clicking “Start” > “All Programs” / “Program” > “Administrative Tools” > “Internet Information Services (IIS) Manager”.
2. In the “Internet Information Services (IIS) Manager” pane, expand “Web Sites” and select your web site, right-click and then click “Properties”.



3. In the “Directory Security” tab, click “Server Certificate”.

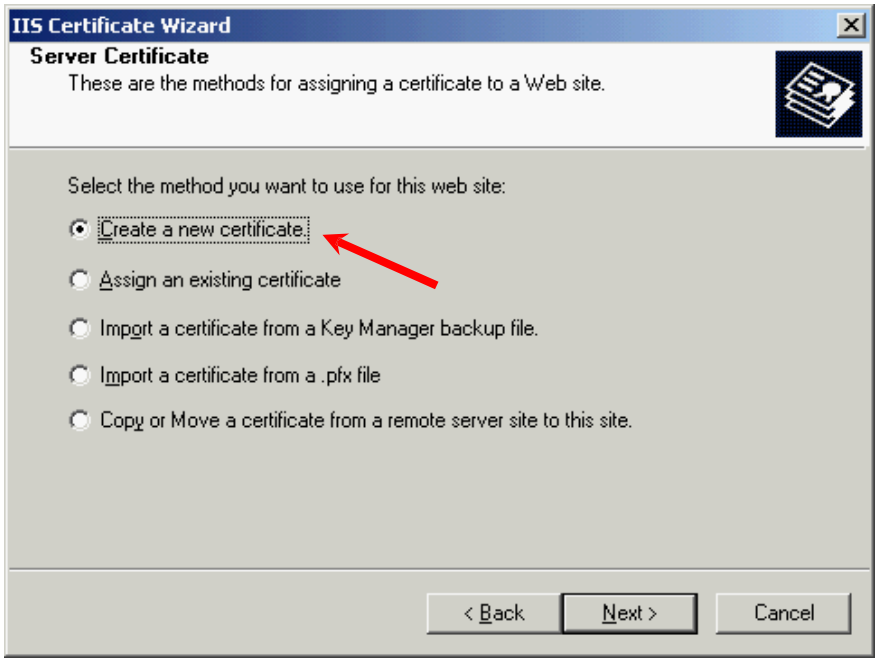


Creating a New Server Certificate

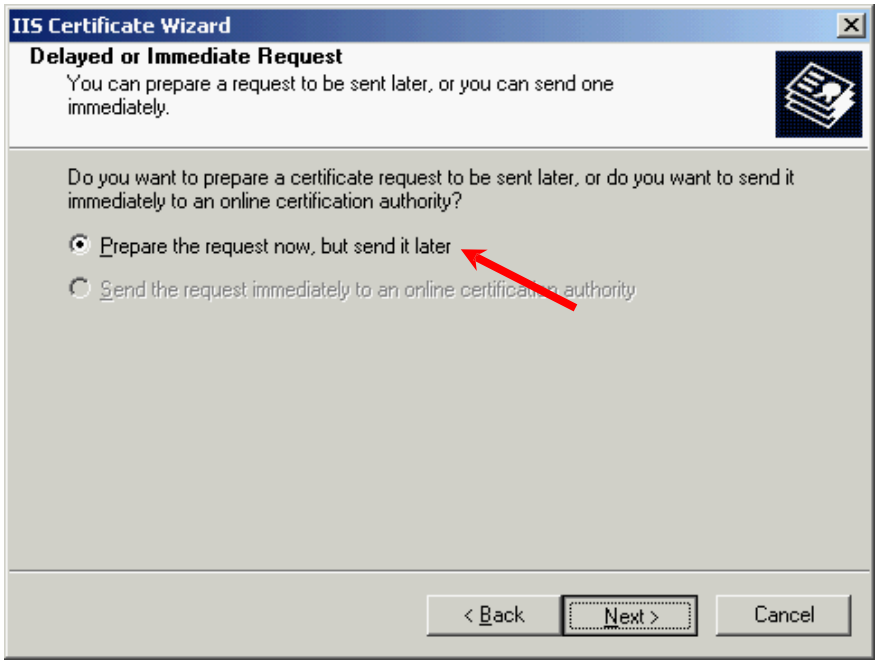
Note: Please skip to Step14 if you are renewing your current server certificate.

4. In the "Web Server Certificate Wizard", click "Next" to continue.

5. Select "Create a new certificate", and then click "Next".

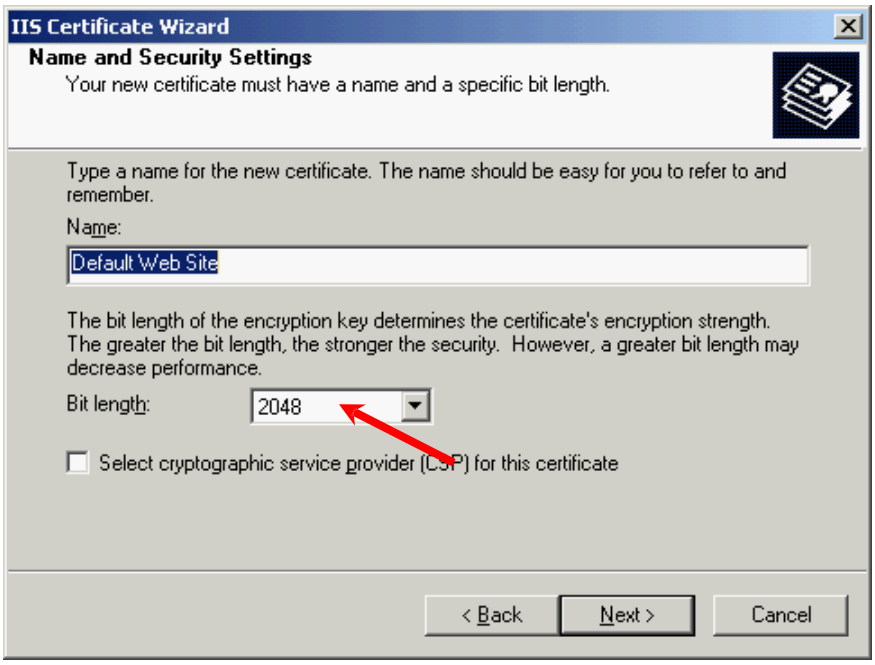


6. Select “Prepare the request now, but send it later”, and then click “Next”.

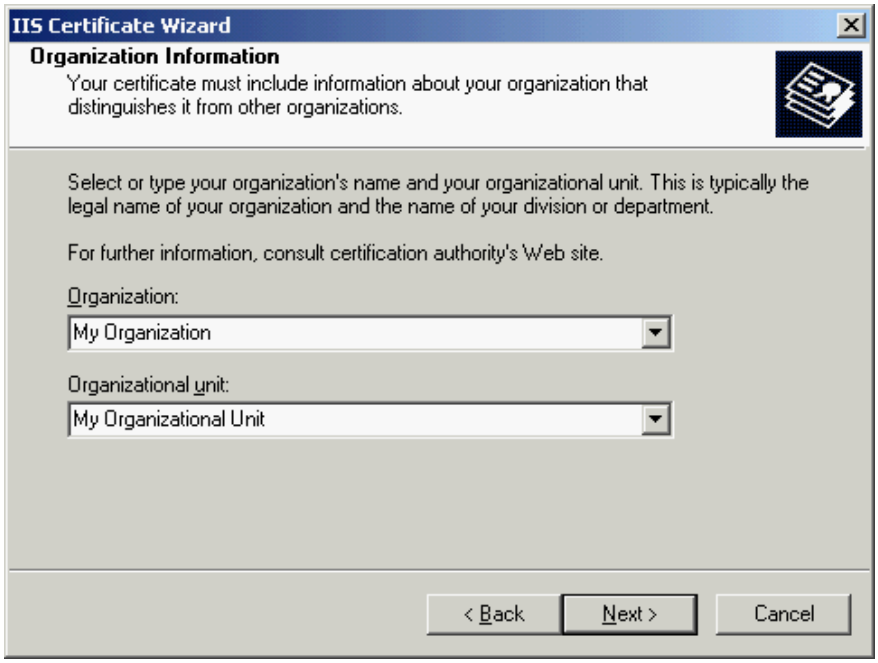


7. Type a name (or accept the default) for the new certificate and choose 2048 for the “Bit length”, and then click “Next”.

Note: Bit length smaller than 2048 may not be strong enough, while greater than 2048 may be incompatible with certain web browsers. It is recommended the bit length of the encryption key to be 2048 in order to support better security strength.



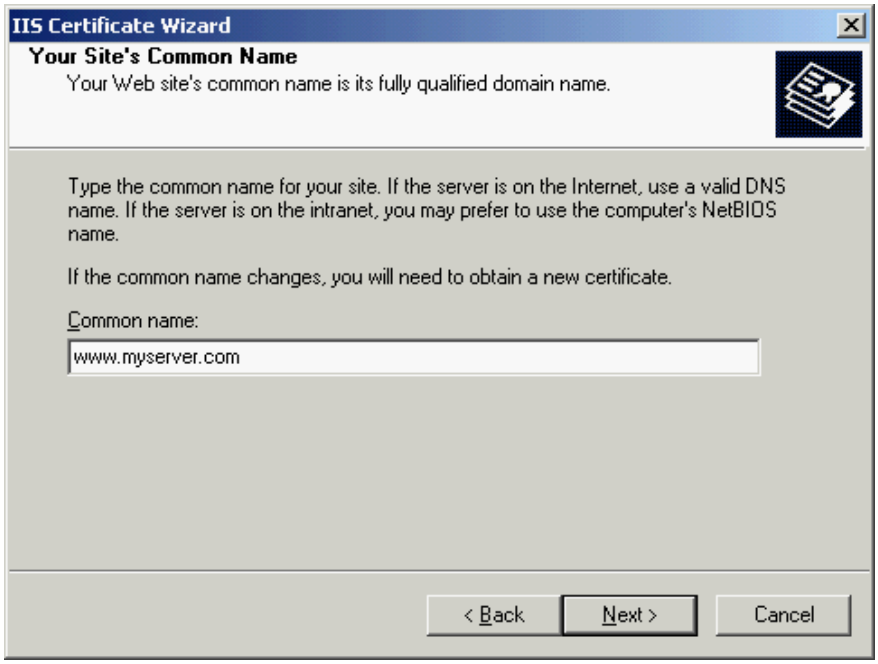
8. Type your organization's name and your organizational unit, and then click "Next".



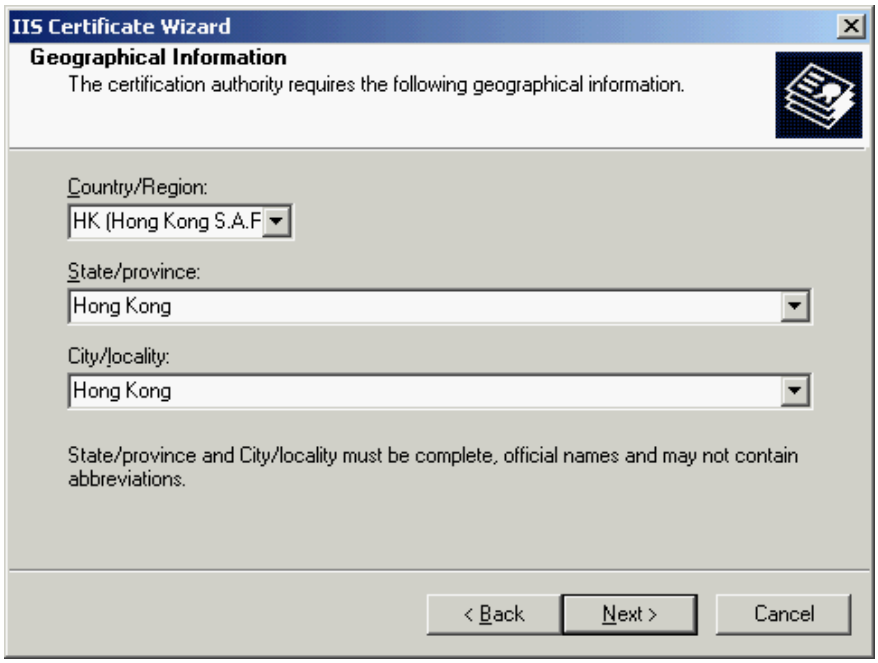
9. Type the common name (i.e. server name) for your site, and then click "Next".

Note: ***For application of e-Cert (Server) with "Multi-domain" feature****, please input the "Common Name" field with "Server name used as Subject Name in the Certificate" being filled in the application form. It is not necessary to specify any "Additional Server Name(s)" in the Subject Alternative Name of the CSR to be generated. It will be assigned by the Hongkong Post CA system automatically based on the information applied in the application form when the certificate is issued.*

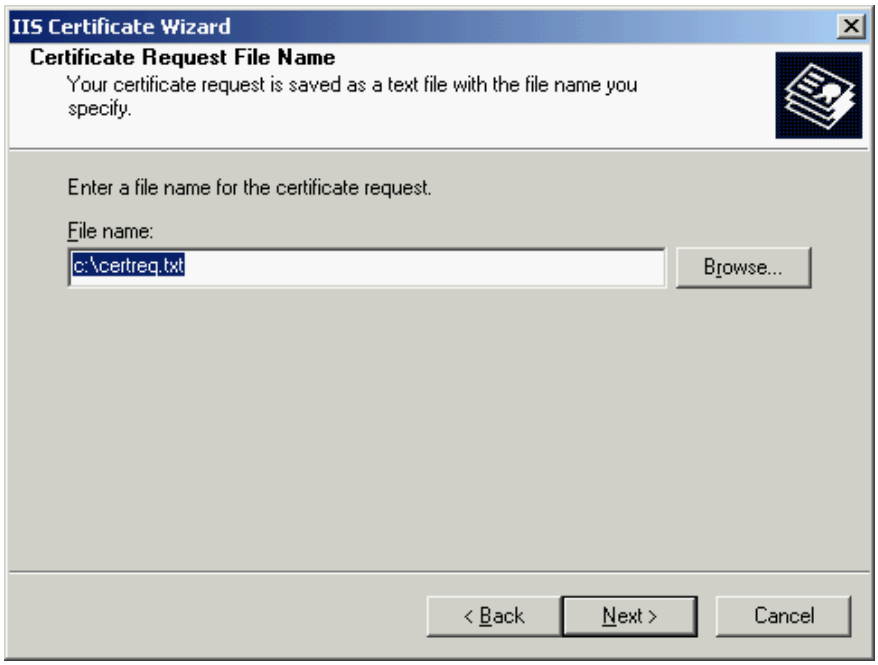
For application of e-Cert (Server) with "Wildcard" feature, *please input the "Common Name" field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk '*', in the left-most component of the server name), e.g. *.myserver.com, being filled in the application form.*



10. Select “HK (Hong Kong S.A.R.)” for the “Country/Region”. Type “Hong Kong” for both “State/province” and “City/locality”, and then click “Next”.

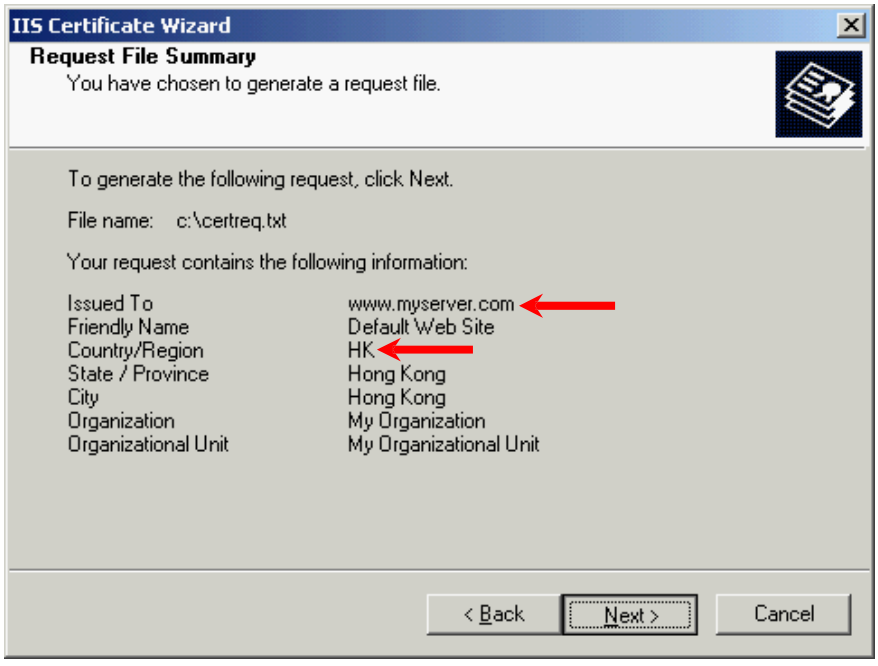


11. Enter a file name for the certificate request, and then click “Next”.

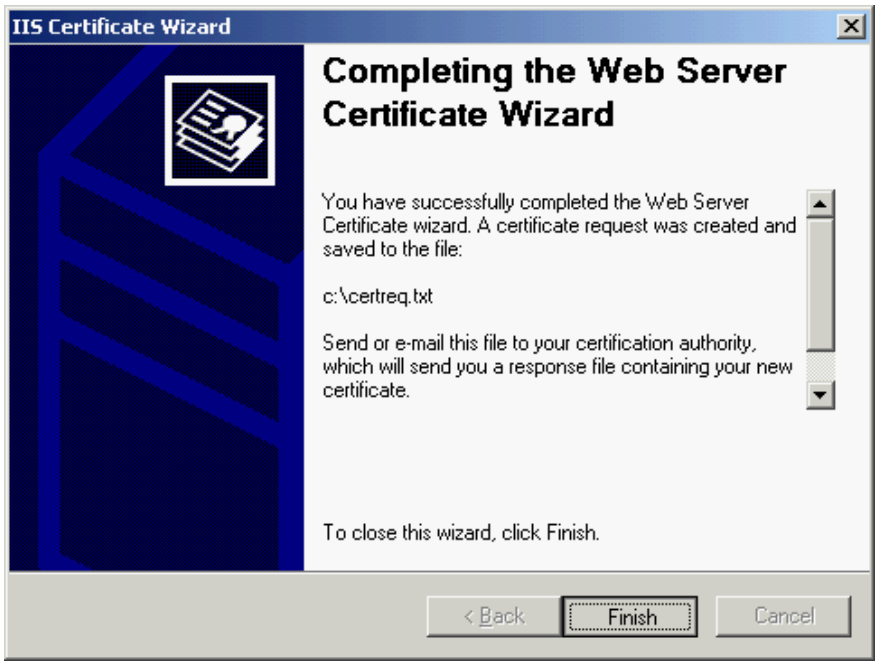


12. Click “Next”.

Note: Please make sure that the correct domain name (i.e. server name) is shown in the “Issued To” field and “HK” in the “Country/Region” field.

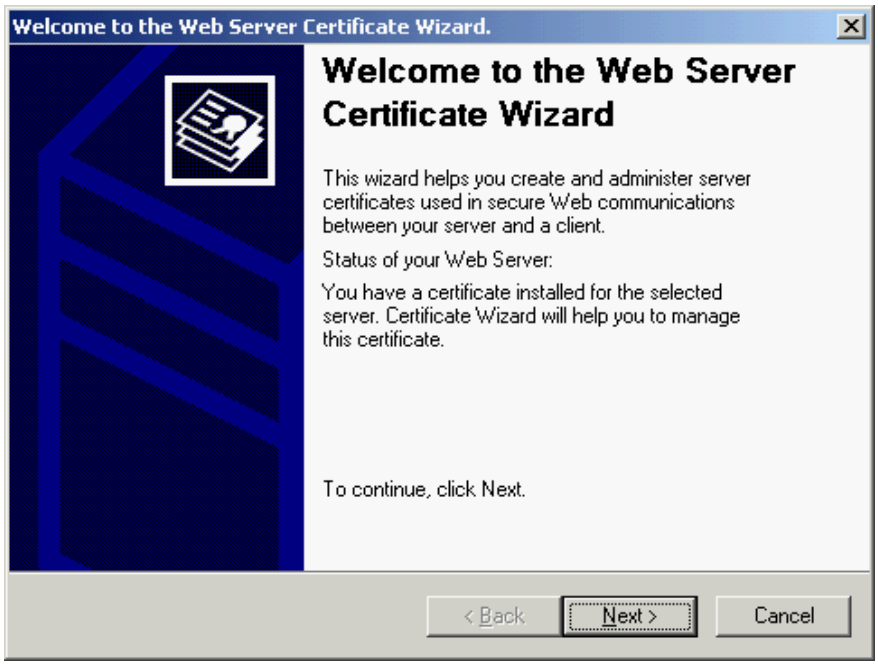


13. Click “Finish” to close the wizard.

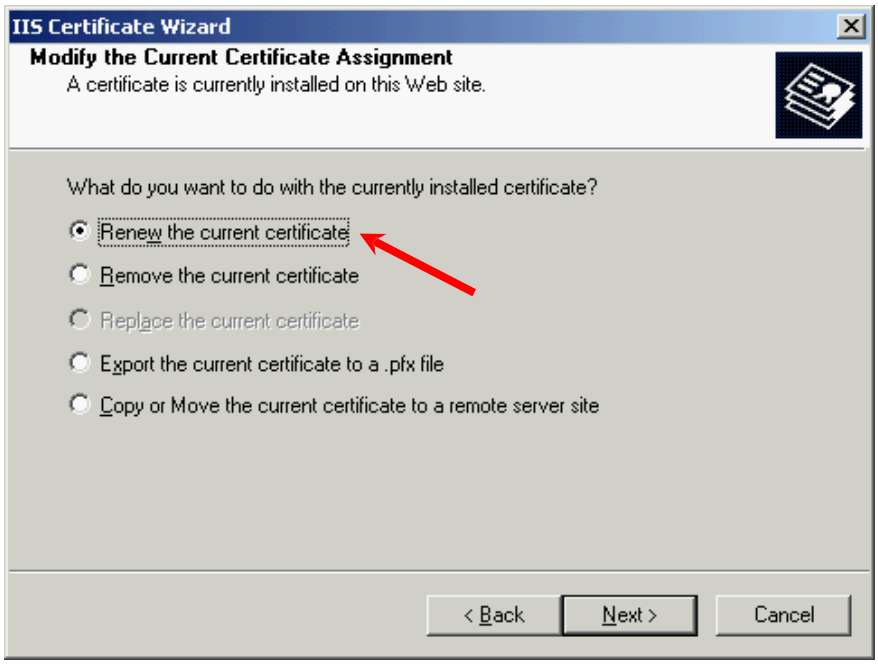


Renewing your Current Server Certificate

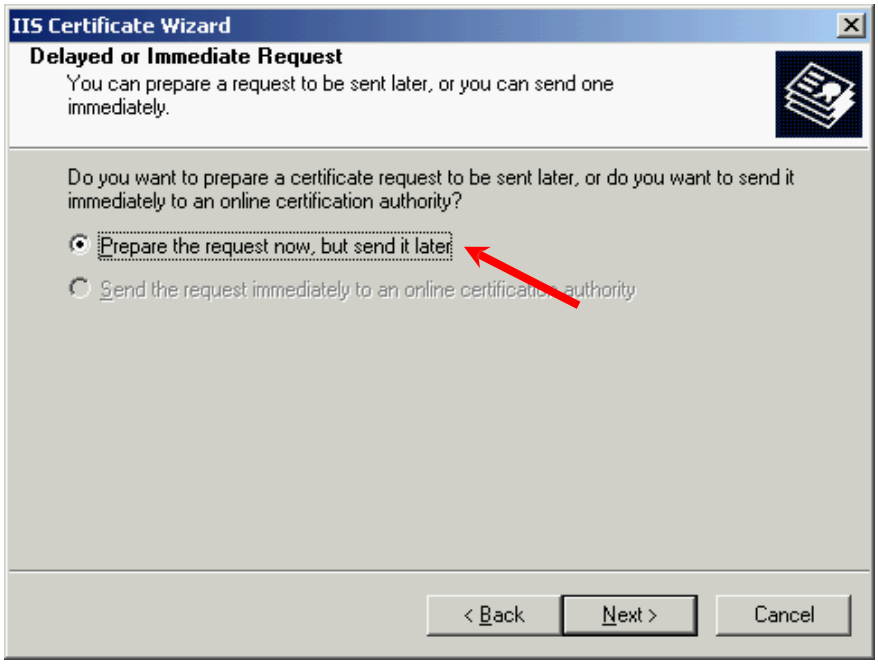
14. In the "Web Server Certificate Wizard", click "Next" to continue.



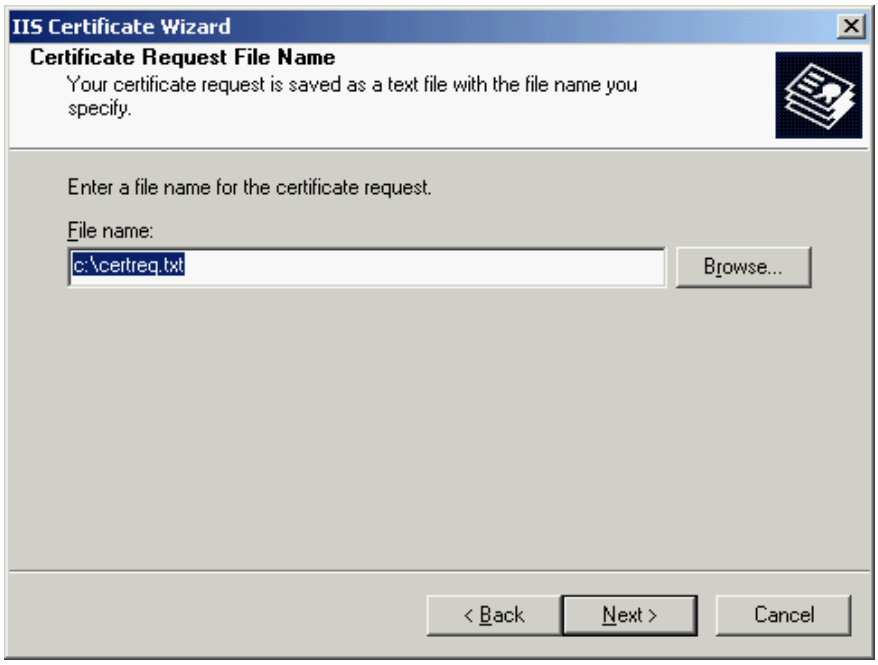
15. Select "Renew the current certificate", and then click "Next".



16. Select “Prepare the request now, but send it later”, and then click “Next”.

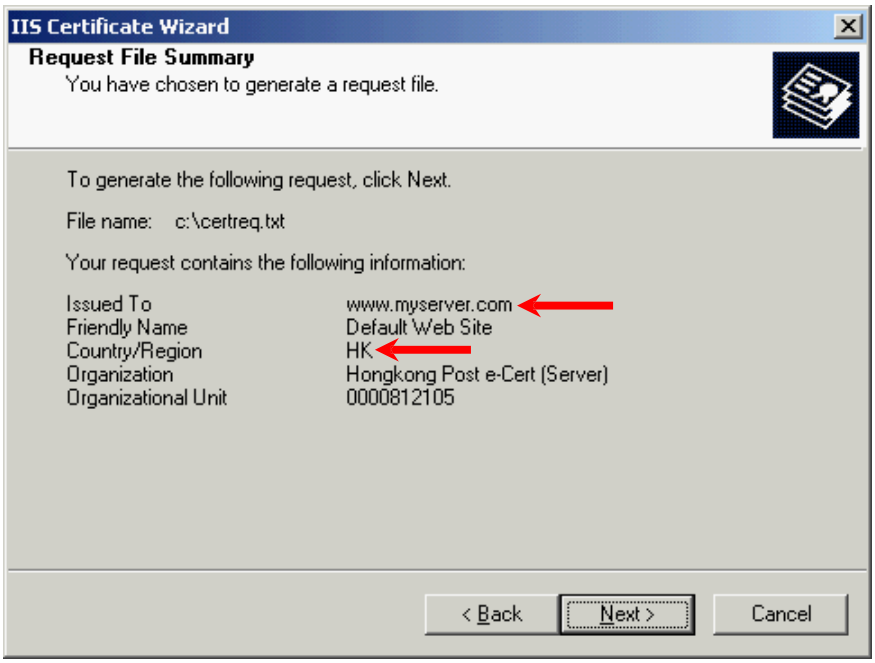


17. Enter a file name for the certificate request, and then click “Next”.

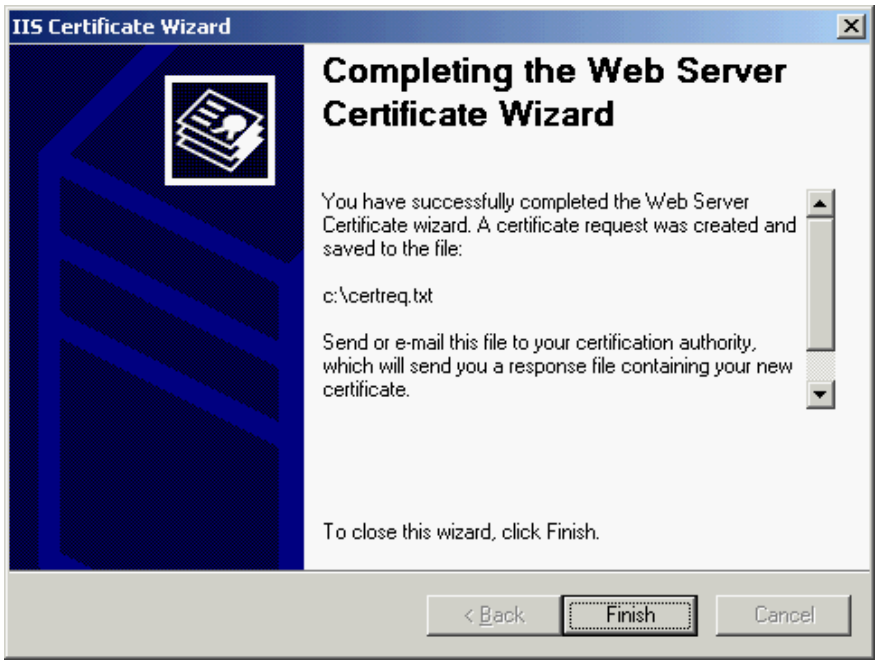


18. Click "Next".

Note: Please make sure that the correct domain name (i.e. server name) is shown in the "Issued To" field and "HK" in the "Country/Region" field.

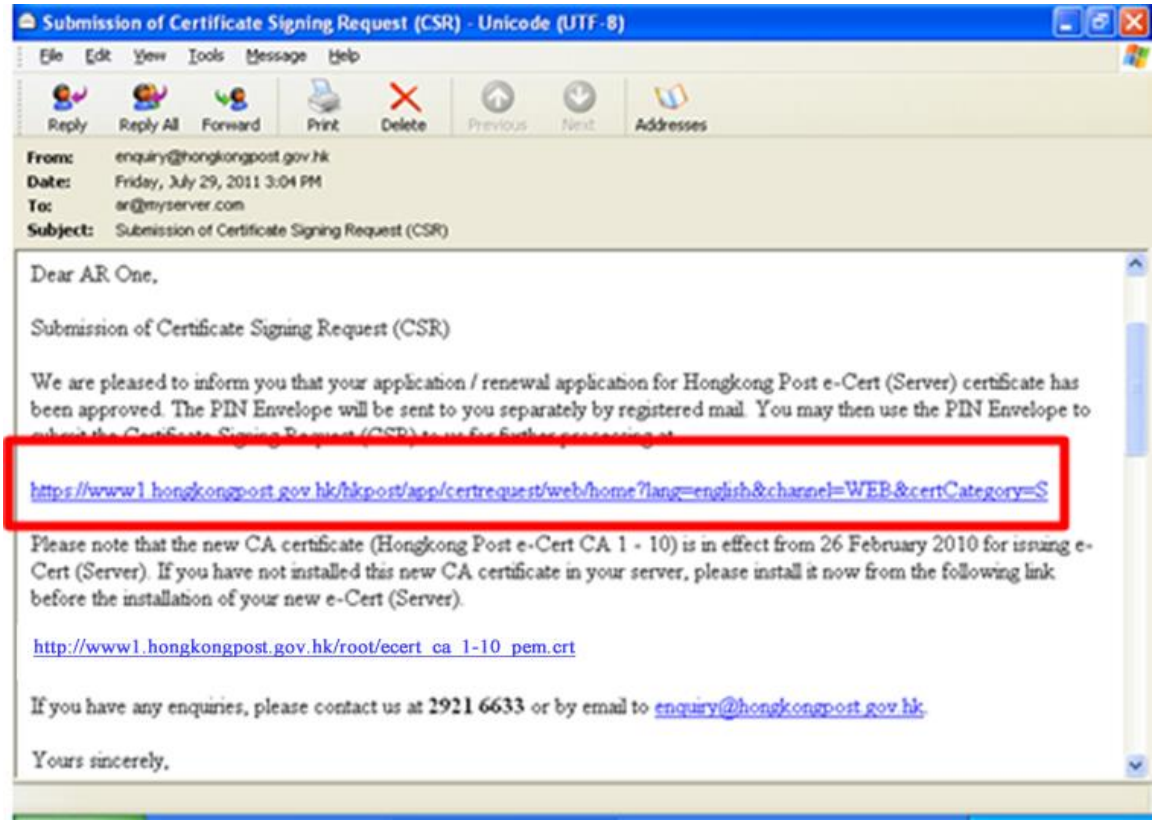


19. Click "Finish" to close the wizard.

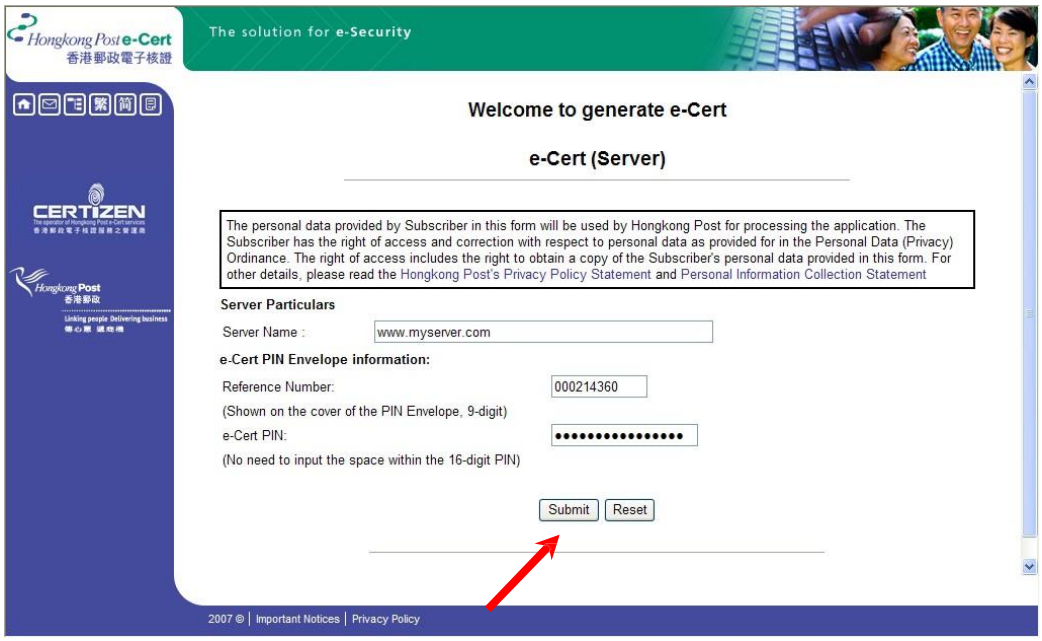


C. Submitting Certificate Signing Request (CSR)

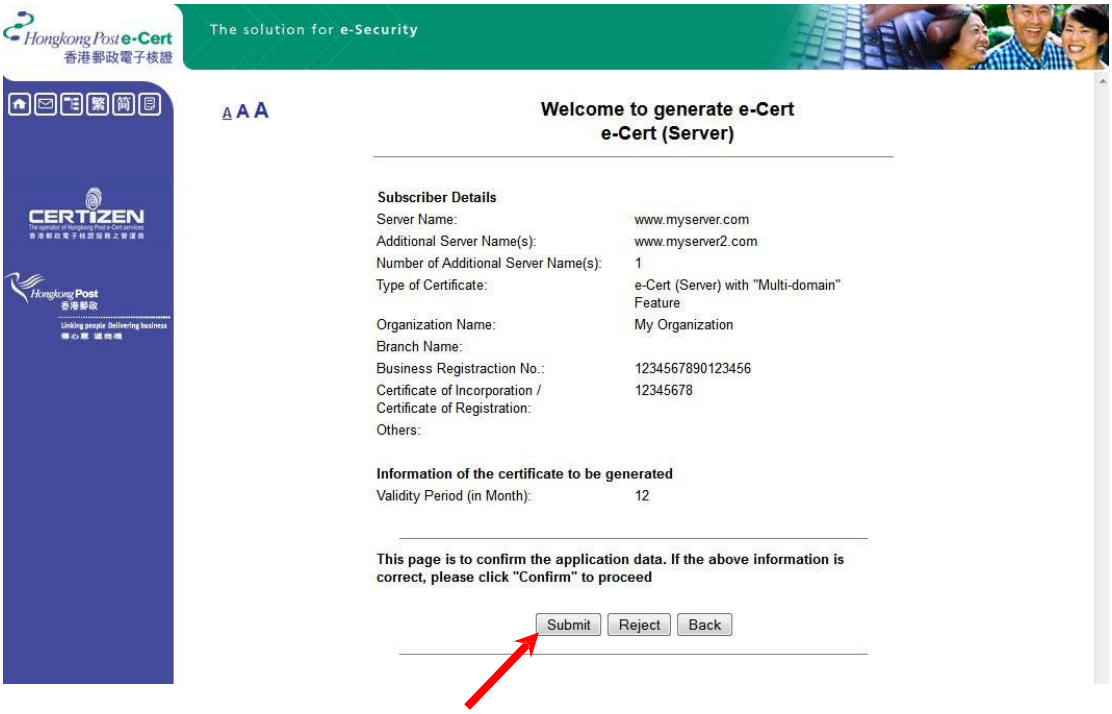
1. Click on the hyperlink in the e-mail with subject "Submission of Certificate Signing Request (CSR)" sent from Hongkong Post Certification Authority to access the Hongkong Post CA web site.



2. Type the "Server Name", the "Reference Number" (9-digit) as shown on the cover of the PIN Envelope and the "e-Cert PIN" (16-digit) as shown inside the PIN Envelope, and then click "Submit".

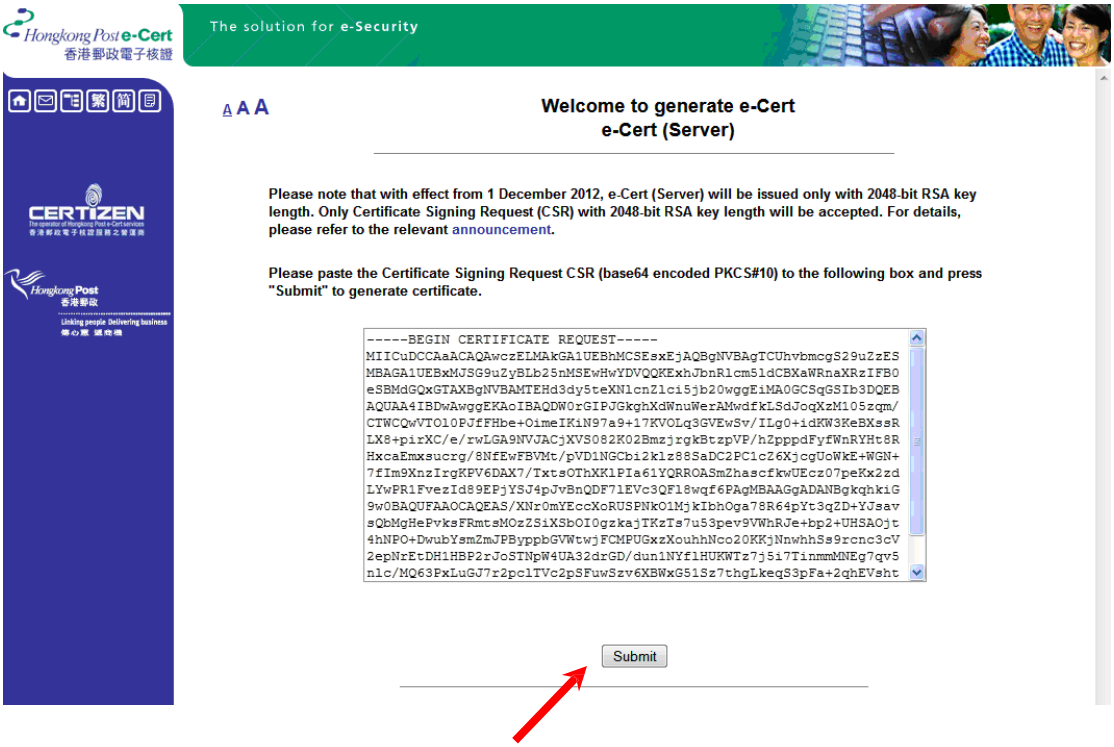


3. Click “Submit” to confirm the application information. (If the information is incorrect, please contact Hongkong Post Certification Authority.)

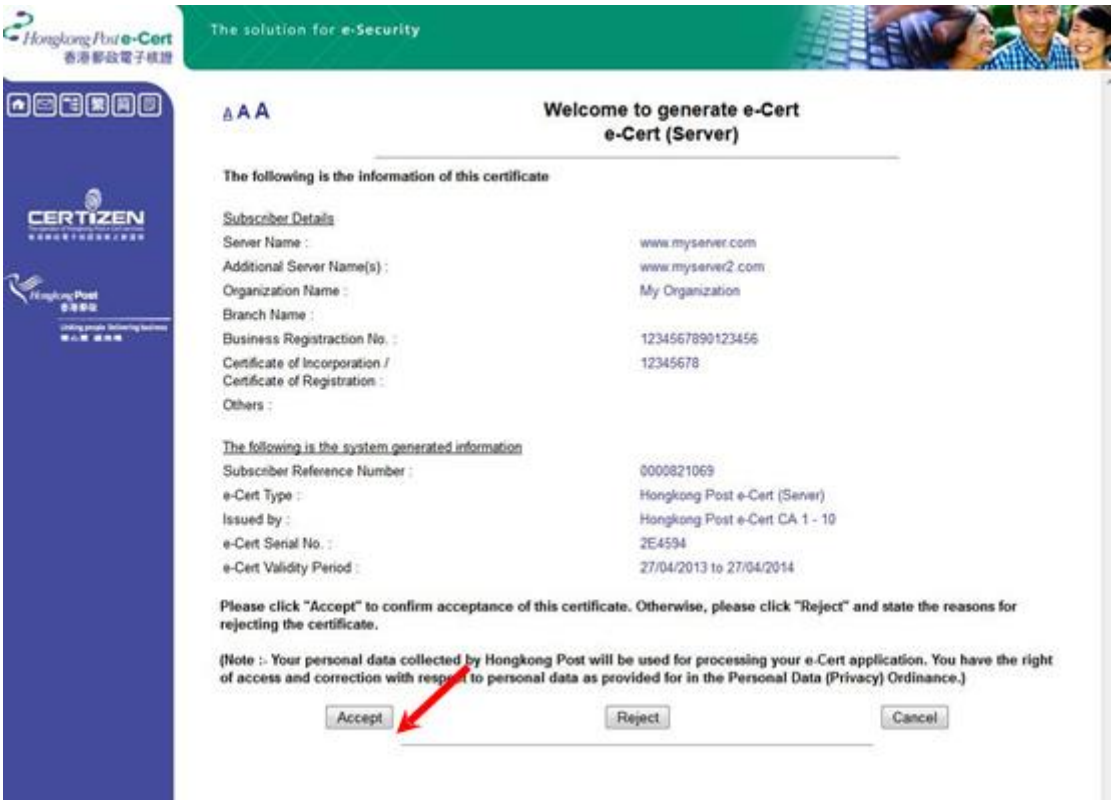


4. Open the previously generated Certificate Signing Request (CSR) with a text editor (e.g. Notepad) and copy the entire content including the "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----". (You may refer to Part B Step 11 or Step 17 for the location of certificate request file.)

5. Paste the content to the text box, and then click “Submit”.



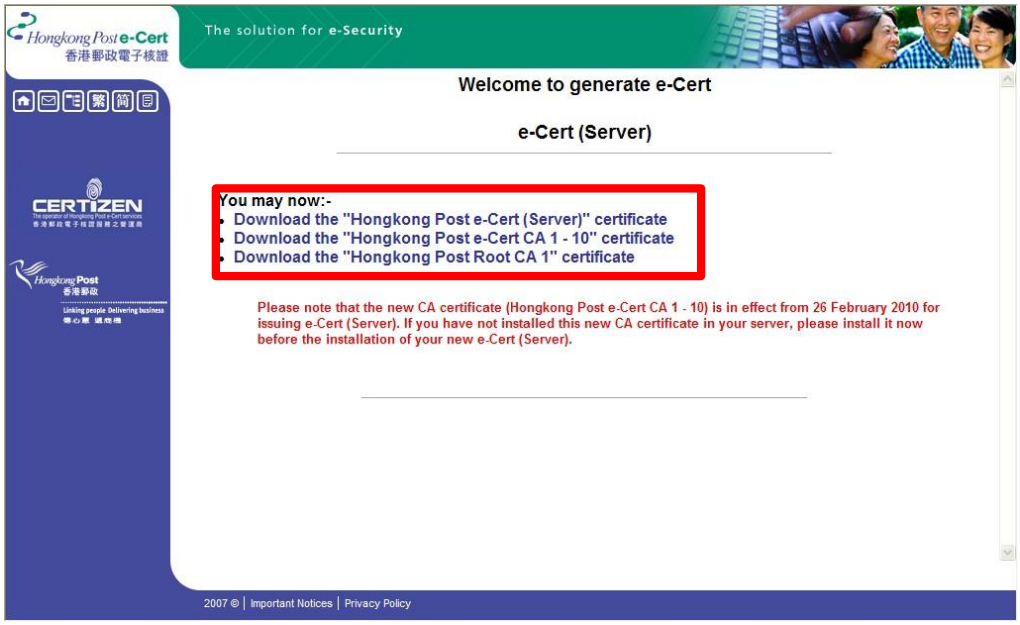
6. Click “Accept” to confirm acceptance of the certificate.



7. Click to download the following certificates:
   - Hongkong Post e-Cert (Server)
   - Hongkong Post e-Cert CA 1 - 10
   - Hongkong Post Root CA 1

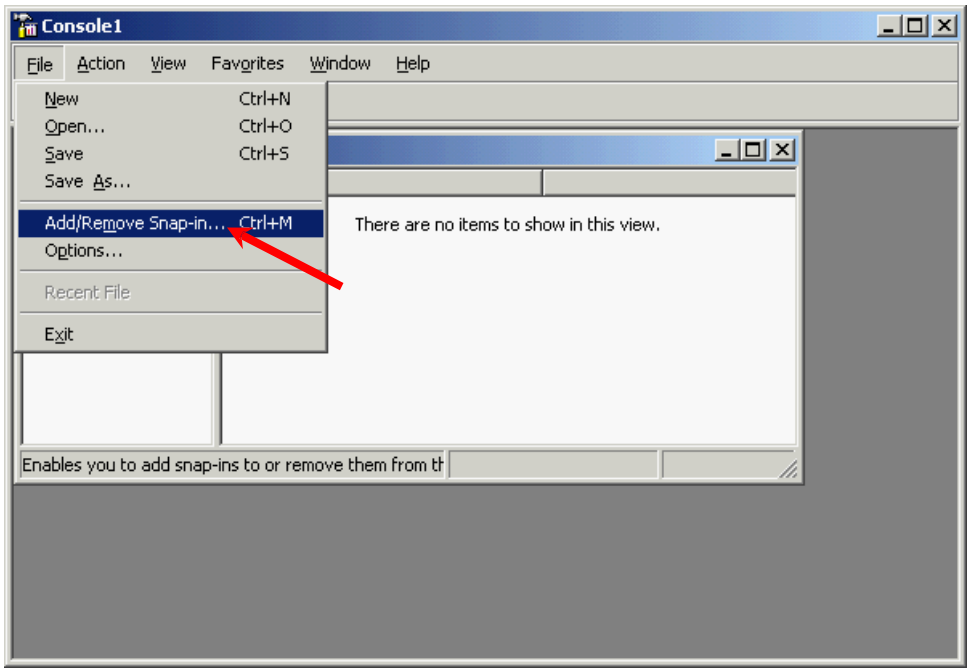
Note: You can also download your e-Cert (Server) from the Search and Download Certificate web page. http://www.hongkongpost.gov.hk/en/sc

Note: If the "Hongkong Post e-Cert CA 1 - 10" certificate and the "Hongkong Post Root CA 1" certificate have been installed on your server before, you only need to download the "Hongkong Post e-Cert (Server)" certificate.

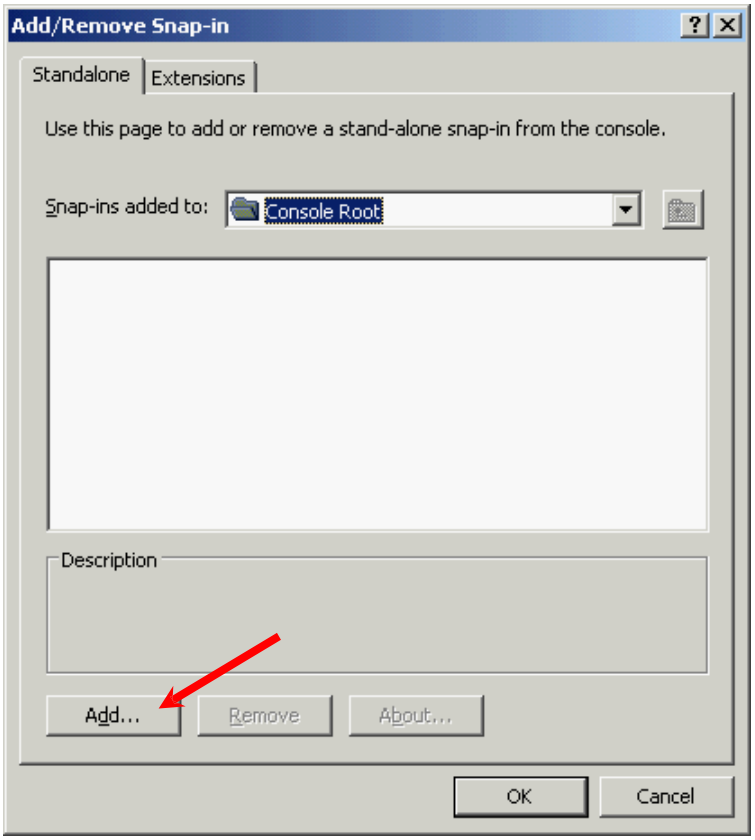


D. Installing Hongkong Post Root CA Certificate

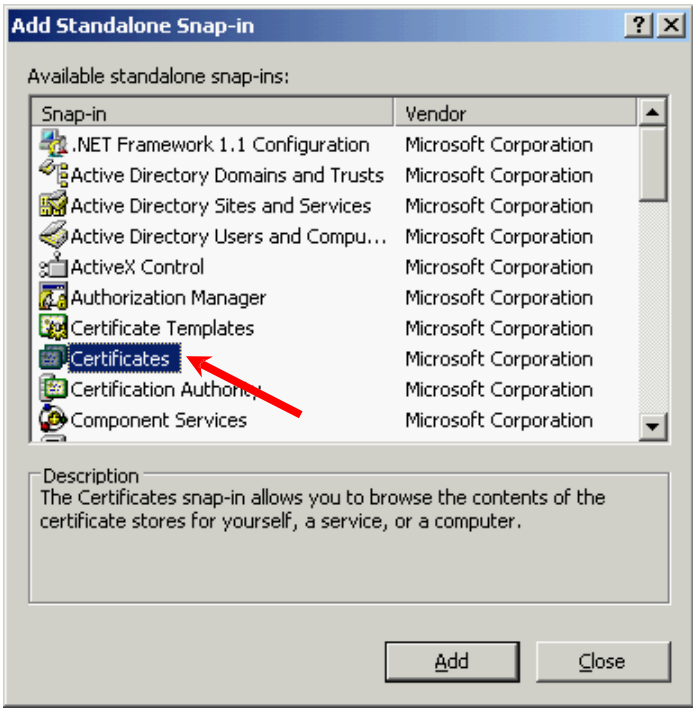
1. Start Microsoft Management Console (MMC) by clicking "Start" > "Run", type "mmc" and click OK, and then select "Add/Remove Snap-in" from the "File" / "Console" menu.



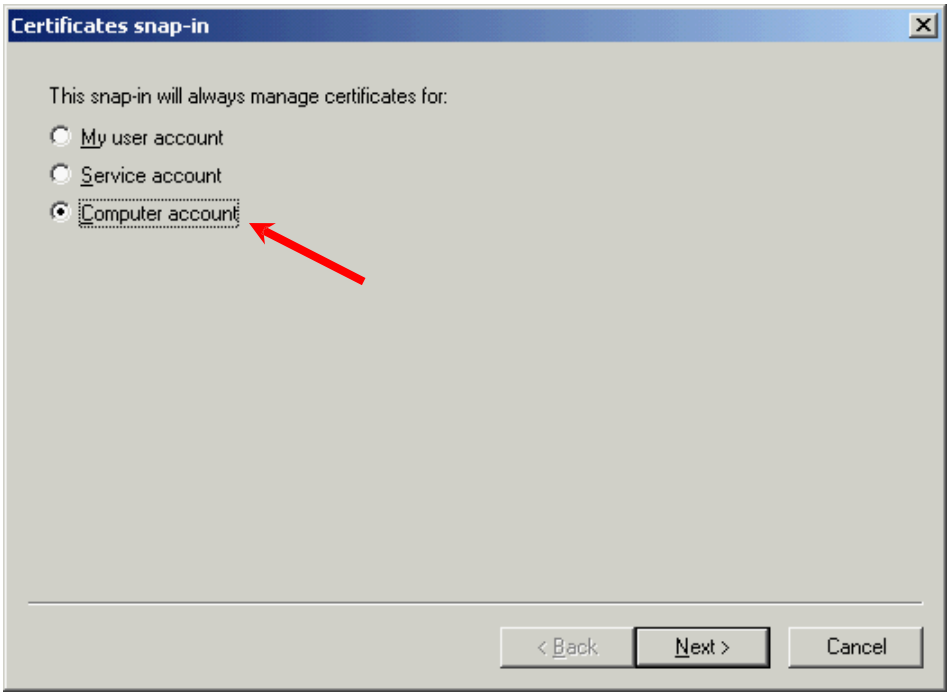
2. Click "Add".



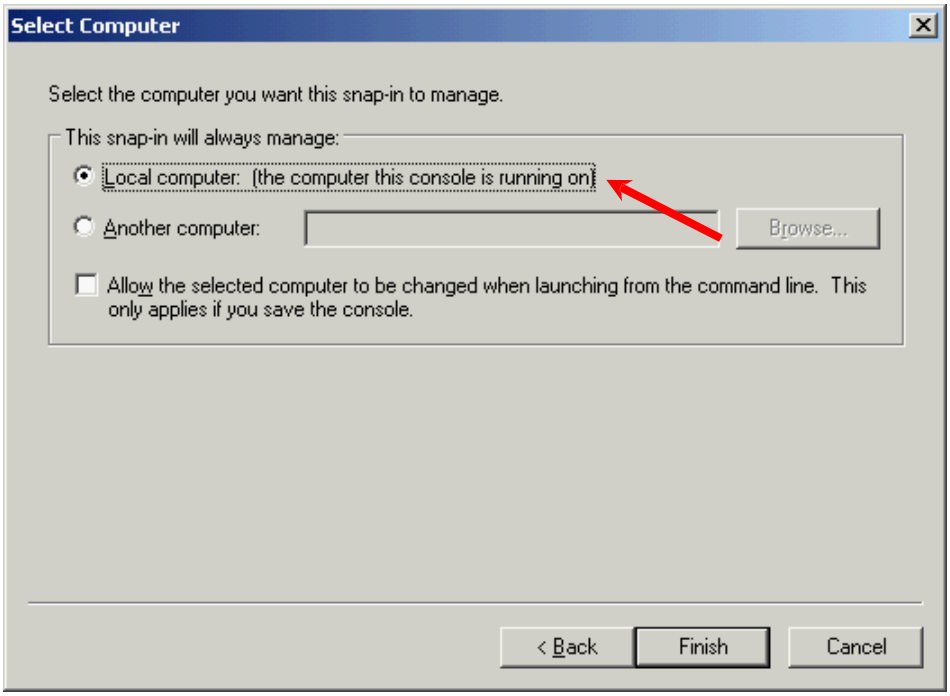
3. Select “Certificates”, and then click “Add”.



4. Select “Computer account”, and then click “Next”.



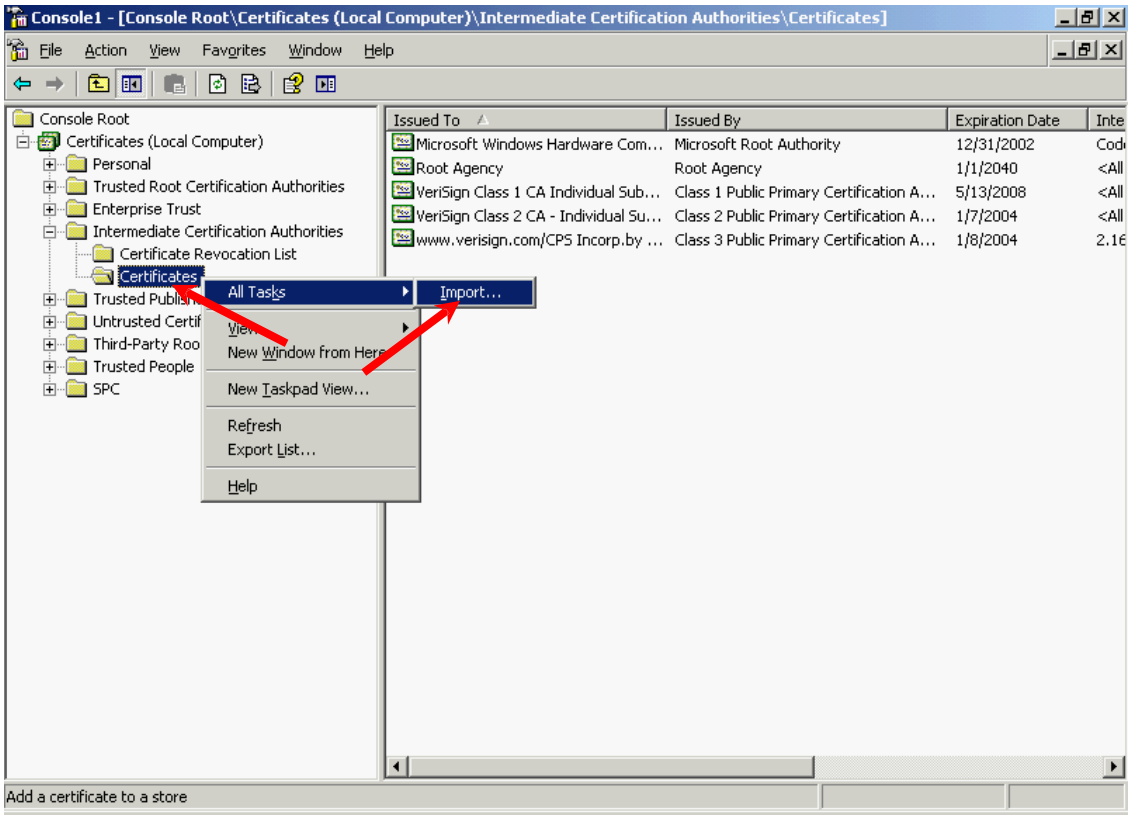
5. Select “Local computer”, and then click “Finish”.



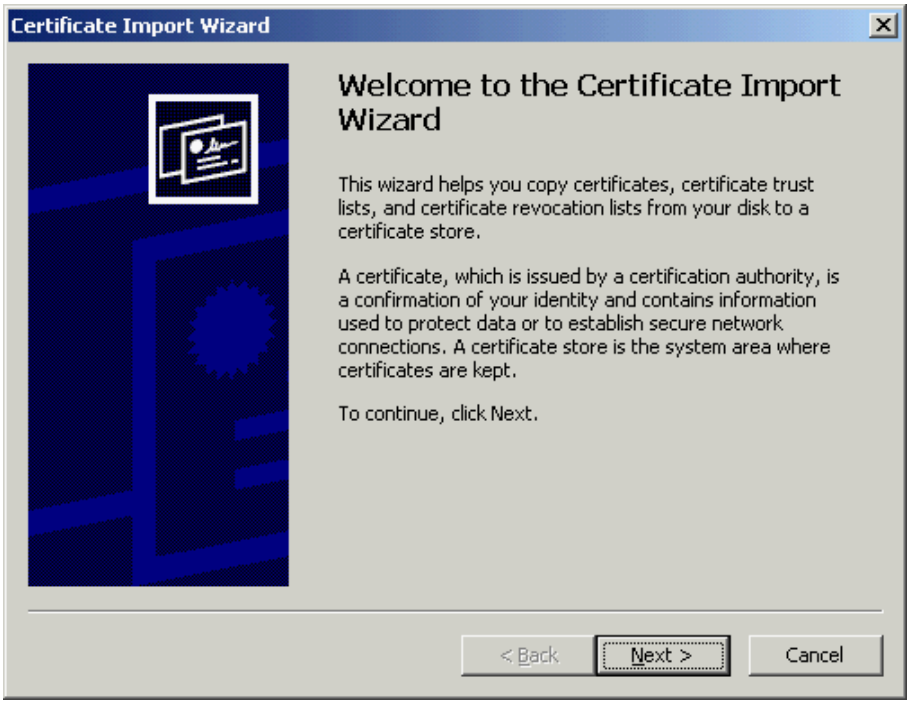
6. Close the “Add Standalone Snap-in” dialog box, and then click “OK” to close the “Add/Remove Snap-in” dialog box.

Installing the "Hongkong Post e-Cert CA 1 - 10" Certificate

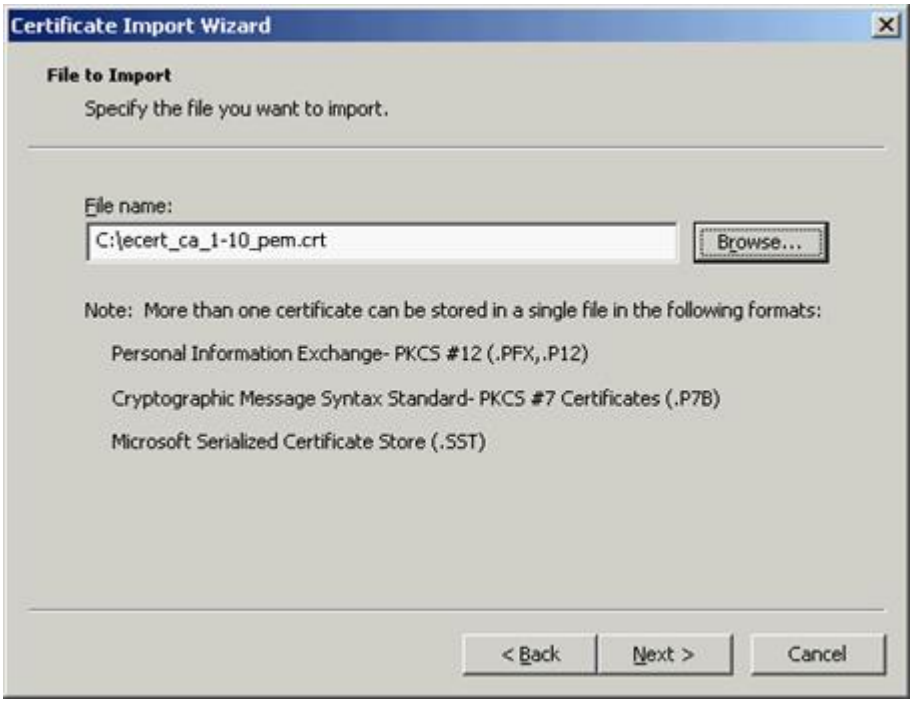
7. Expand "Intermediate Certification Authorities" and right-click "Certificates", and then select "All Tasks" > "Import".



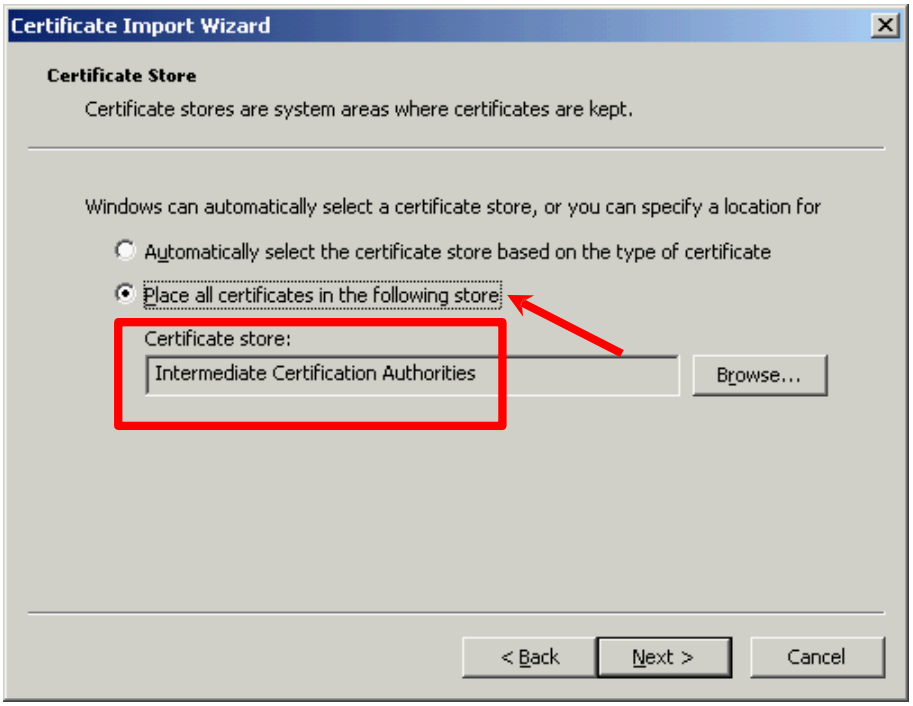
8. In the "Certificate Import Wizard", click "Next" to continue.



9. Click "Browse" to locate the "Hongkong Post e-Cert CA 1 - 10" certificate that you downloaded in Part C Step 7 (ecert_ca_1-10_pem.crt), and then click "Next".



10. Select "Place all certificates in the following store", and then click "Next".



11. Click “Finish” to close the wizard.

12. Click “OK” to complete.

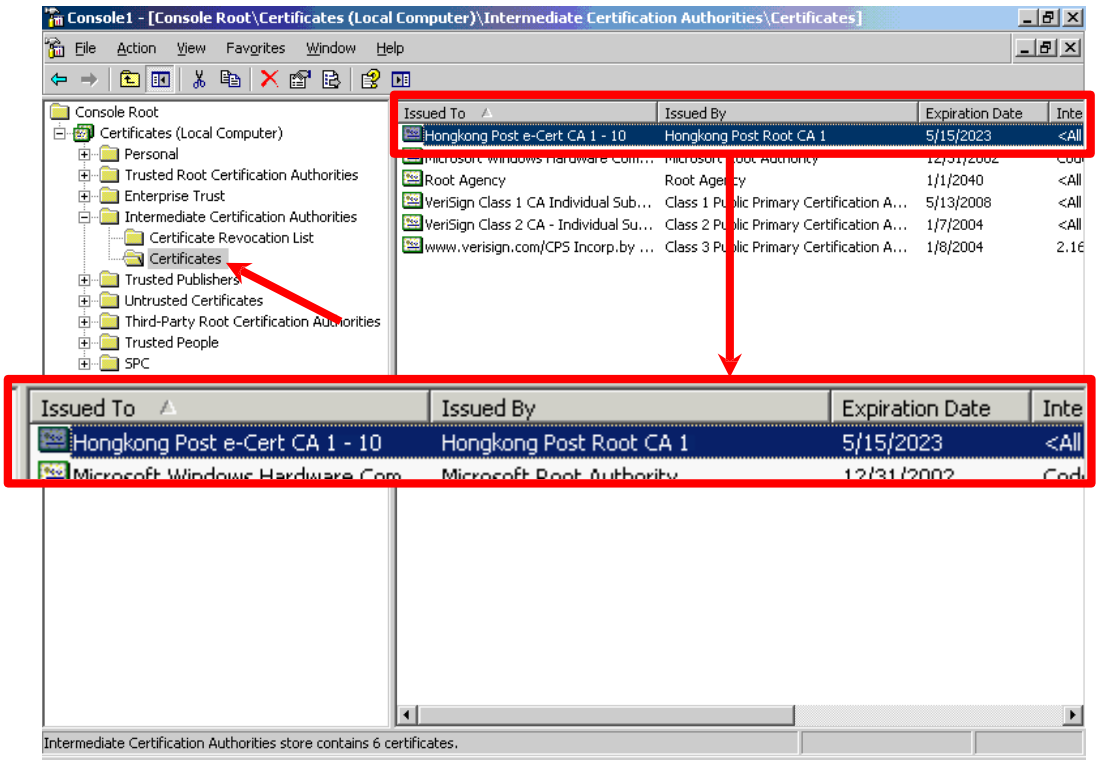
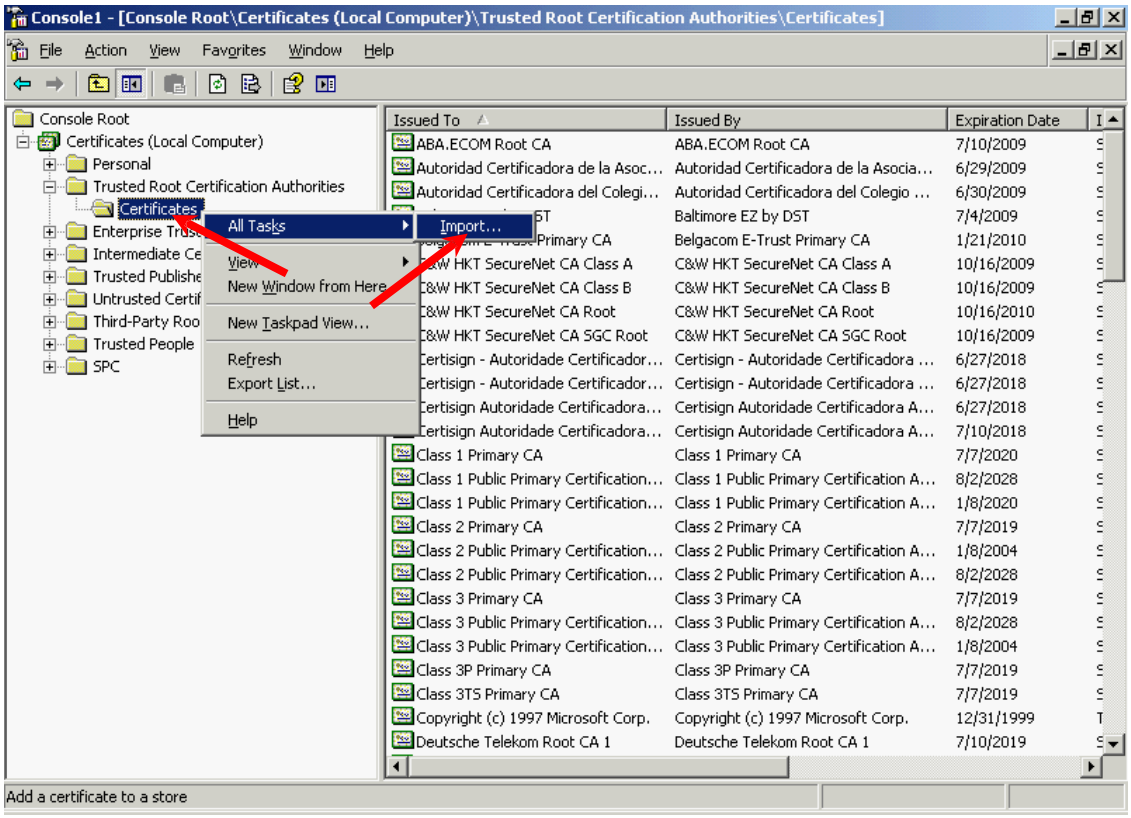


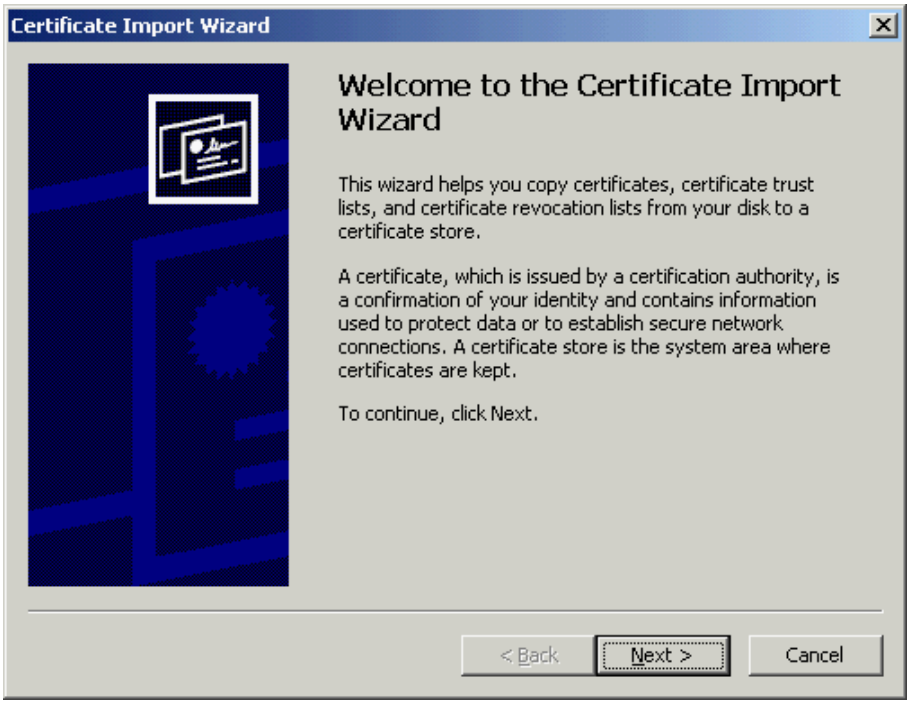
Figure 1: “Hongkong Post e-Cert CA 1 - 10” certificate has been successfully installed

Installing the "Hongkong Post Root CA 1" Certificate

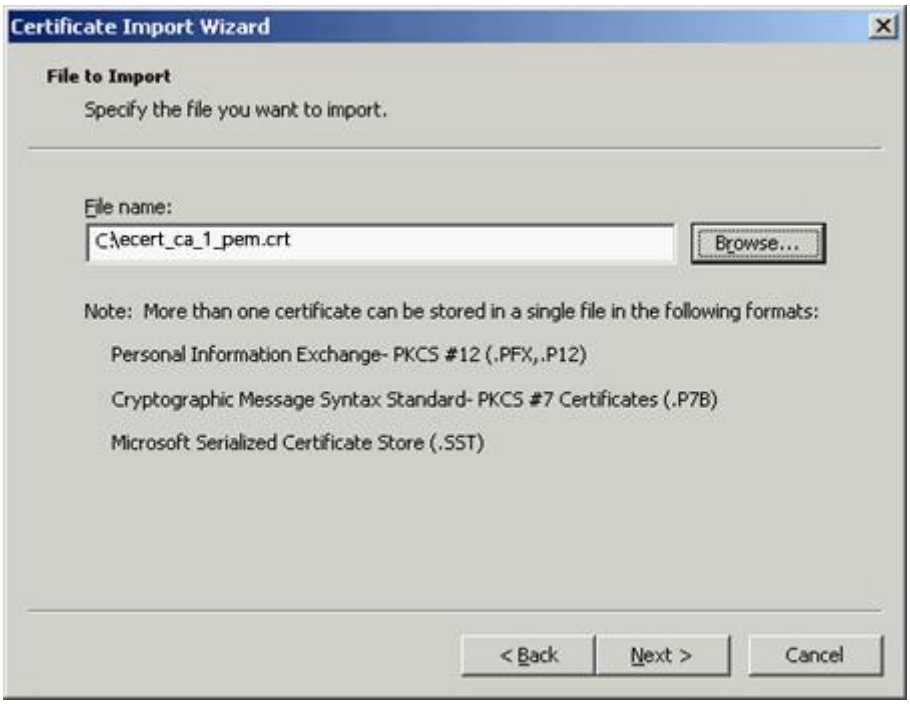
13. Expand "Trusted Root Certification Authorities" and right-click "Certificates", and then select "All Tasks" > "Import".



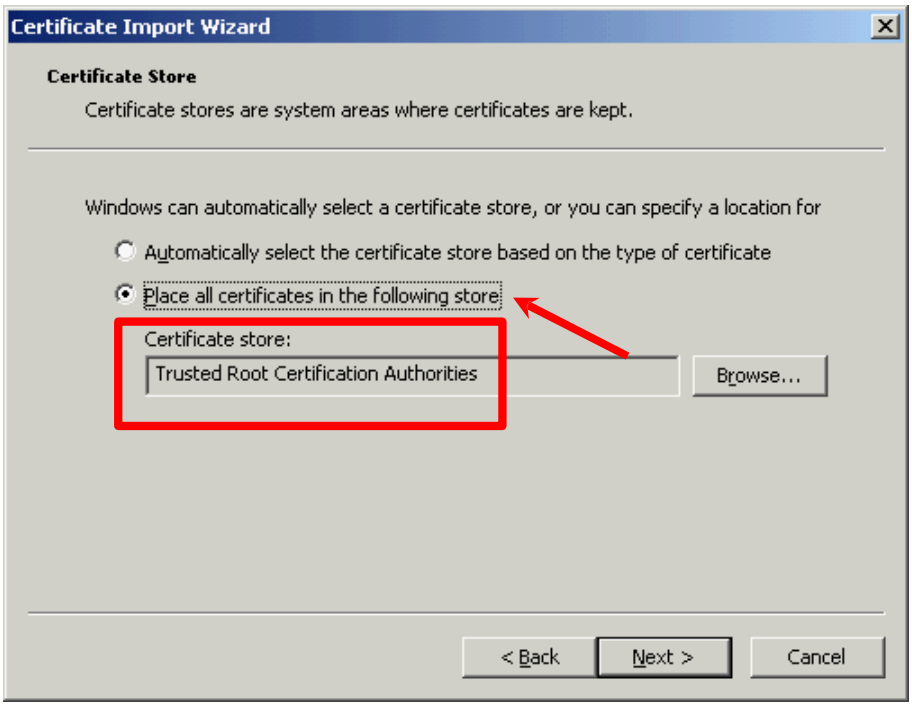
14. In the "Certificate Import Wizard", click "Next" to continue.



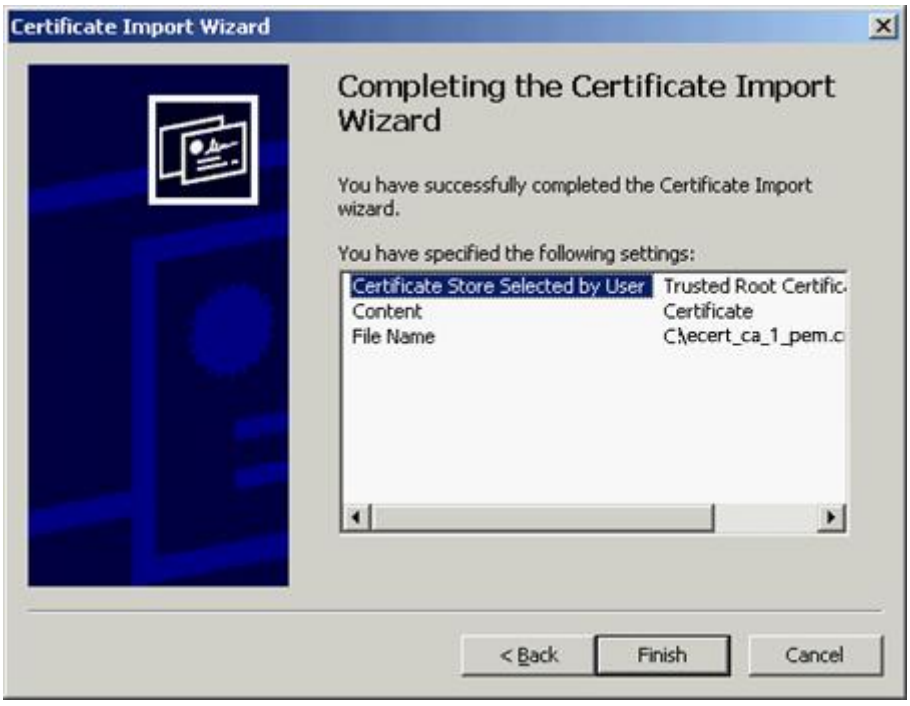
15. Click "Browse" to locate the "Hongkong Post Root CA 1" certificate that you downloaded in Part C Step 7 (ecert_ca_1_pem.crt), and then click "Next".



16. Select "Place all certificates in the following store", and then click "Next".



17. Click “Finish” to close the wizard.



18. Click “OK” to complete.

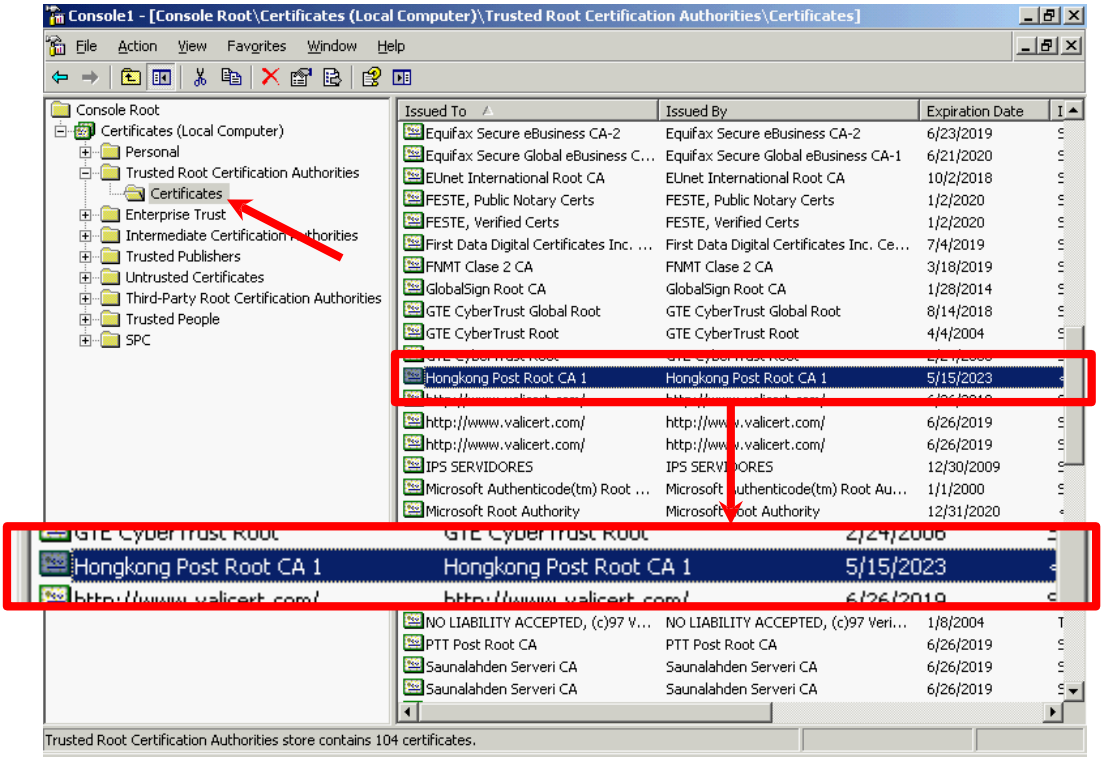
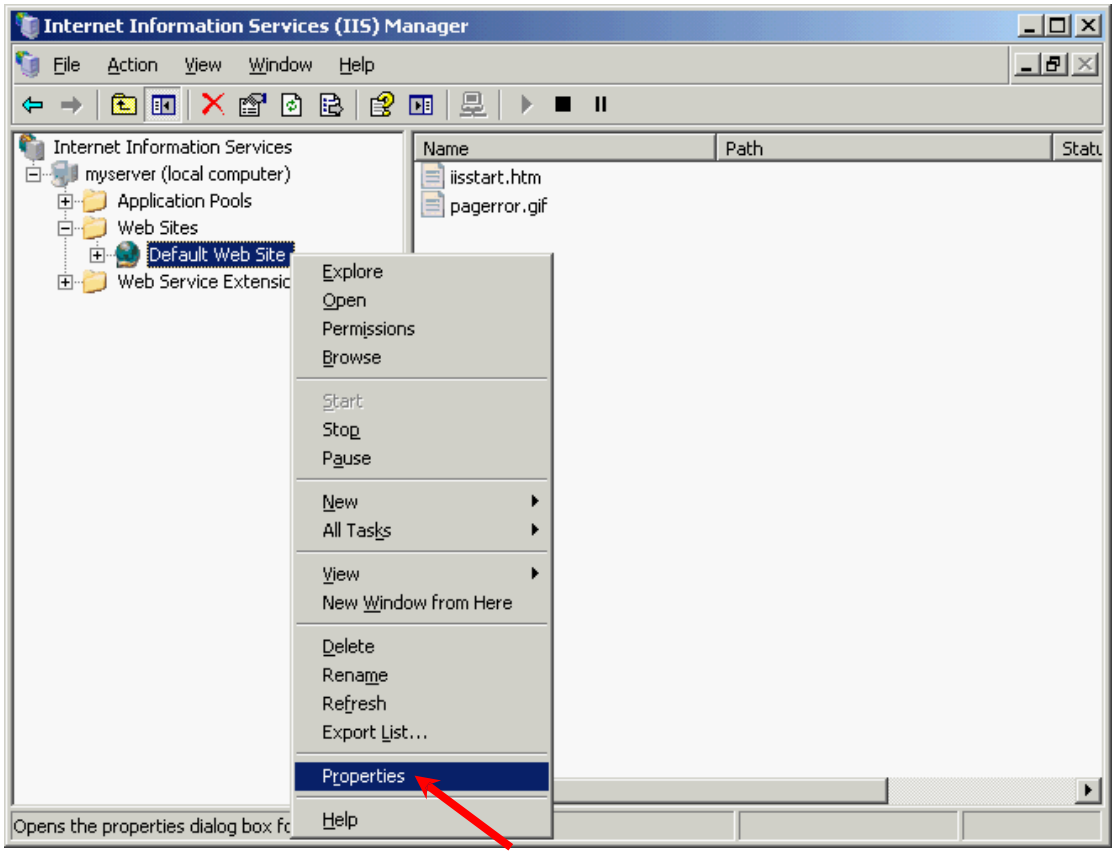


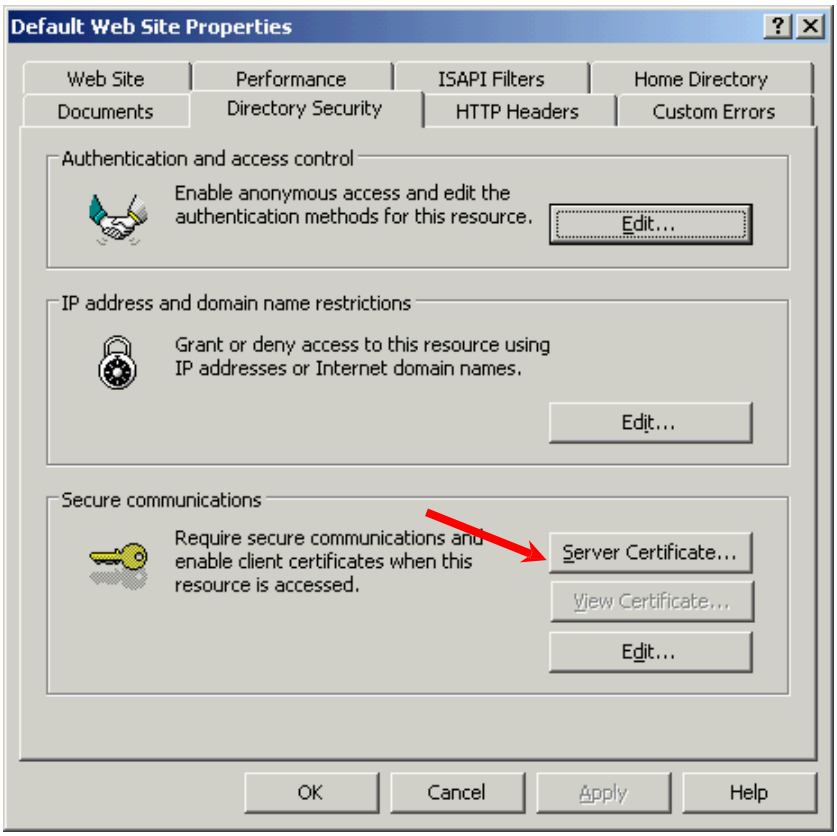
Figure 2: “Hongkong Post Root CA 1” certificate has been successfully installed

E. Installing Server Certificate

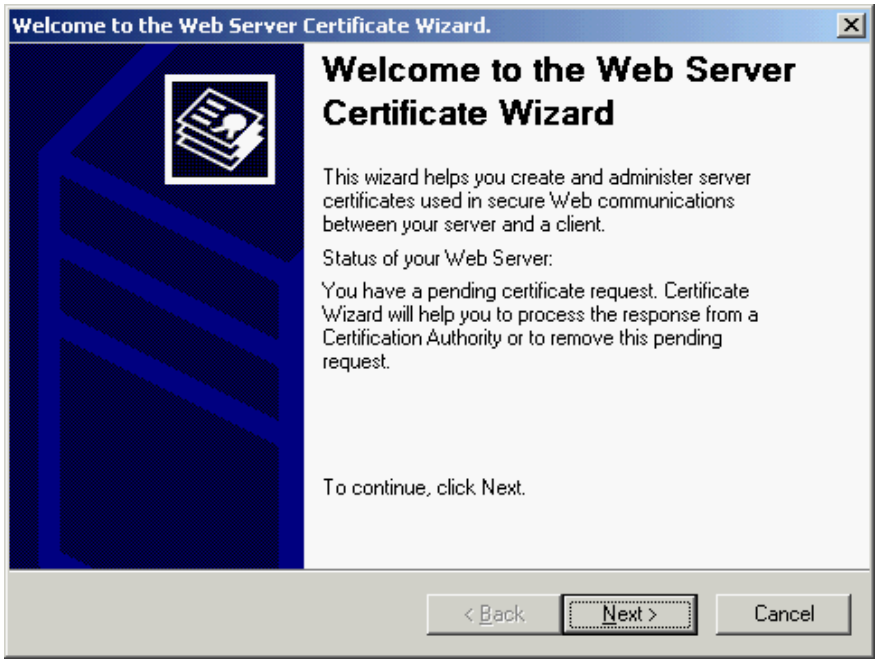
1. Start Internet Information Services (IIS) Manager by clicking “Start” > “All Programs” / “Program” > “Administrative Tools” > “Internet Information Services (IIS) Manager”.
2. In the “Internet Information Services (IIS) Manager” pane, expand “Web Sites” and select your web site, right-click and then click “Properties”.



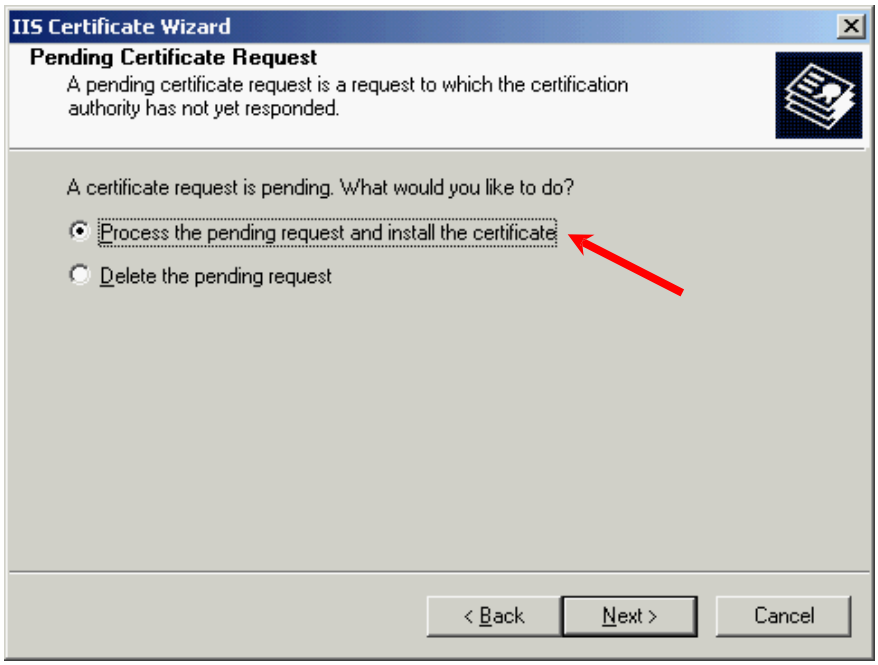
3. In the “Directory Security” tab, Click “Server Certificate”.



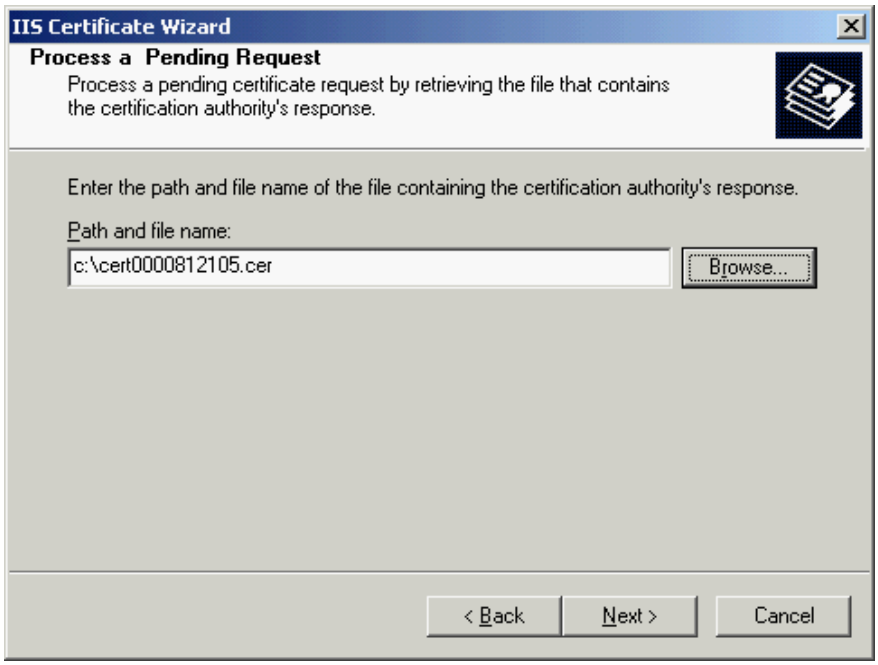
4. In the “Web Server Certificate Wizard”, click “Next” to continue.



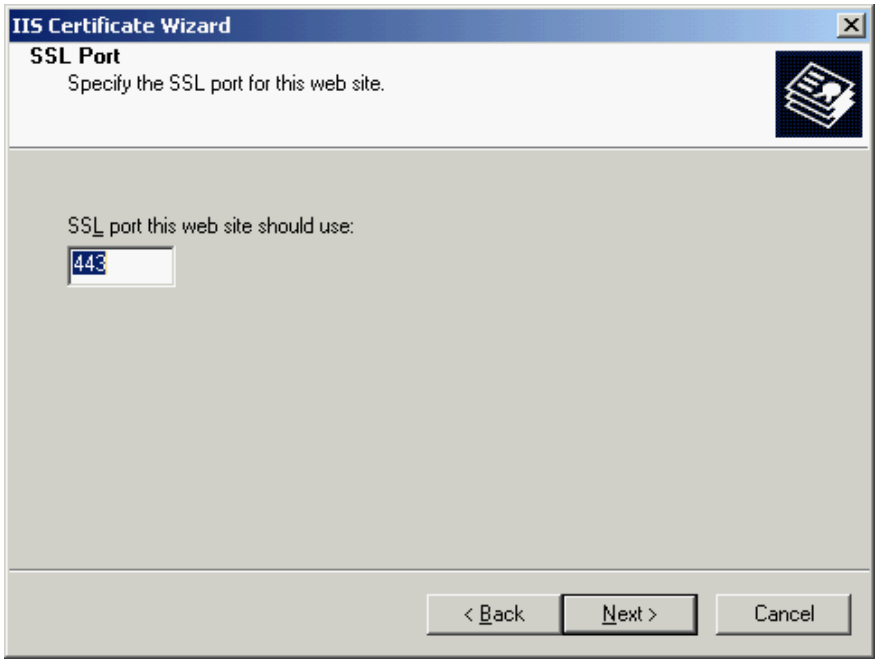
5. Select "Process the pending request and install the certificate", and then click "Next".



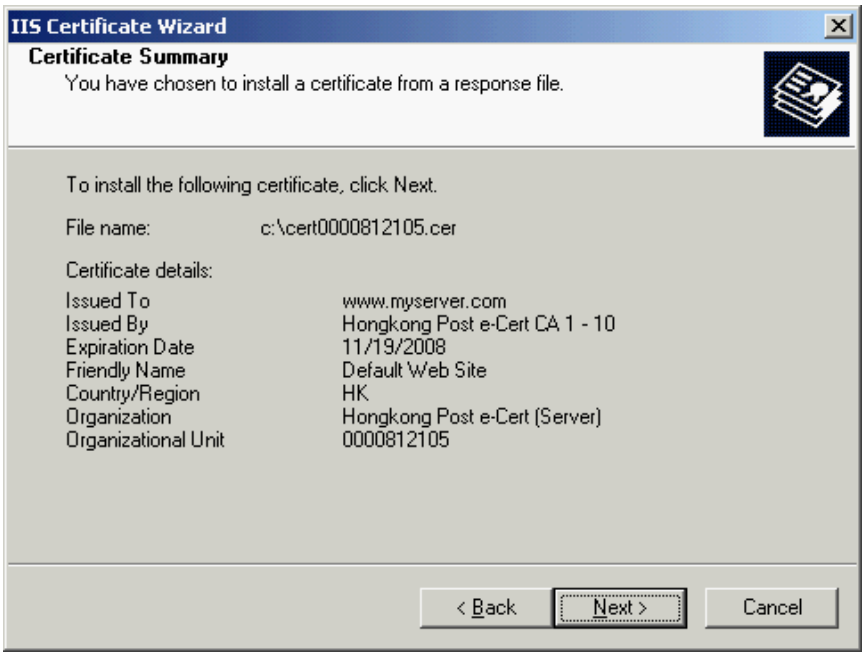
6. Click "Browse" to locate the "Hongkong Post e-Cert (Server)" certificate that you downloaded in Part C Step 7, and then click "Next".



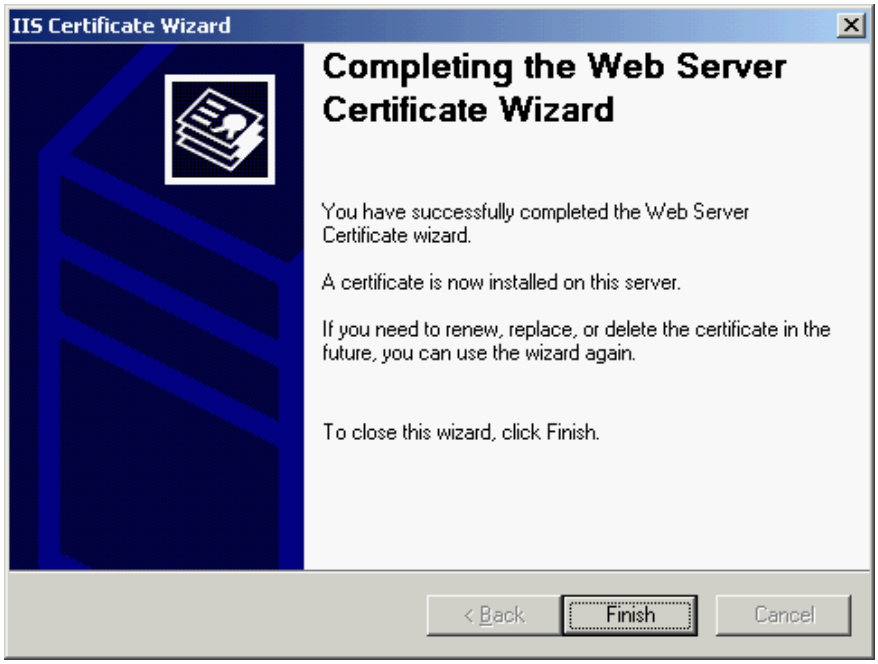
7. Specify 443 for the "SSL port this web site should use", and then click "Next". (For IIS 5.0 , please skip this step and go to step 8)



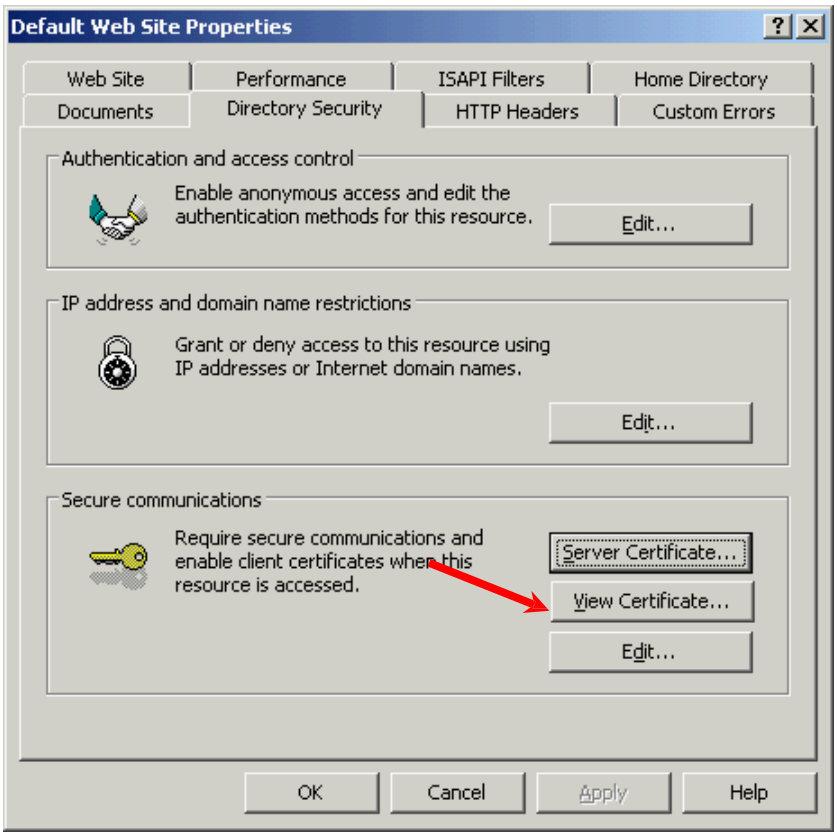
8. Click "Next".



9. Click “Finish” to close the wizard.



10. Click “View Certificate” to view the server certificate.



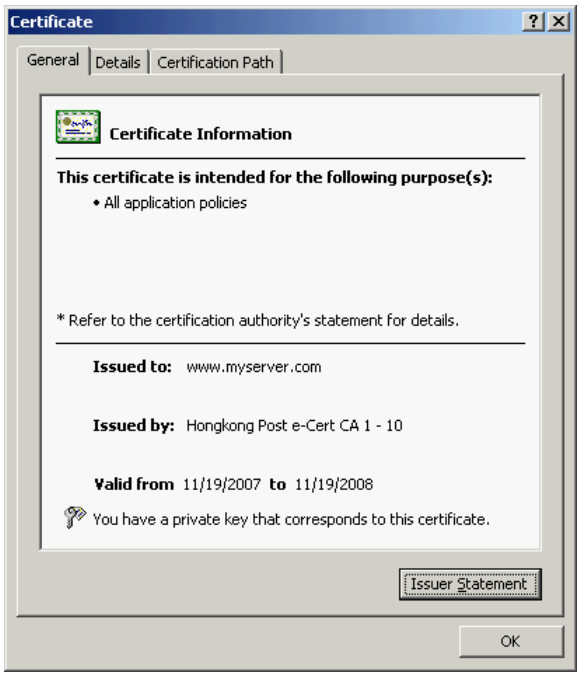
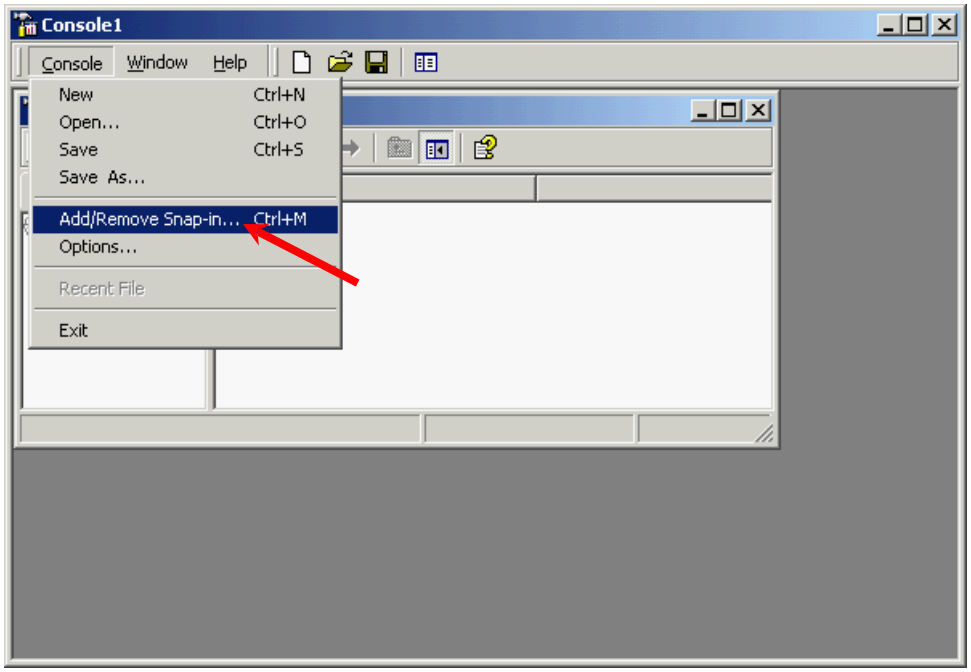


Figure 3: “Hongkong Post e-Cert (Server)” certificate has been successfully installed

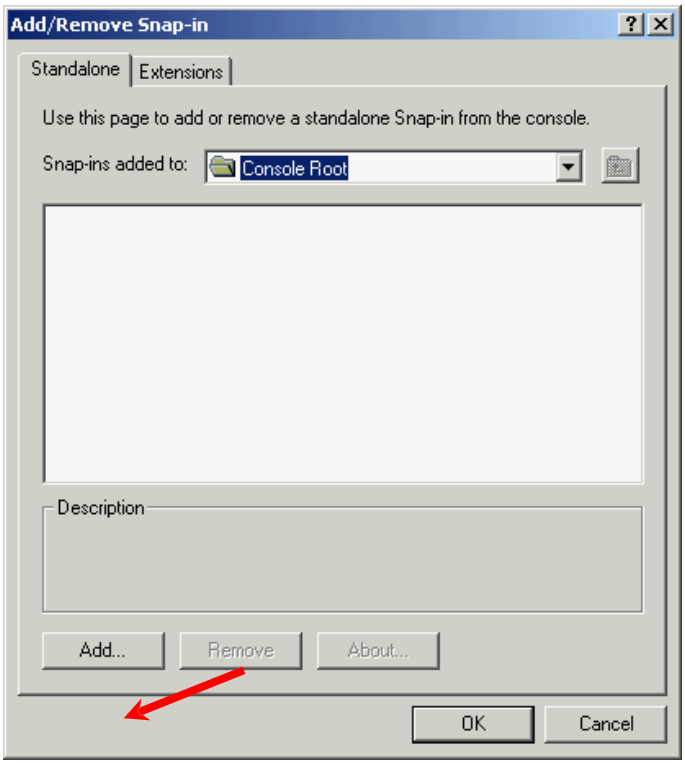
F. Backing up the Private Key

Backing up the Private Key for IIS 5.0

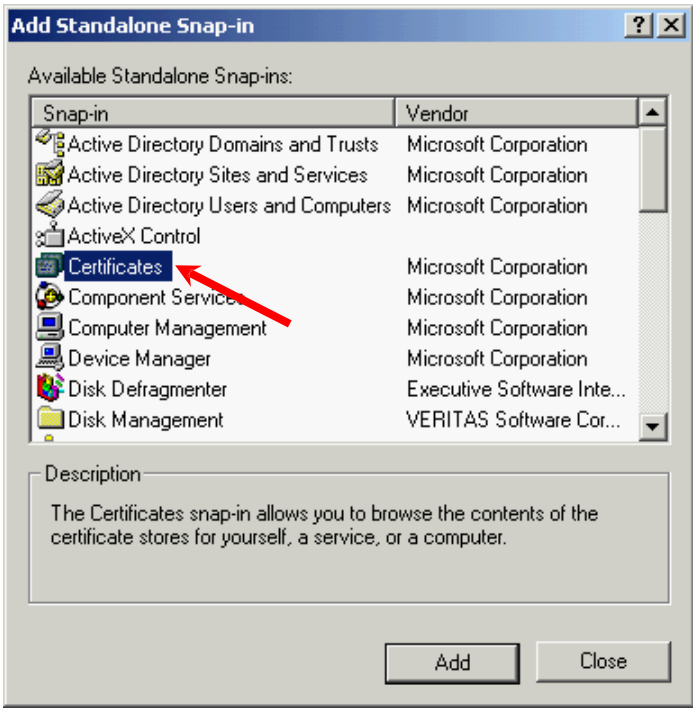
1. Start Microsoft Management Console (MMC) by clicking "Start" > "Run", type "mmc" and click OK, and then select "Add/Remove Snap-in" from the "Console" menu.



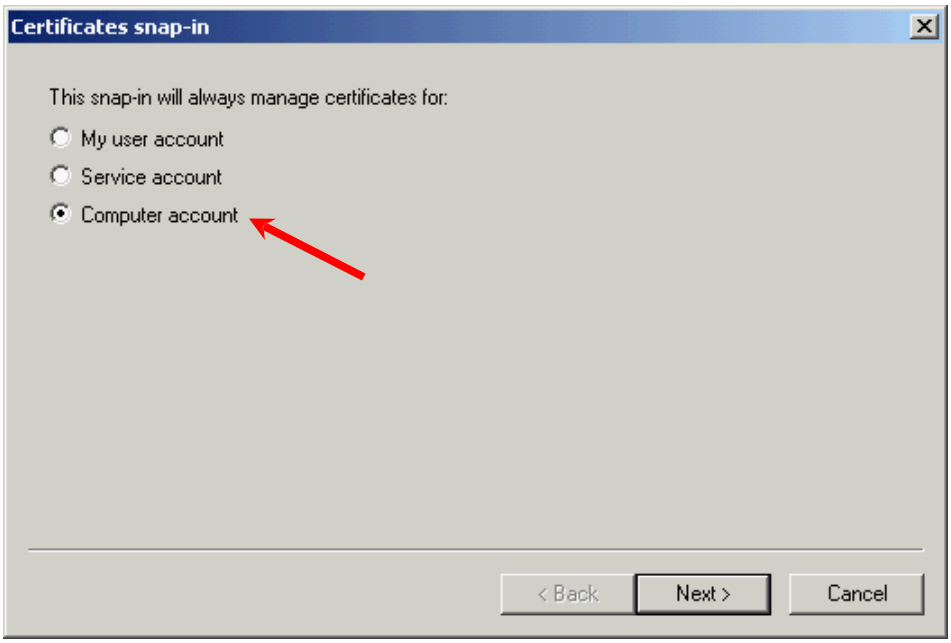
2. Click "Add".



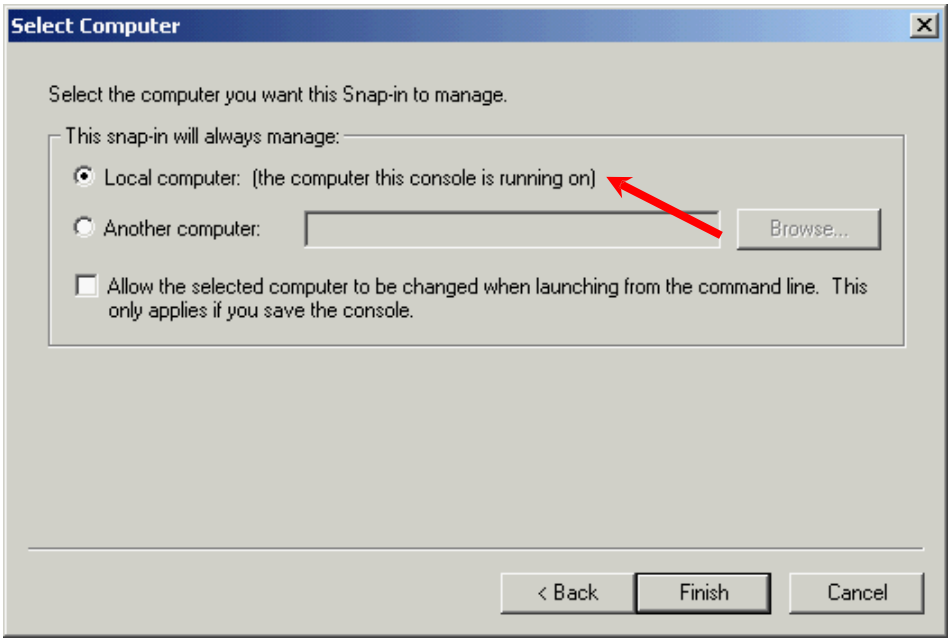
3. Select “Certificates”, and then click “Add”.



4. Select “Computer account”, and then click “Next”.

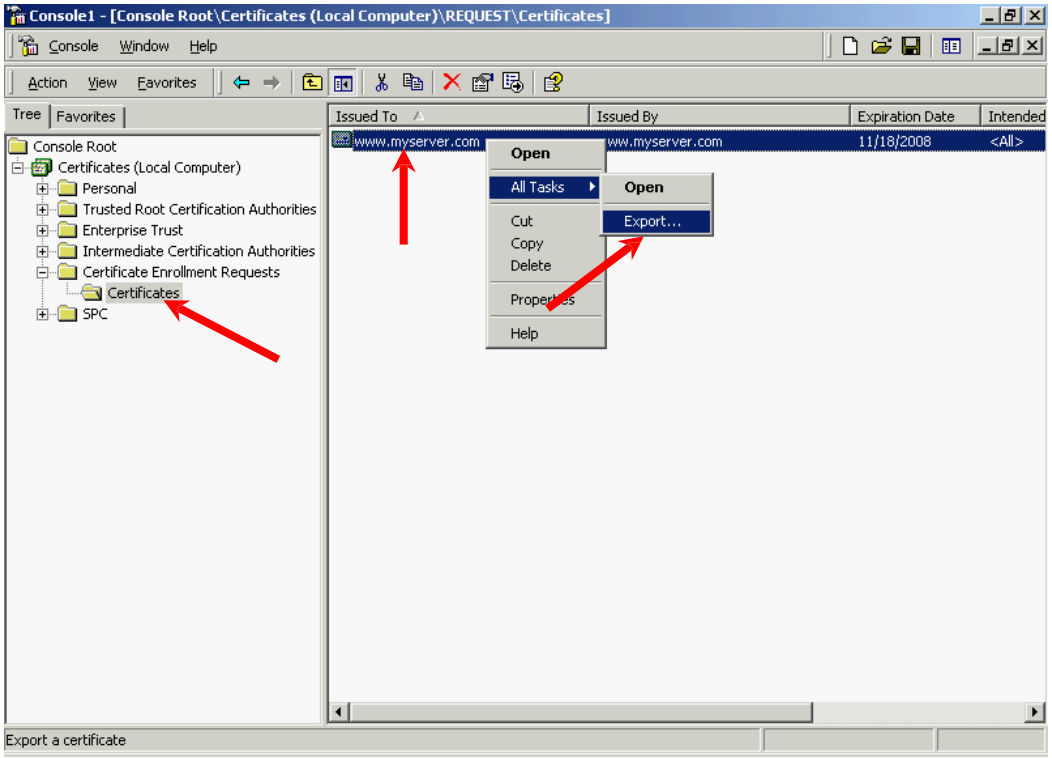


5. Select “Local computer”, and then click “Finish”.

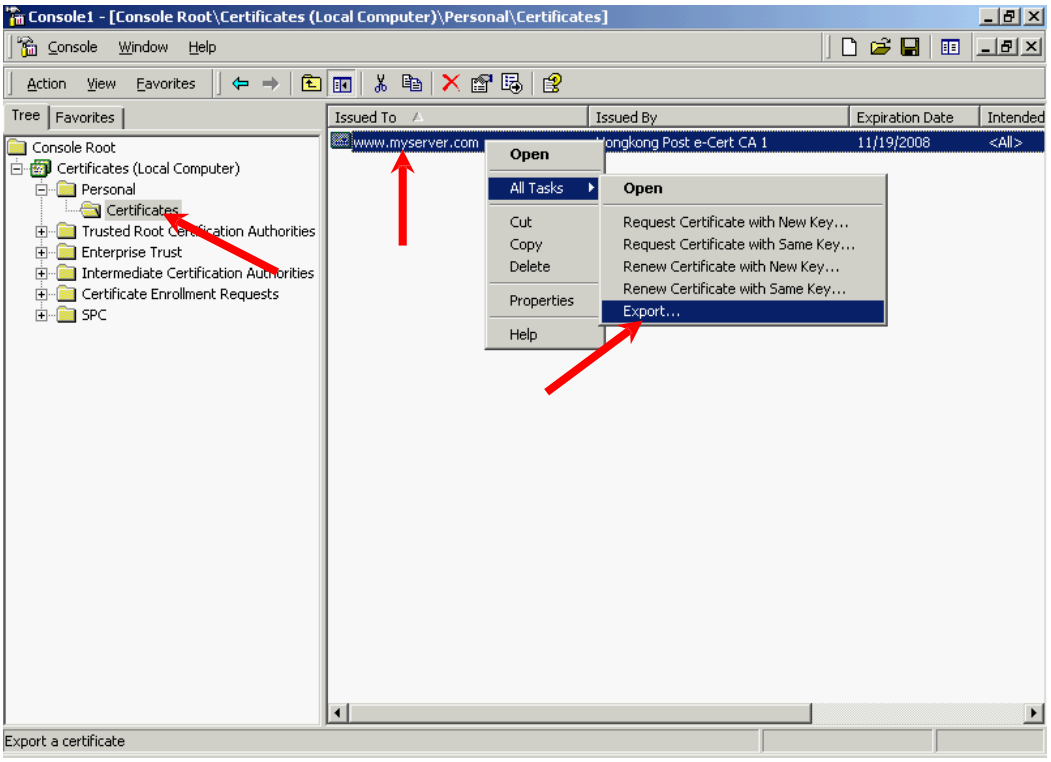


6. Close the “Add Standalone Snap-in” dialog box, and then click “OK” to close the “Add/Remove Snap-in” dialog box.

7. Backup the private key.
   - To backup the private key of a pending request, expand “Certificate Enrollment Requests” (or named “REQUESTS” in some systems) and select “Certificates”, select the pending request that you just created, right-click and then select “All Tasks” > “Export”.

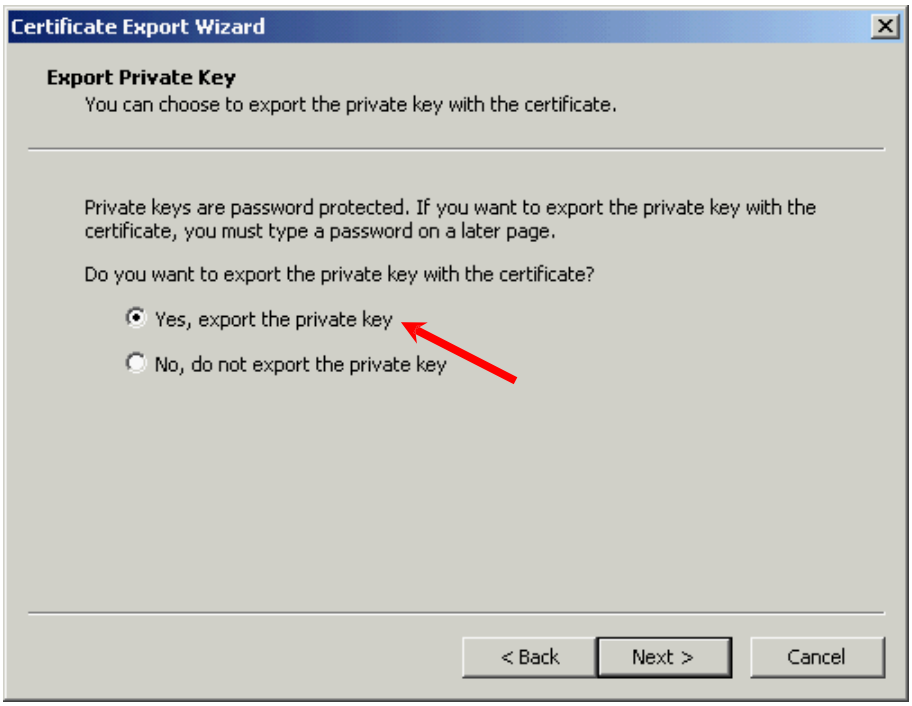


- To backup the private key of an existing certificate, expand "Personal" and select "Certificates", select the certificate that you would like to make a backup, right-click and then select "All Tasks" > "Export".

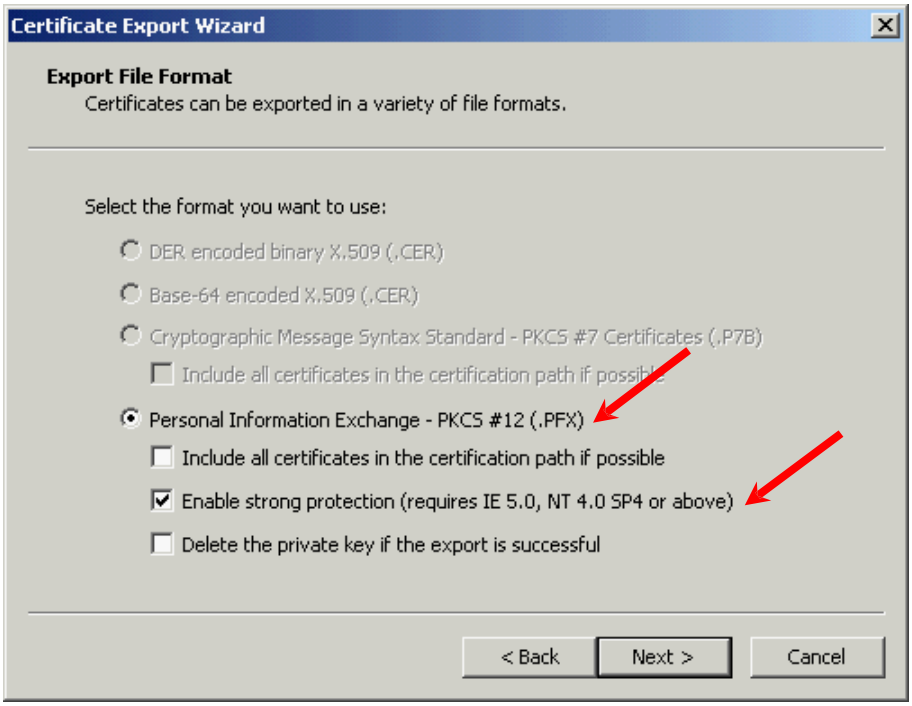


8. In the "Certificate Export Wizard", click "Next" to continue.

9. Select “Yes, export the private key”, and then click “Next”.

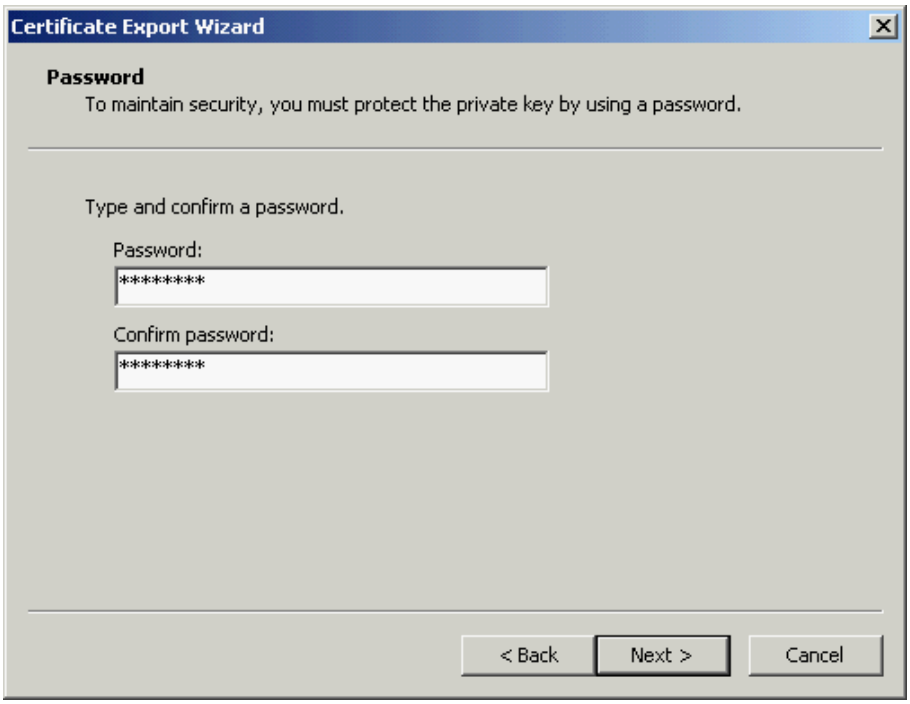


10. Select “Personal Information Exchange - PKCS #12” and check the box “Enable strong protection”, and then click “Next”

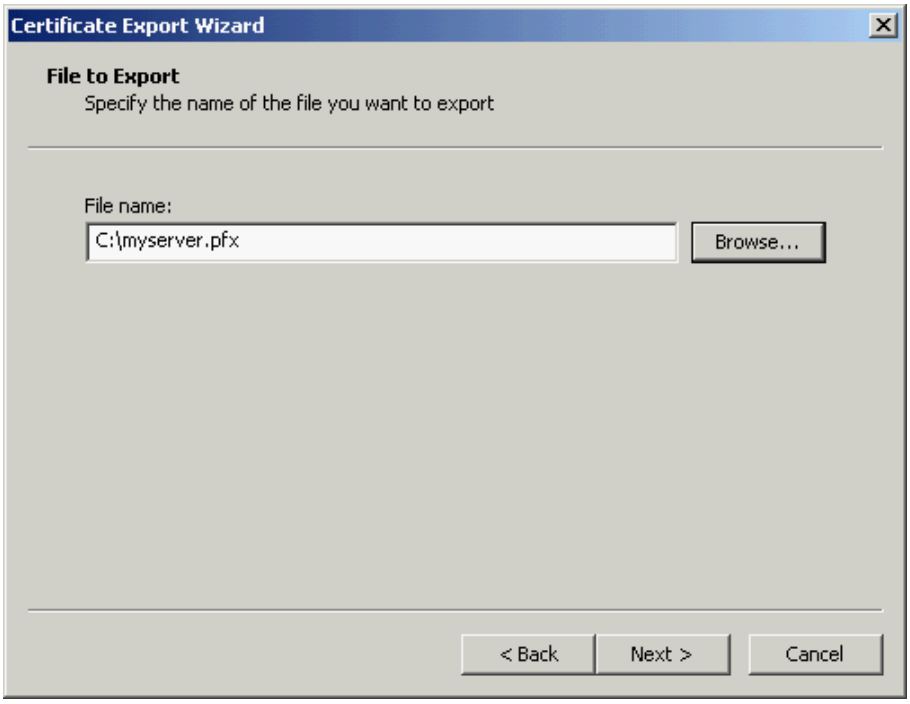


11. Type and confirm a password for the private key, and then click “Next”.

> *Note: It is very important that you remember this password. If you forget it, you will be unable to restore your private key.*



12. Specify the name of the file you want to export, and then click “Next”. (By default, the file will be saved with a .PFX extension.)

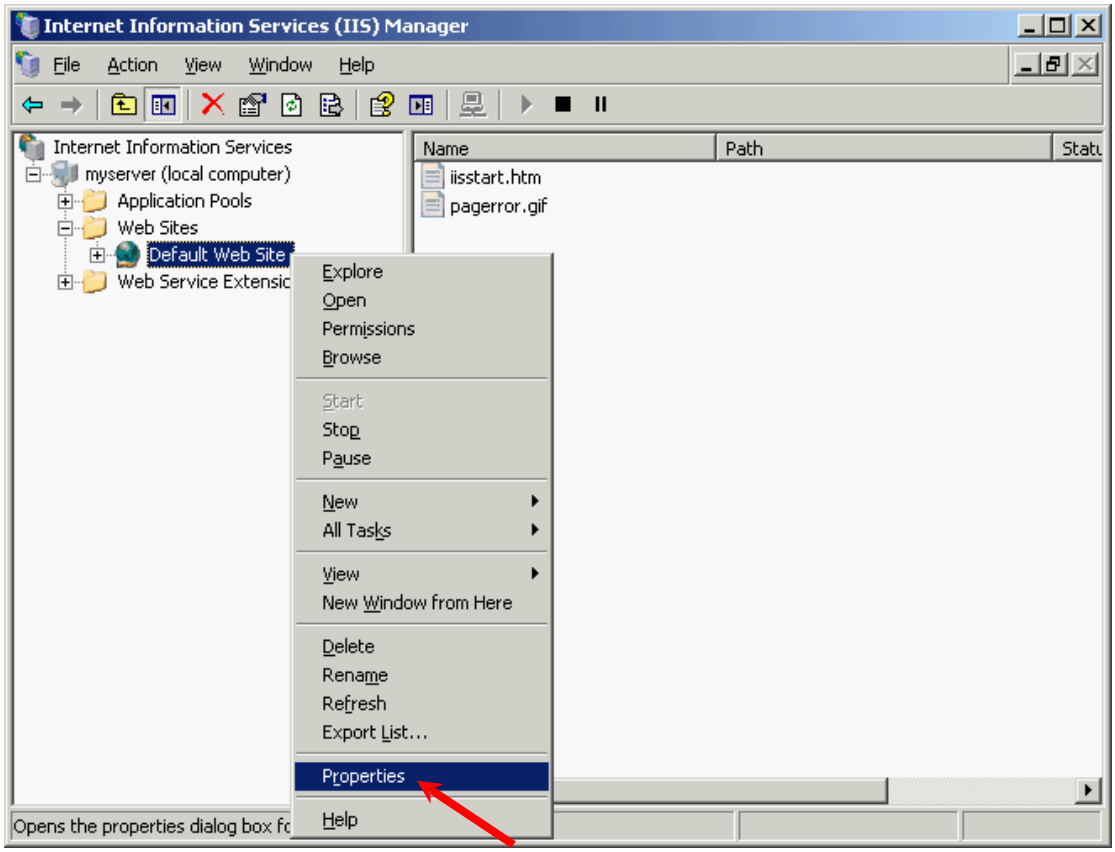


13. Click “Finish” to close the wizard.

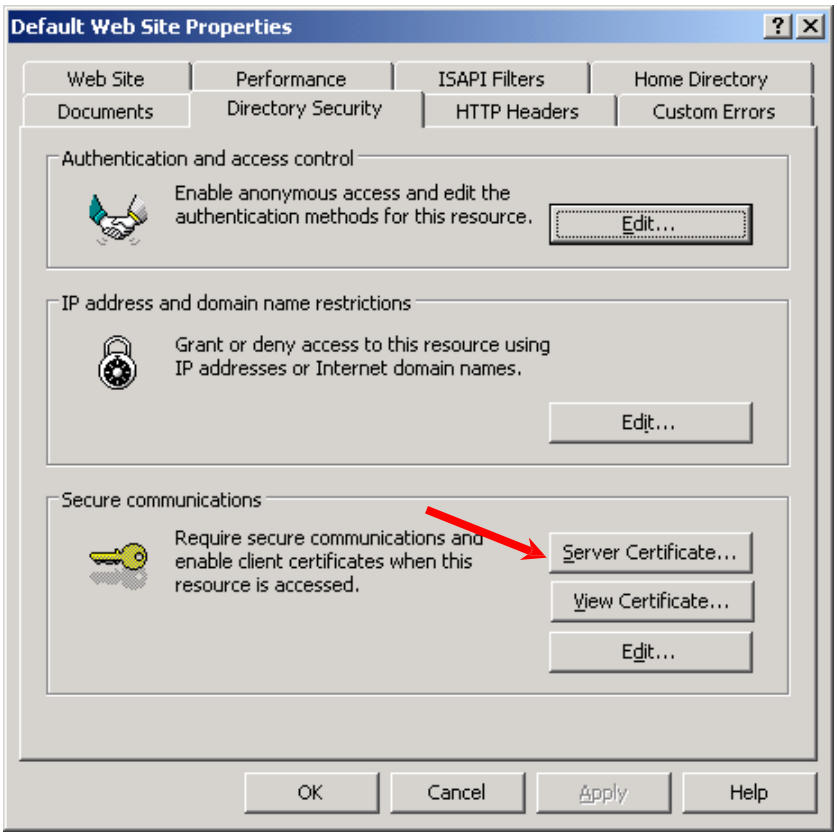
14. Click “OK” to complete.

Backing up the Private Key for IIS 6.0

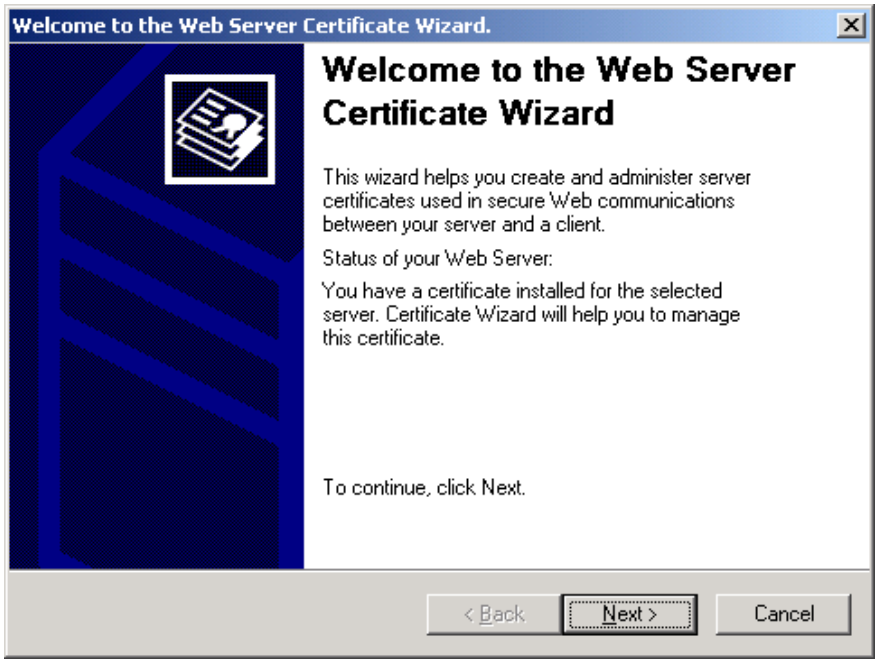
1. Start Internet Information Services (IIS) Manager by clicking “Start” > “All Programs” > “Administrative Tools” > “Internet Information Services (IIS) Manager”.
2. In the “Internet Information Services (IIS) Manager” pane, expand “Web Sites” and select your web site, right-click and then click “Properties”.



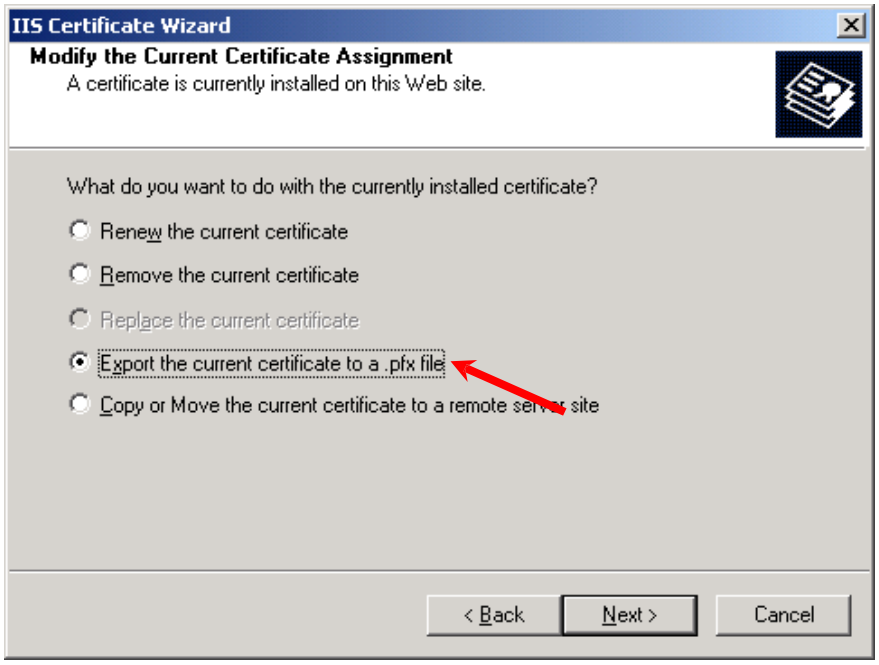
3. In the “Directory Security” tab, click “Server Certificate”.



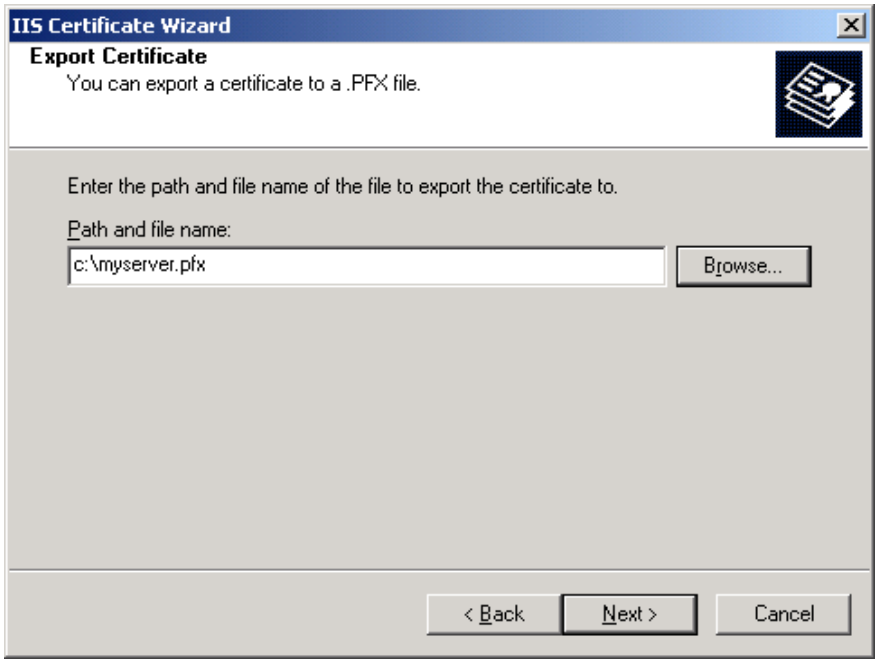
4. In the “Web Server Certificate Wizard”, click “Next” to continue.



5. Select “Export the current certificate to a .pfx file”, and then click “Next”.

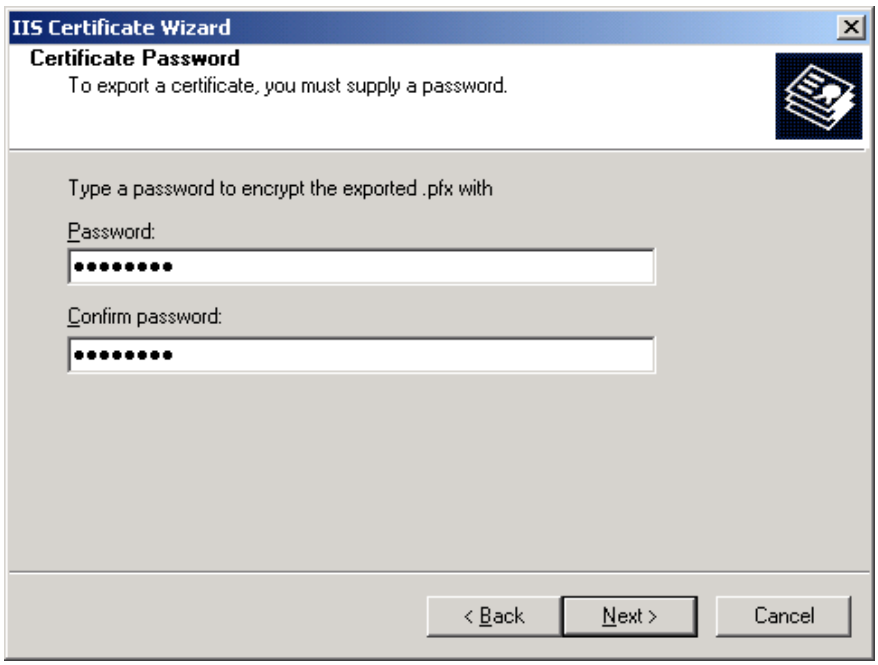


6. Enter the path and file name of the file to export the certificate to, and then click “Next”.

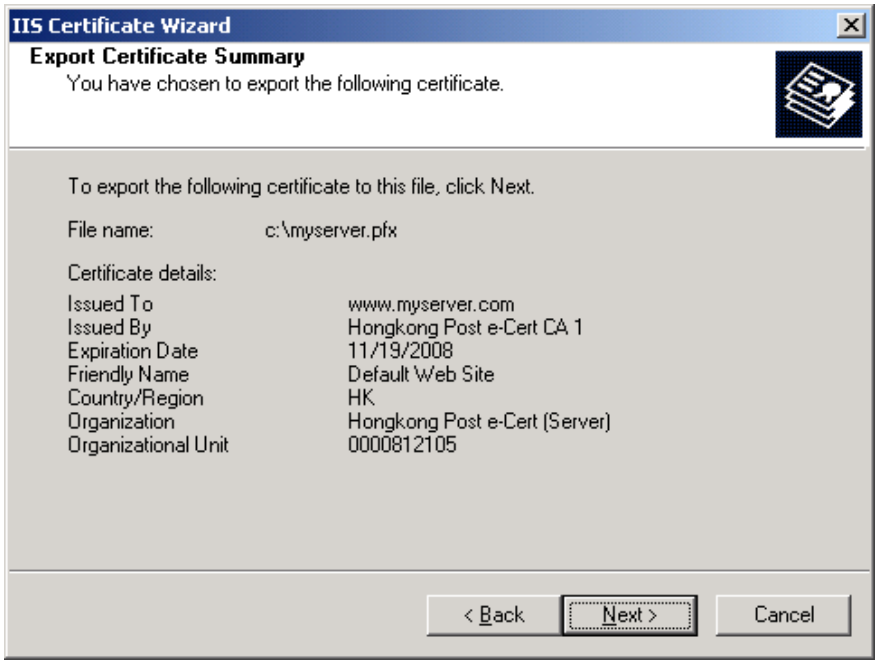


7. Type and confirm a password to encrypt the exported .pfx with, and then click "Next".

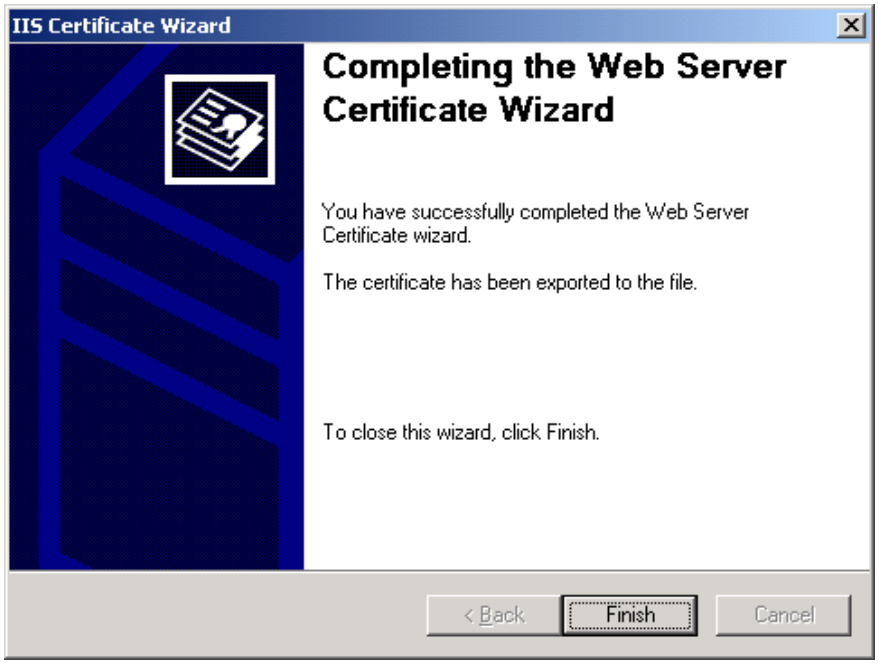
Note: It is very important that you remember this password. If you forget it, you will be unable to restore your private key.



8. Click "Next".



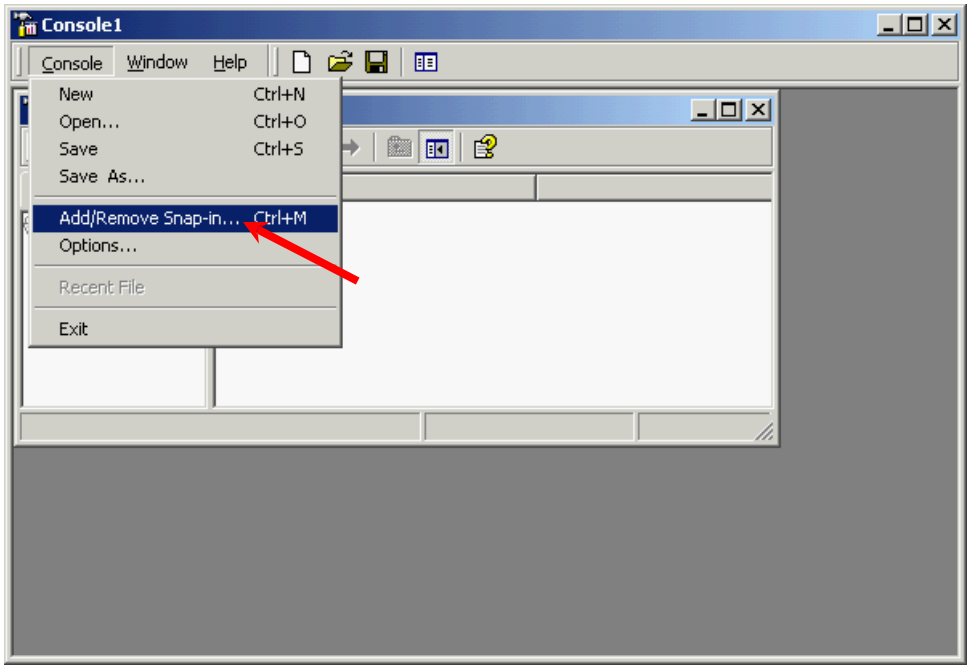
9. Click “Finish” to close the wizard.



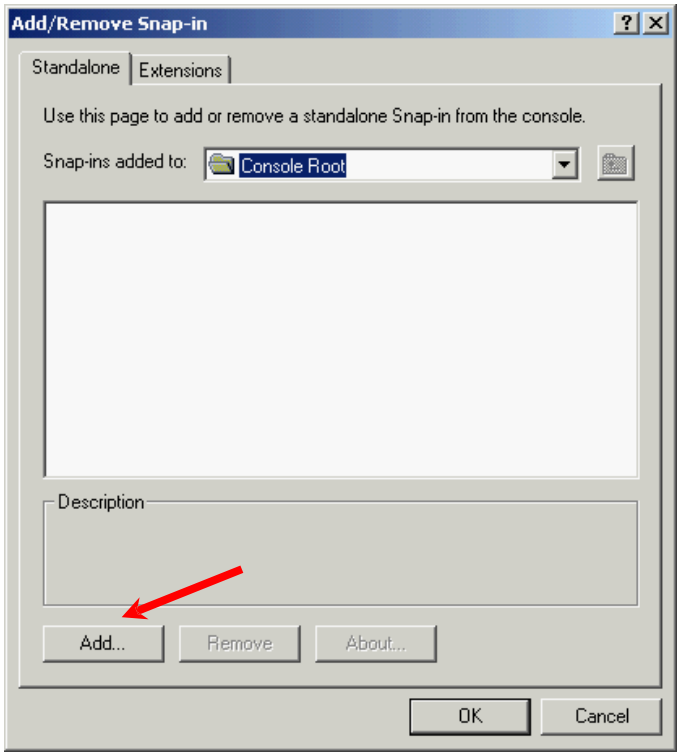
G. Restoring the Private Key

Restoring the Private Key for IIS 5.0

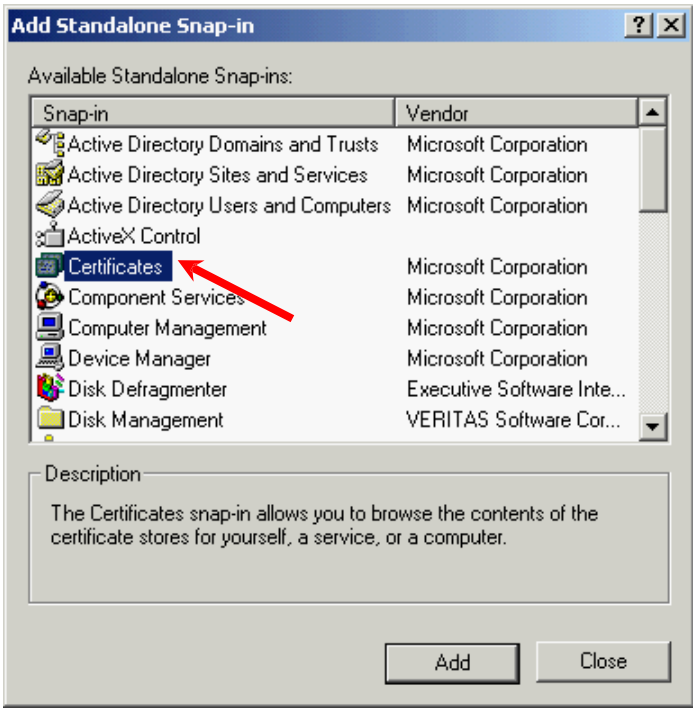
1. Start Microsoft Management Console (MMC) by clicking "Start" > "Run", type "mmc" and click OK, and then select "Add/Remove Snap-in" from the "Console" menu.



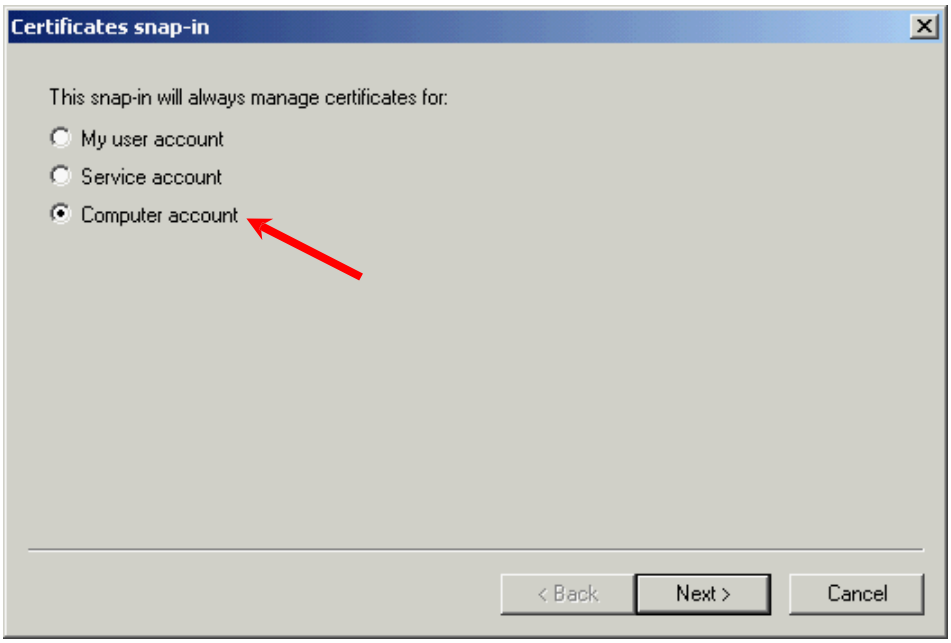
2. Click "Add".



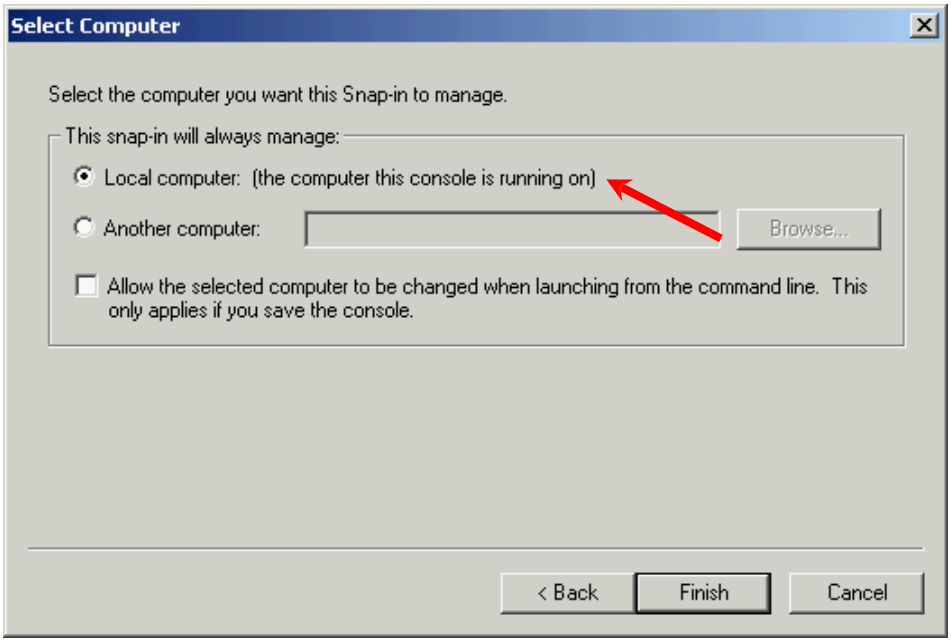
3. Select “Certificates”, and then click “Add”.



4. Select “Computer account”, and then click “Next”.

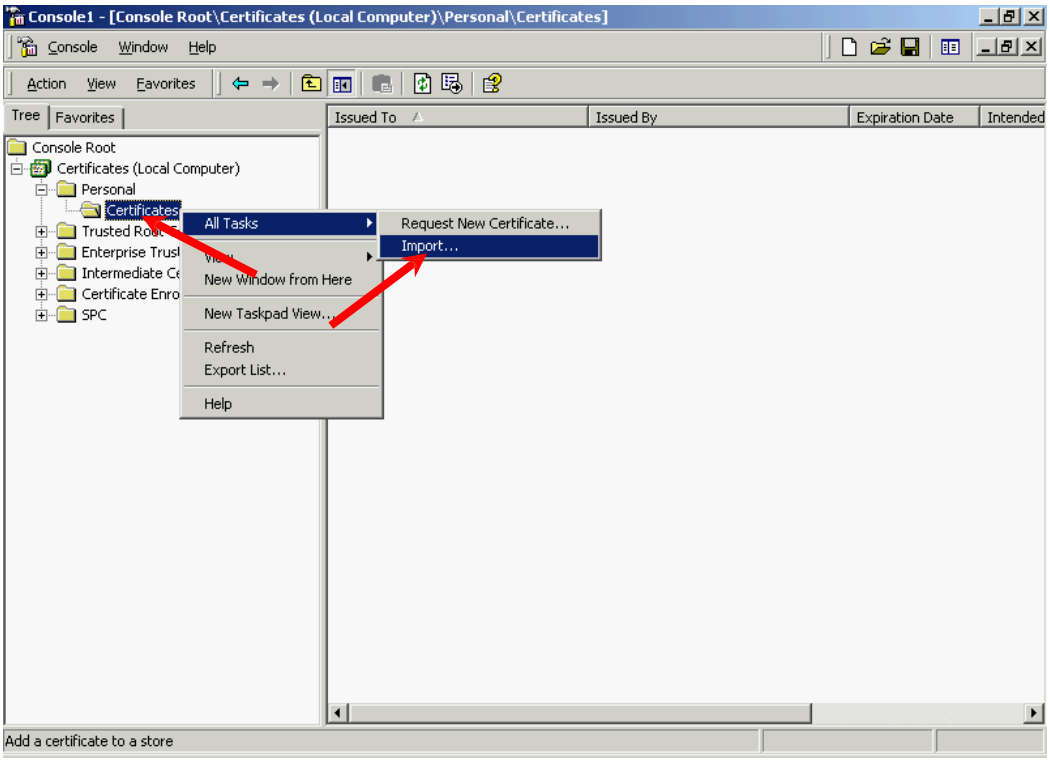


5. Select “Local computer”, and then click “Finish”.

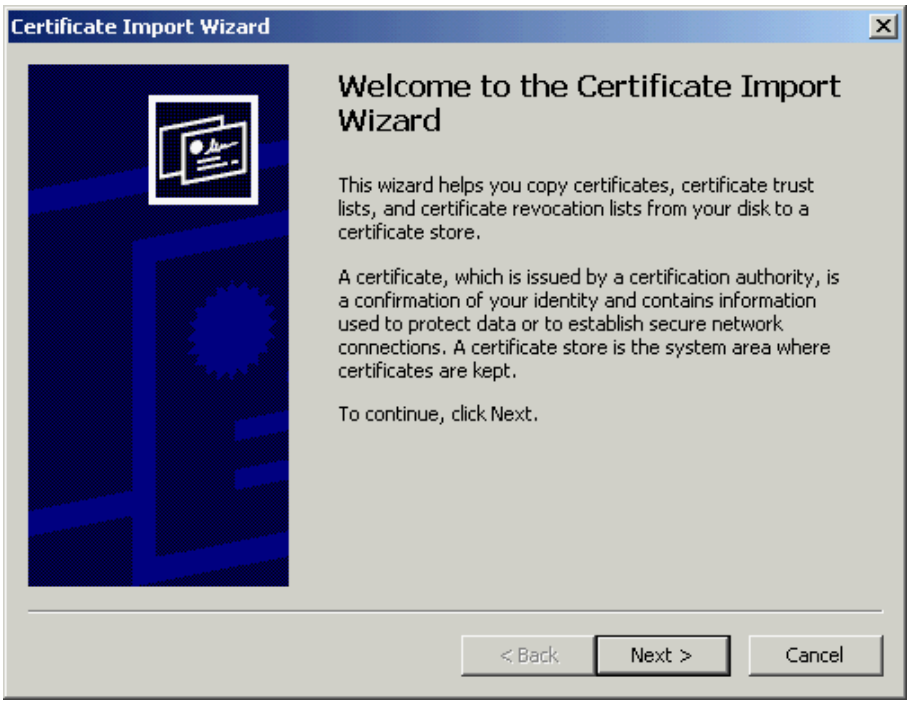


6. Close the “Add Standalone Snap-in” dialog box, and then click “OK” to close the “Add/Remove Snap-in” dialog box.

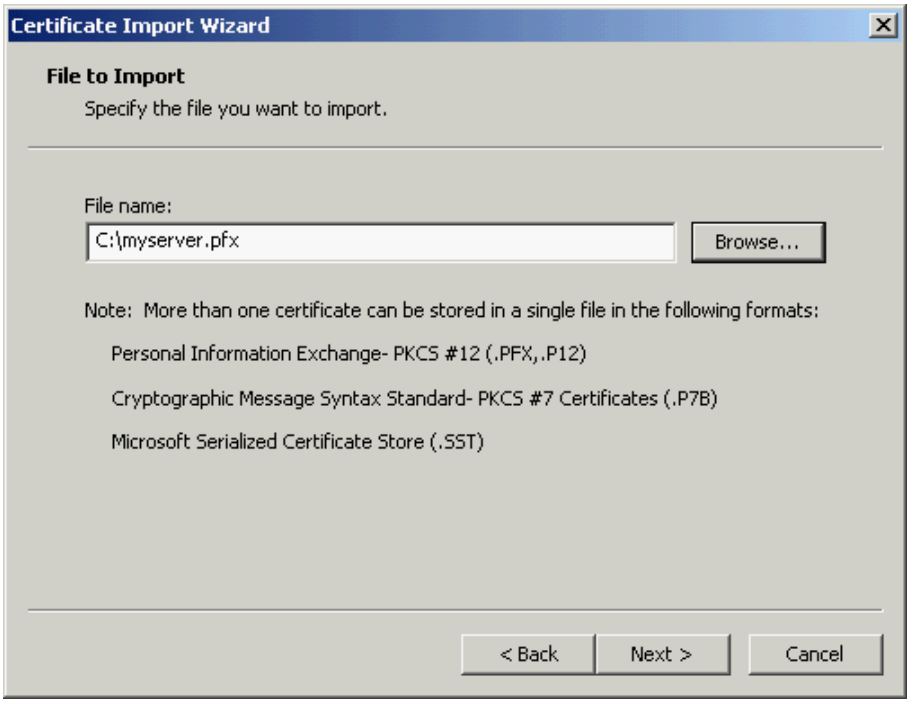
7. Expand “Personal” and select “Certificates”, right-click and then select “All Tasks” > “Import”. (To restore the private key of a pending request, expand “Certificate Enrollment Requests” (or named “REQUESTS” in some systems).)



8. In the “Certificate Import Wizard”, click “Next” to continue.

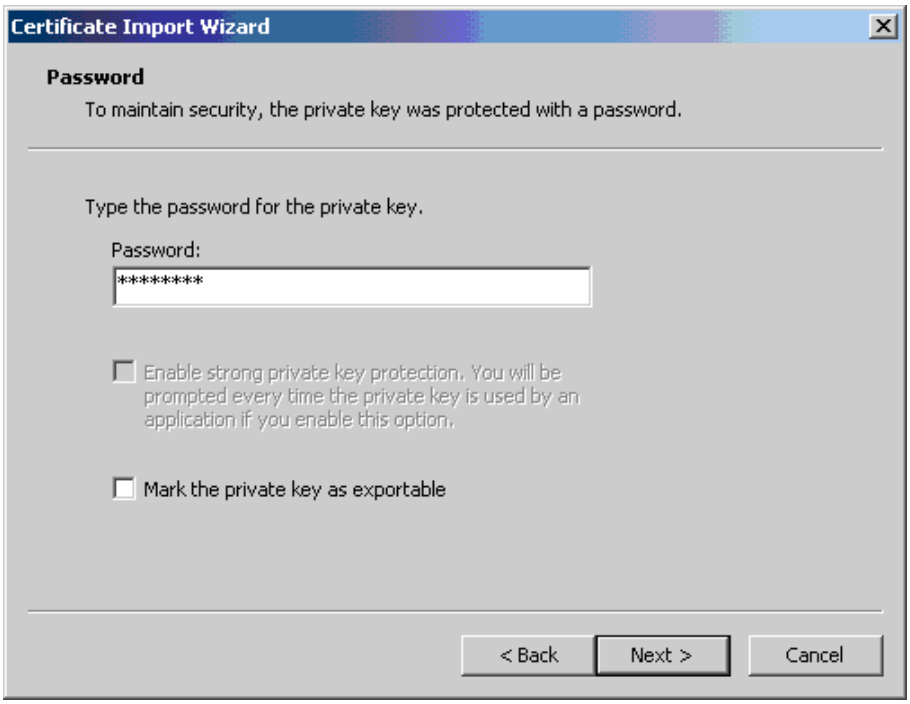


9. Click “Browse” to locate the backup file of your private key, and then click “Next”.

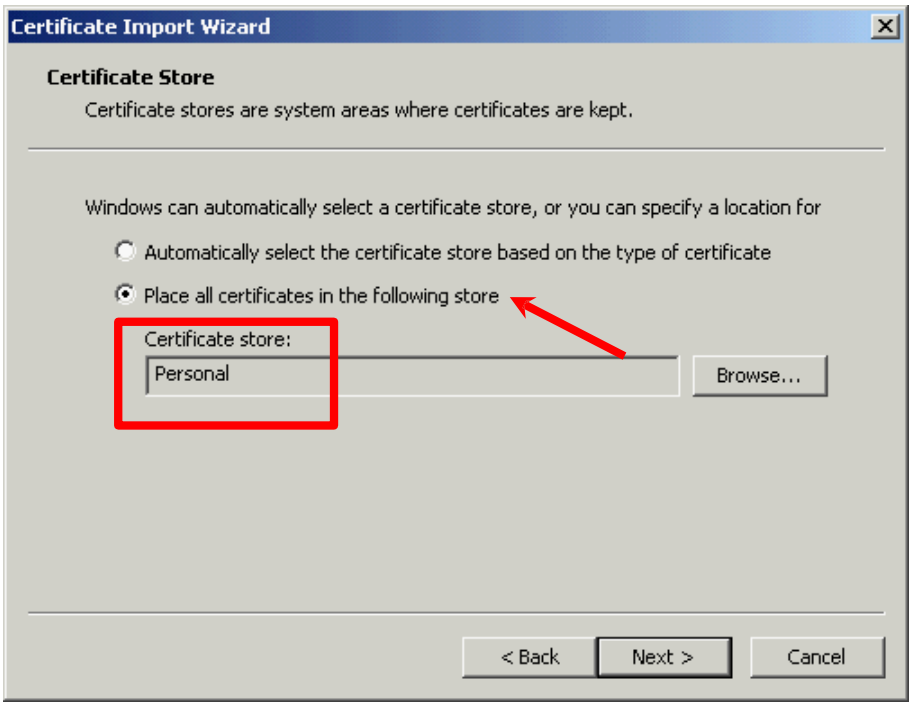


10. Type the password for the private key and then click “Next”.

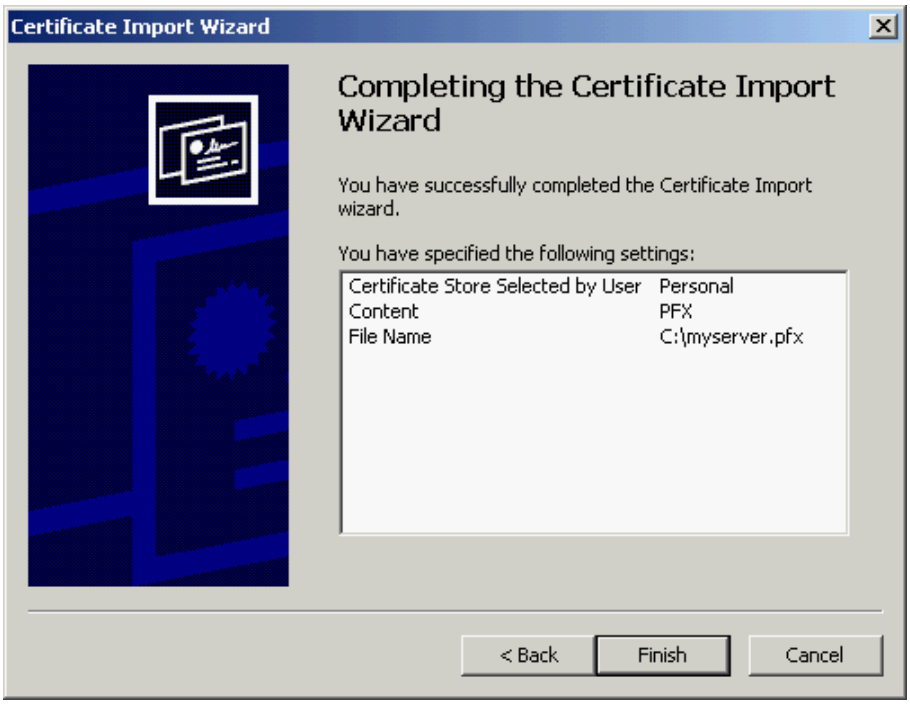
> *Note: To allow you to back up or transport your private key at a later time, you may mark this private key as exportable.*



11. Select “Place all certificates in the following store”, and then click “Next”.



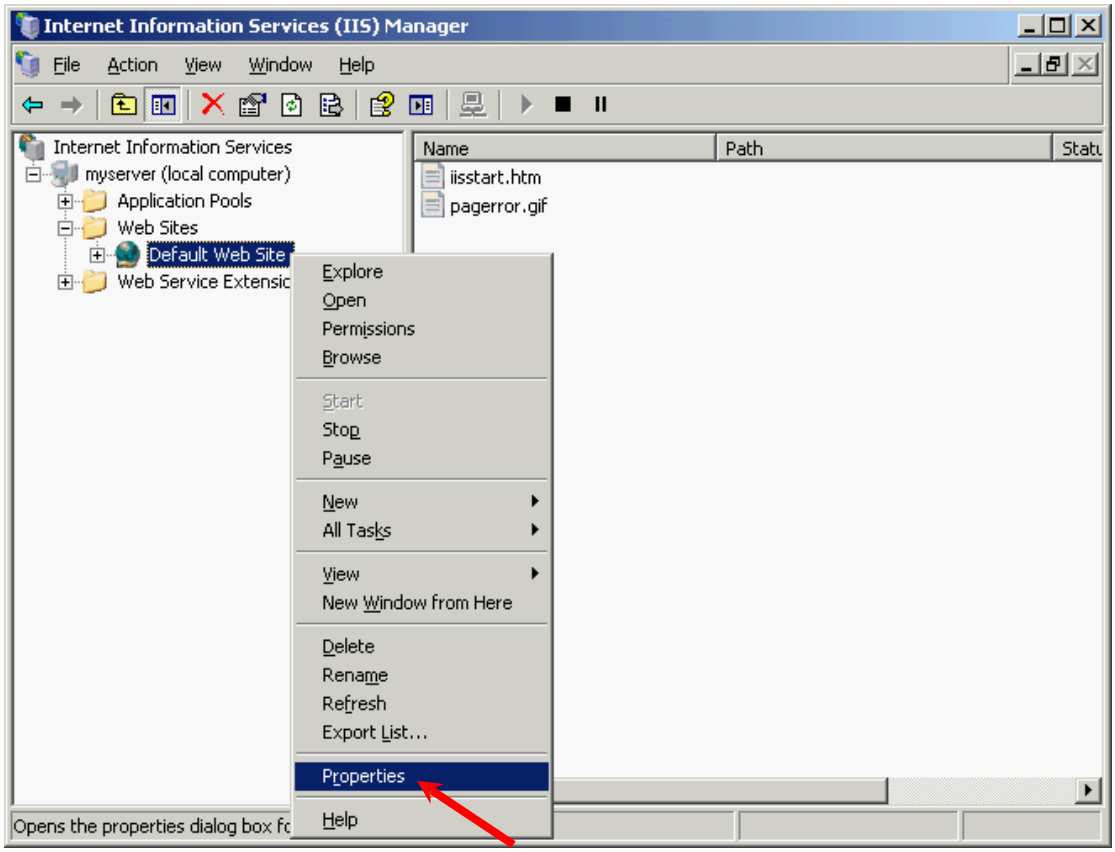
12. Click “Finish” to close the wizard.



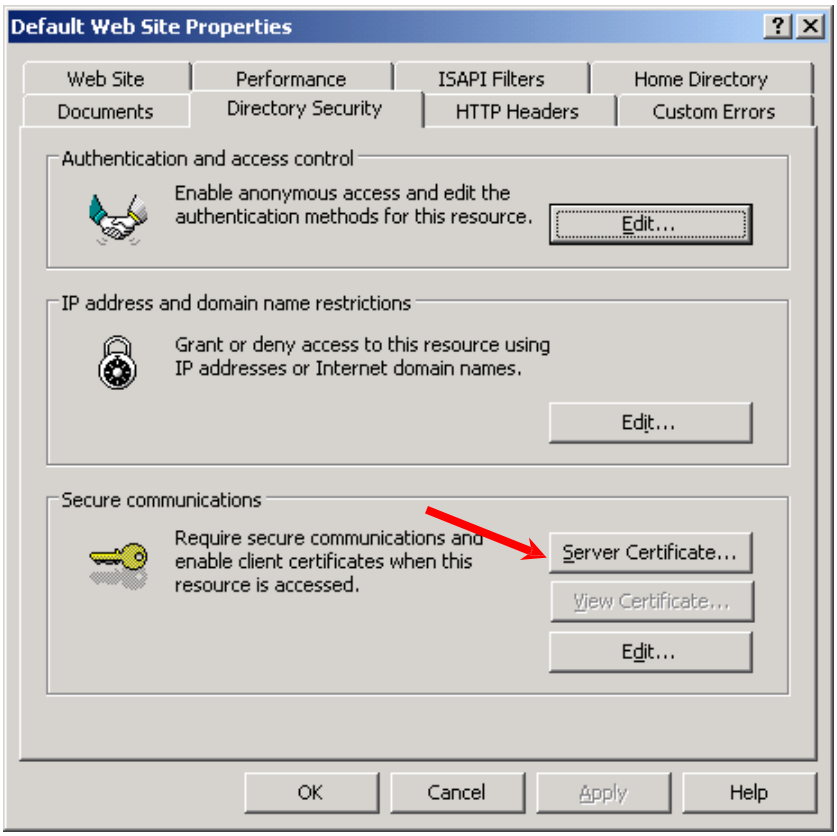
13. Click “OK” to complete.

Restoring the Private Key for IIS 6.0

1. Start Internet Information Services (IIS) Manager by clicking "Start" > "All Programs" > "Administrative Tools" > "Internet Information Services (IIS) Manager".
2. In the "Internet Information Services (IIS) Manager" pane, expand "Web Sites" and select your web site, right-click and then click "Properties".

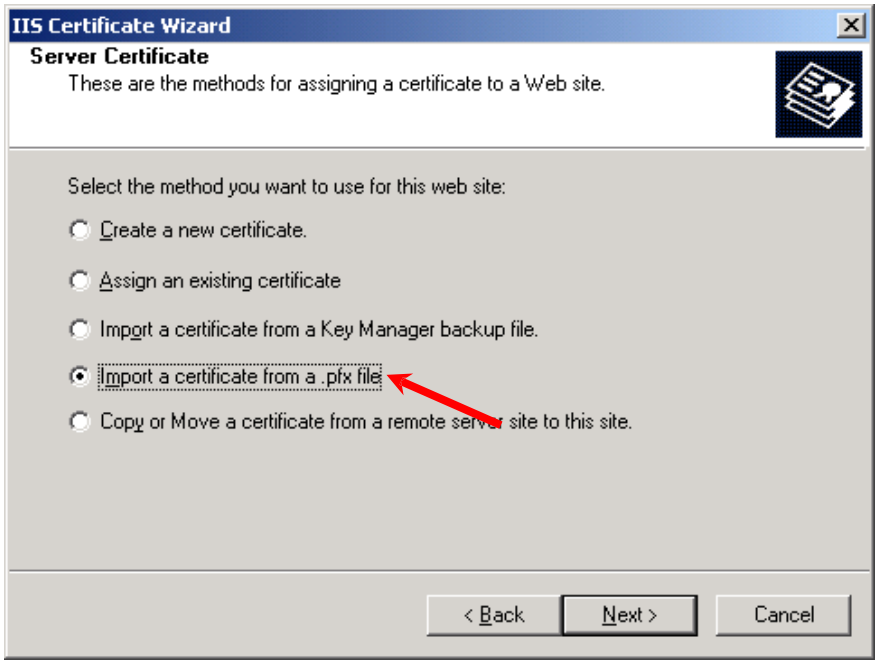


3. In the “Directory Security” tab, click “Server Certificate”.



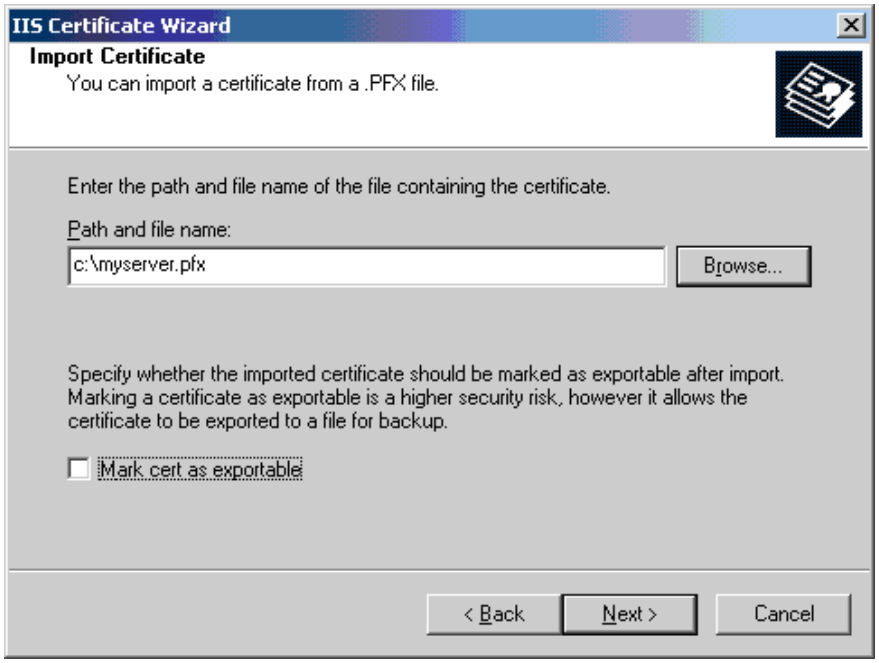
4. In the “Web Server Certificate Wizard”, click “Next” to continue.

5. Select “Import a certificate from a .pfx file”, and then click “Next”.

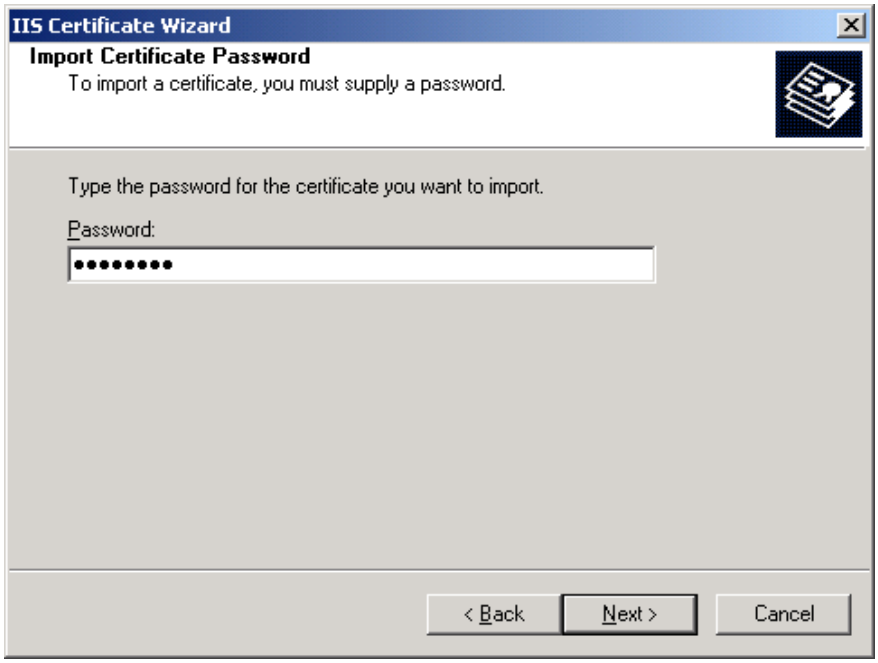


6. Enter the path and file name of the file containing the certificate and then click “Next”.

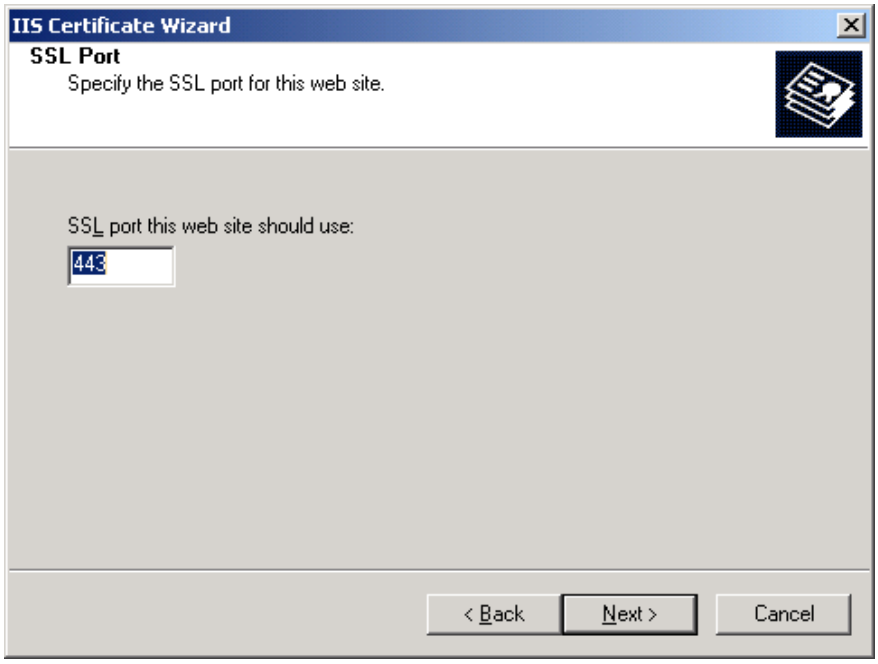
Note: To allow you to back up or transport your certificate at a later time, you may mark this certificate as exportable.



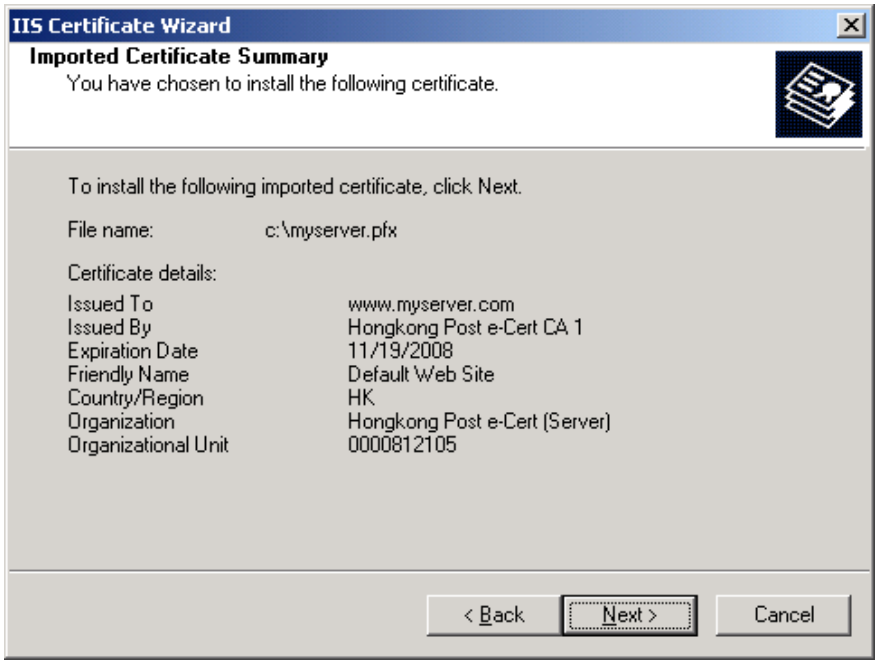
7. Type the password for the certificate you want to import, and then click "Next".



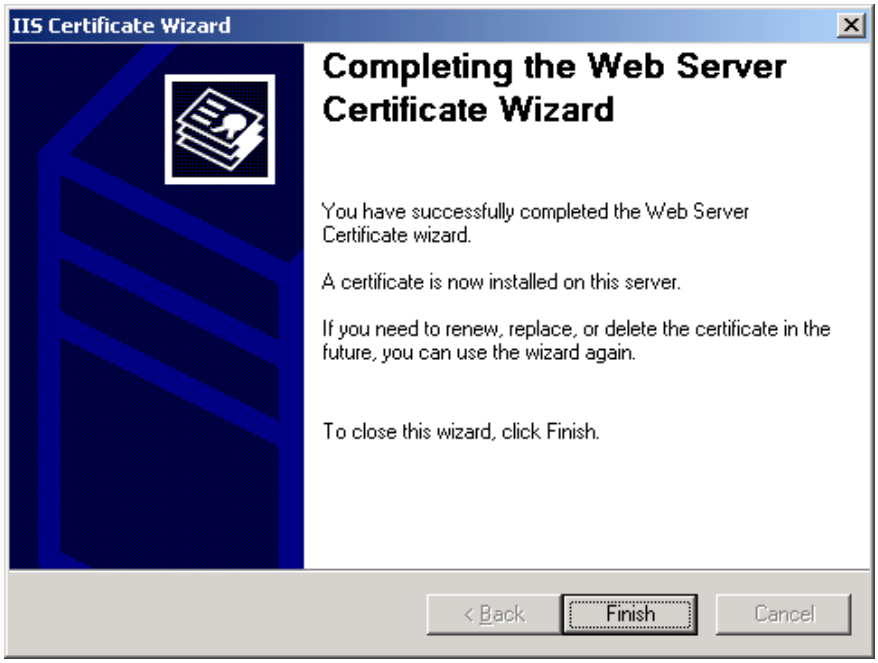
8. Specify 443 for the "SSL port this web site should use", and then click "Next".

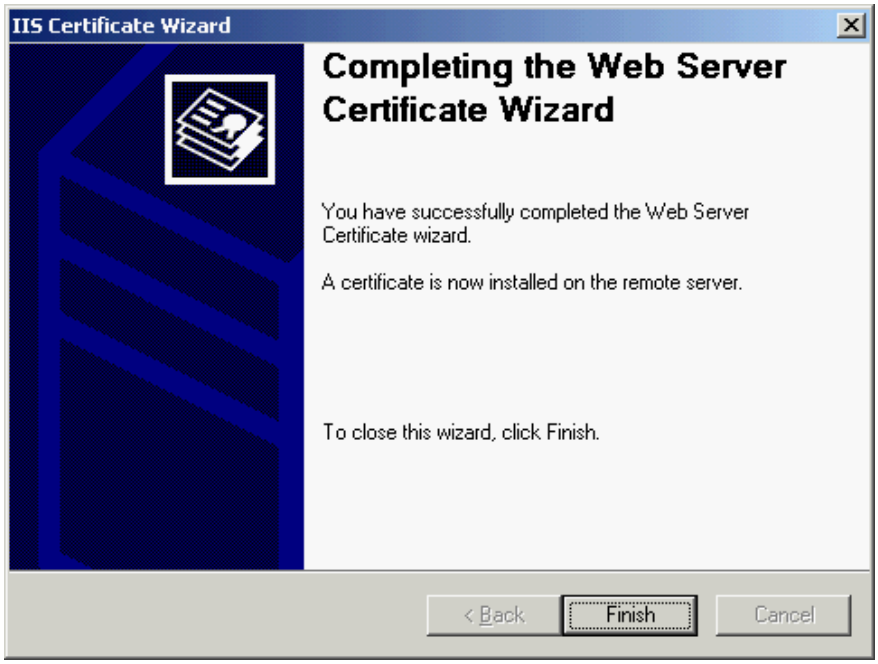


9. Click “Next”.



10. Click “Finish” to close the wizard.




IIS Certificate Wizard
Completing the Web Server Certificate Wizard
You have successfully completed the Web Server Certificate wizard.
A certificate is now installed on the remote server.
To close this wizard, click Finish.
< Back
Finish
Cancel