



## **e-Cert (Server) User Guide**

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

## Table of Content

---

A.	Guidelines for e-Cert (Server) Applicant .....	2
	New Application .....	3
	Renewal Application .....	4
B.	Generating Certificate Signing Request (CSR) .....	5
	Creating a New Server Certificate .....	7
	Renewing your Current Server Certificate .....	13
C.	Submitting Certificate Signing Request (CSR) .....	16
D.	Installing Hongkong Post Root CA Certificate .....	20
	Installing the “Hongkong Post e-Cert CA 1 - 10” Certificate .....	23
	Installing the “Hongkong Post Root CA 1” Certificate .....	26
E.	Installing Server Certificate .....	29
F.	Backing up the Private Key .....	35
	Backing up the Private Key for IIS 5.0 .....	35
	Backing up the Private Key for IIS 6.0 .....	42
G.	Restoring the Private Key .....	47
	Restoring the Private Key for IIS 5.0 .....	47
	Restoring the Private Key for IIS 6.0 .....	53

---

---

## 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:

F. Backing up the Private Key.....	35
G. Restoring the Private Key.....	47

## **New Application**

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

B.	Generating Certificate Signing Request (CSR) .....	5
	Creating a New Server Certificate .....	7
C.	Submitting Certificate Signing Request (CSR) .....	16
D.	Installing Hongkong Post Root CA Certificate .....	20
	Installing the “Hongkong Post e-Cert CA 1 - 10” Certificate .....	23
	Installing the “Hongkong Post Root CA 1” Certificate .....	26
E.	Installing Server Certificate .....	29

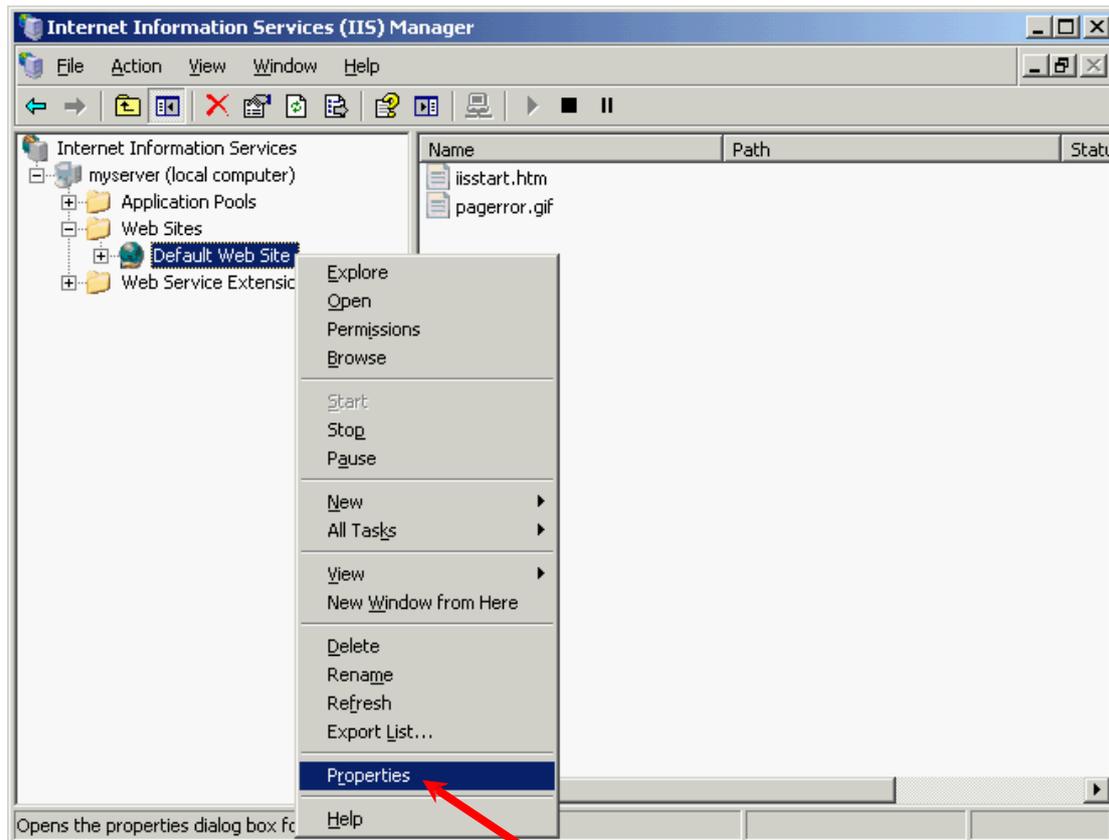
## **Renewal Application**

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

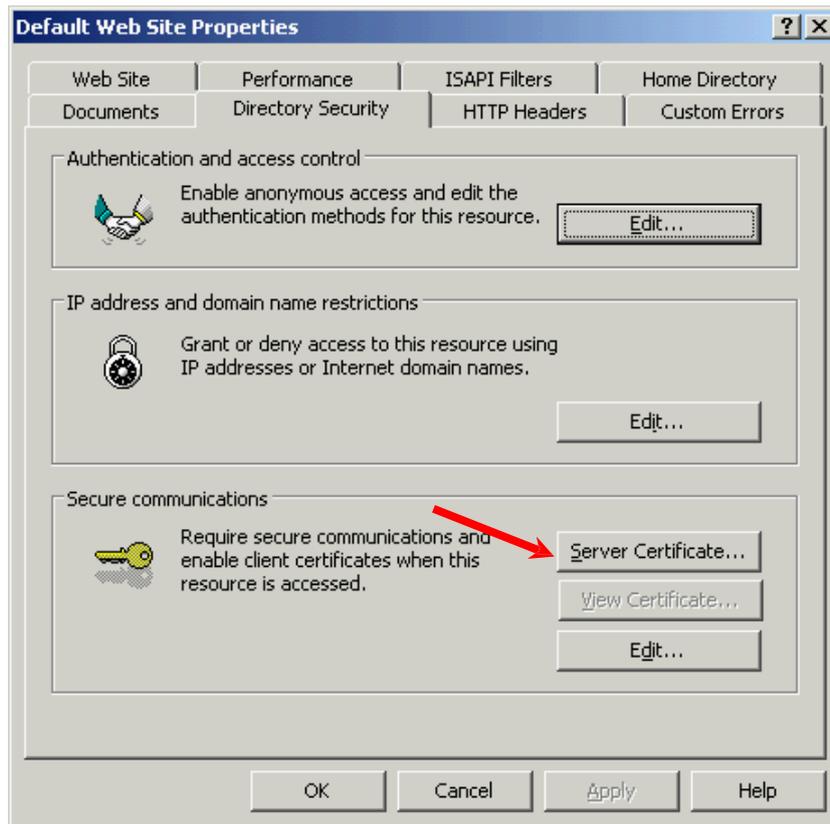
B.	Generating Certificate Signing Request (CSR) .....	5
	Renewing your Current Server Certificate .....	13
C.	Submitting Certificate Signing Request (CSR) .....	16
E.	Installing Server Certificate.....	29

## 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”.



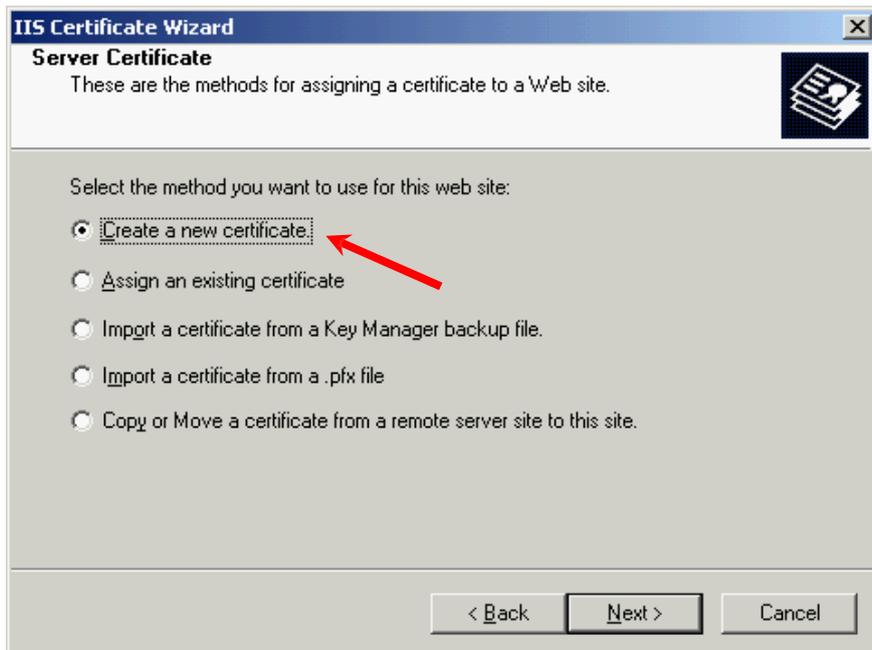
## **Creating a New Server Certificate**

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

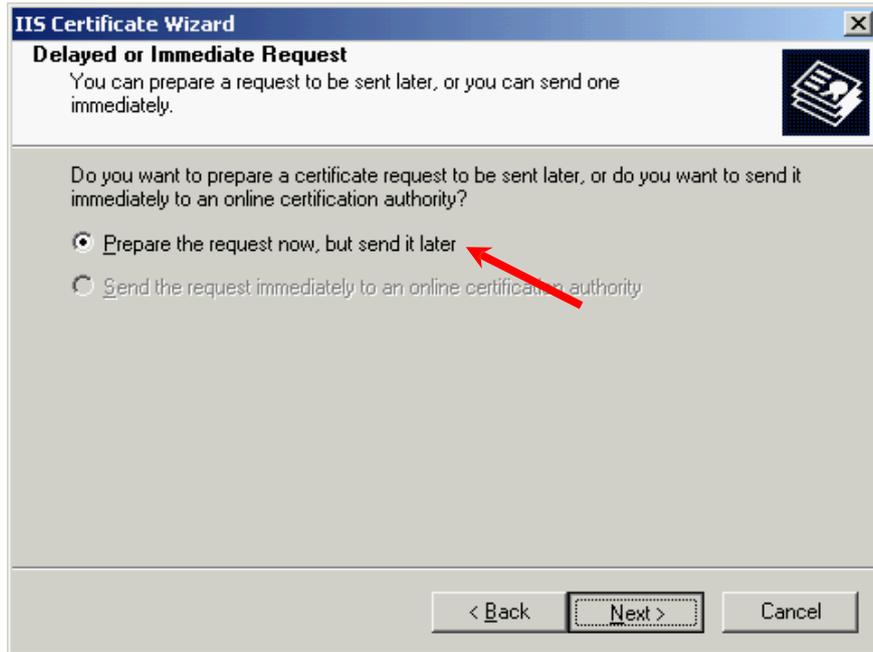
4. In the “Web Server Certificate Wizard”, click “Next” to continue.



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

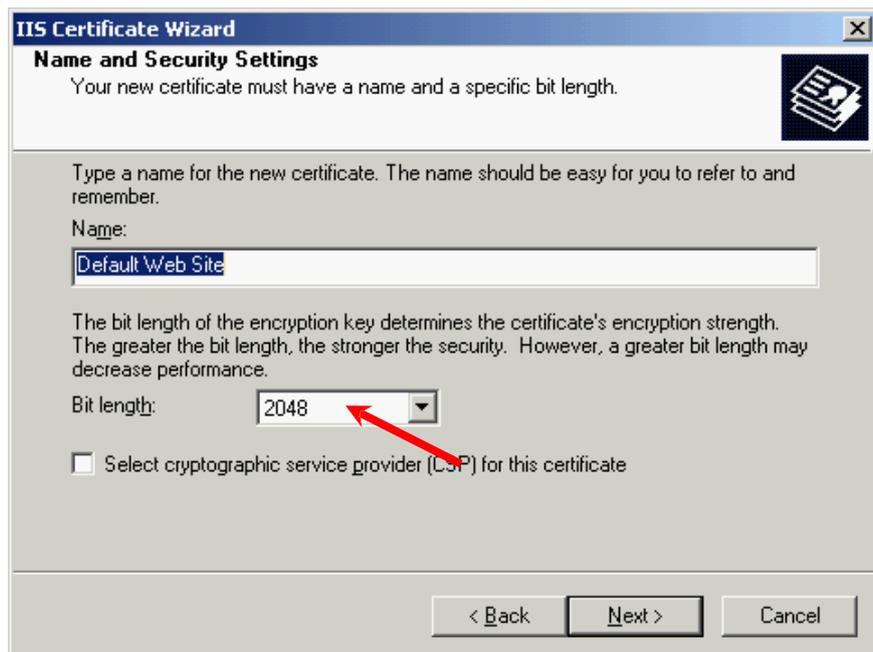


6. Select “Prepare the request now, but send it later”, and then click “Next”.

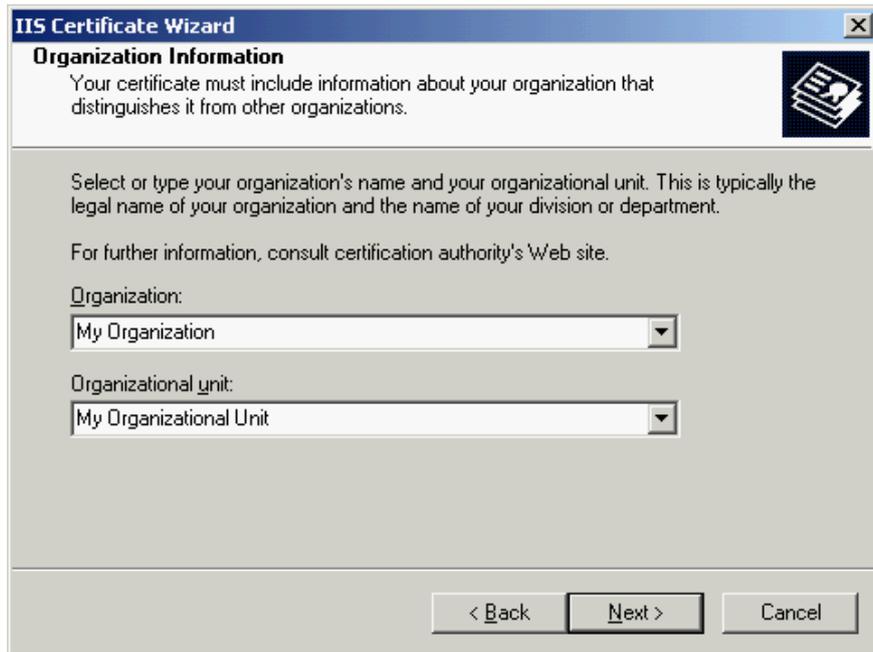


7. Type a name (or accept the default) for the new certificate and choose 2048 for the “Bit length”, and then click “Next”.

*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”.



The screenshot shows the 'IIS Certificate Wizard' dialog box, specifically the 'Organization Information' step. The title bar reads 'IIS Certificate Wizard'. Below the title bar, the text says 'Organization Information' and 'Your certificate must include information about your organization that distinguishes it from other organizations.' There is a small icon of a certificate on the right. The main area contains 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 'For further information, consult certification authority's Web site.' There are two dropdown menus: 'Organization:' with 'My Organization' selected, and 'Organizational unit:' with 'My Organizational Unit' selected. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

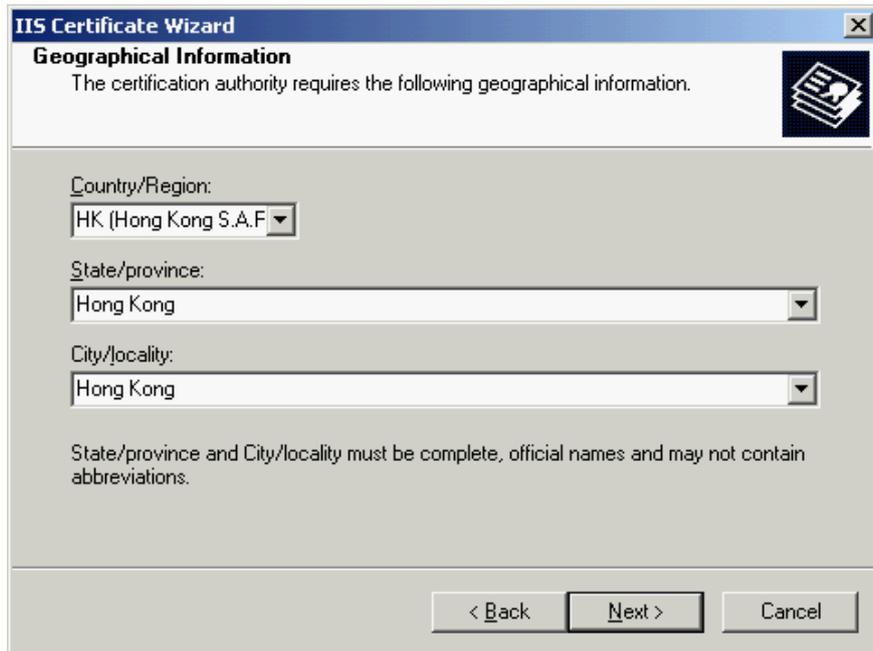
9. Type the common name (i.e. server name) for your site, and then click “Next”.

*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.*

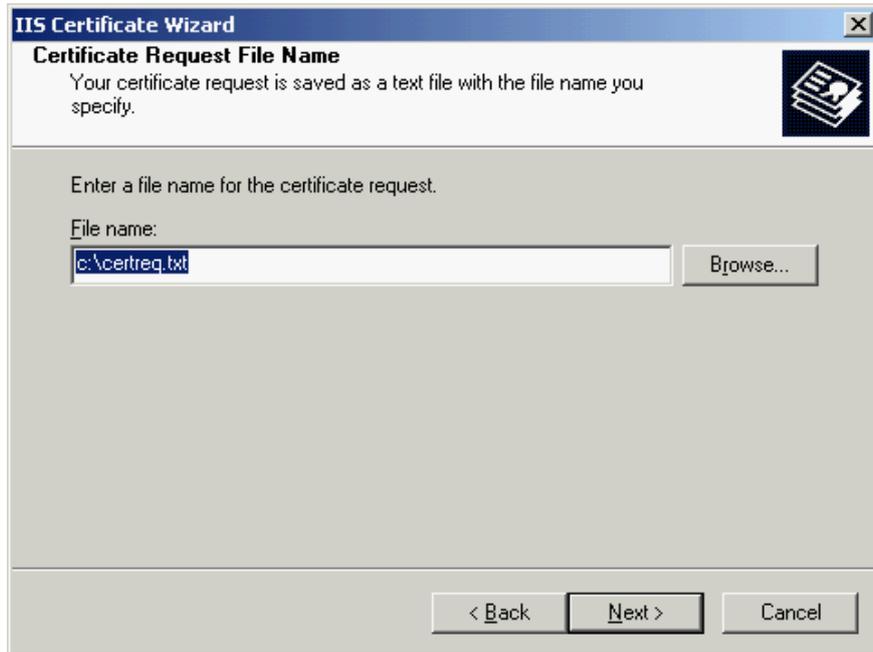
*For application of e-Cert (Server) with "Wildcard" feature, please input the “Common Name” field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk ‘\*’, in the left-most component of the server name), e.g. \*.myserver.com, being filled in the application form.*



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".

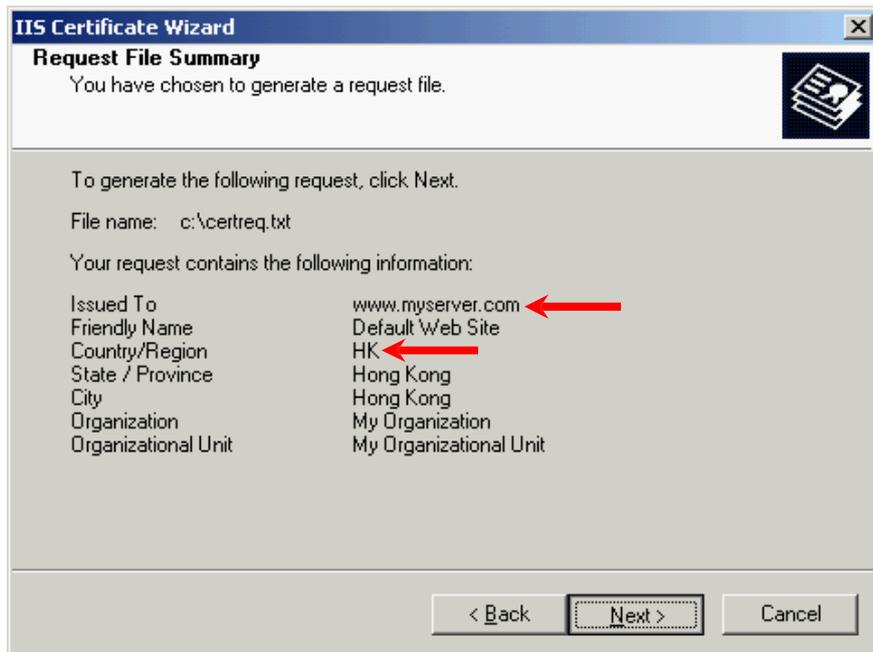


11. Enter a file name for the certificate request, and then click “Next”.



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.

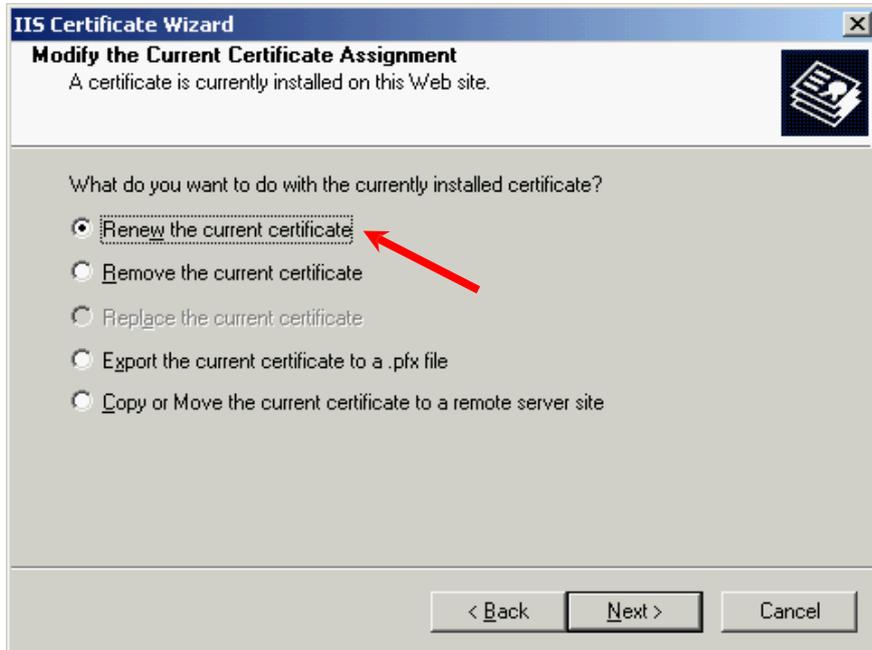


## **Renewing your Current Server Certificate**

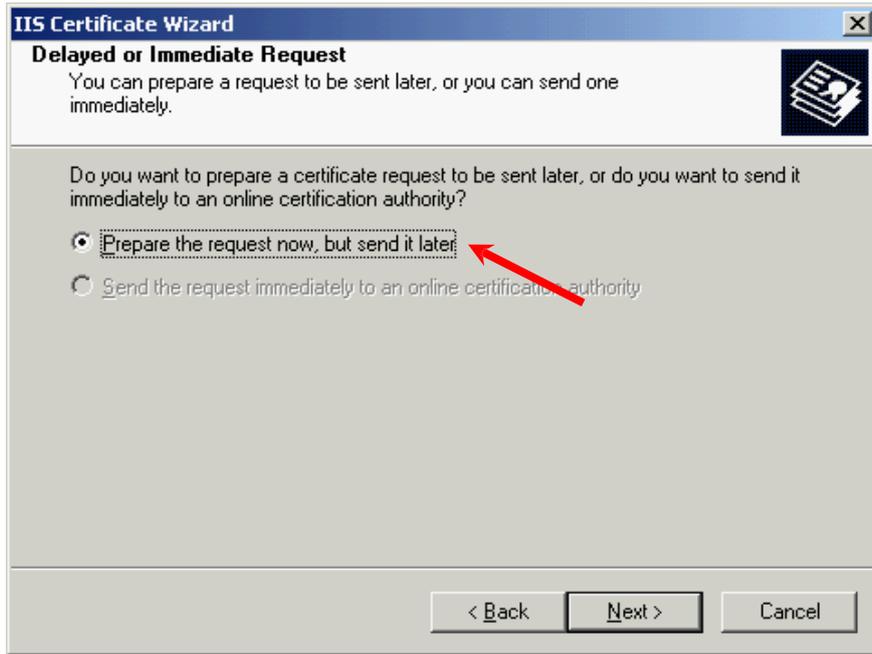
14. In the “Web Server Certificate Wizard”, click “Next” to continue.



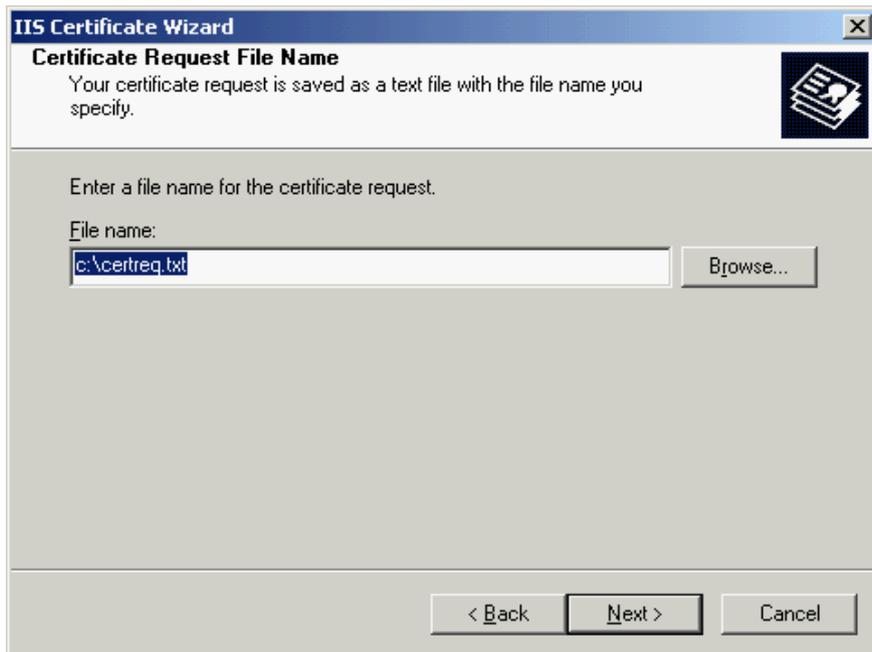
15. Select “Renew the current certificate”, and then click “Next”.



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

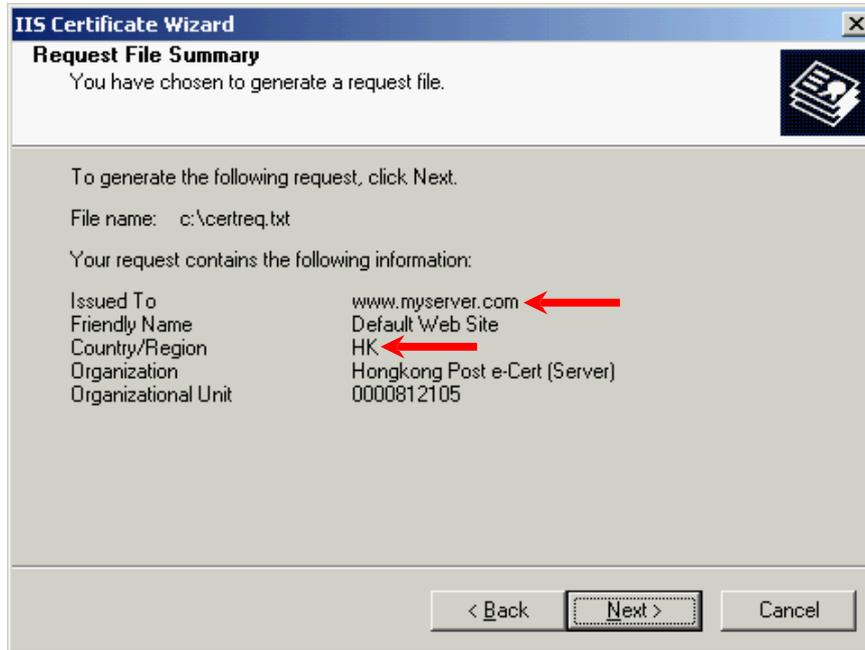


17. Enter a file name for the certificate request, and then click “Next”.



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.*

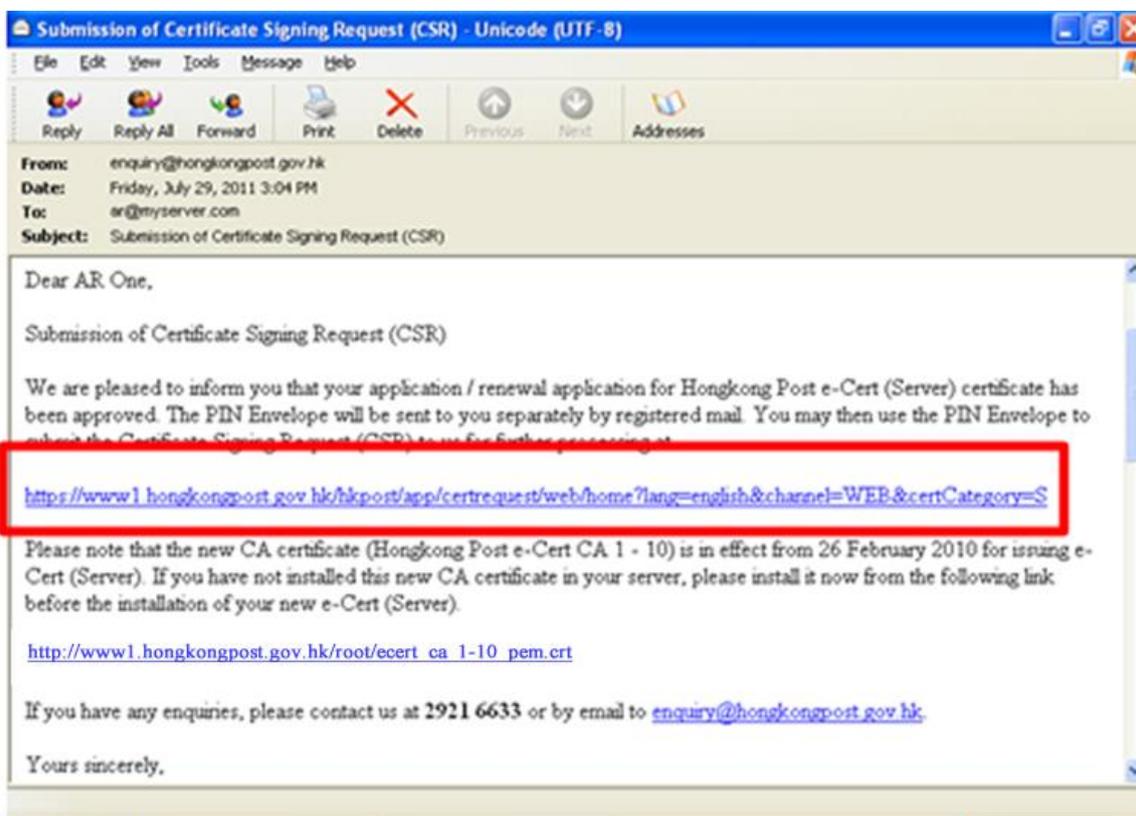


19. Click “Finish” to close the wizard.



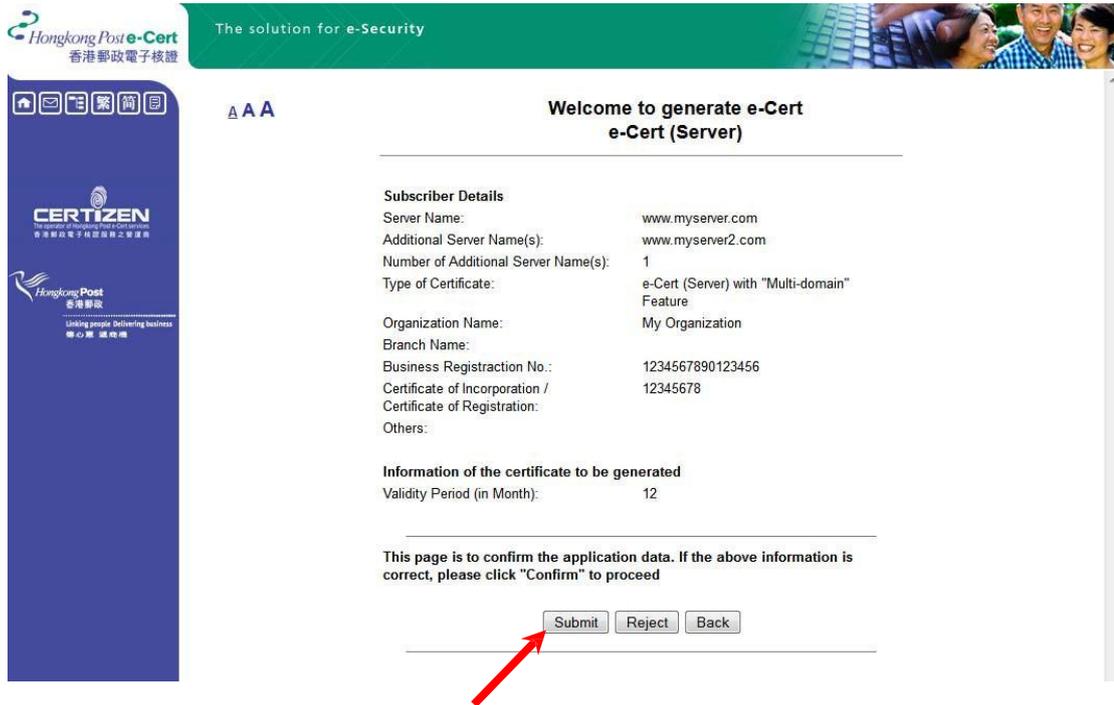
## C. Submitting Certificate Signing Request (CSR)

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”.

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



- 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”.

The screenshot shows the 'Welcome to generate e-Cert e-Cert (Server)' page. It includes a sidebar with the CERTIZEN logo and navigation icons. The main content area contains instructions and a text box with the following text:

Please note that with effect from 1 December 2012, e-Cert (Server) will be issued only with 2048-bit RSA key length. Only Certificate Signing Request (CSR) with 2048-bit RSA key length will be accepted. For details, please refer to the relevant announcement.

Please paste the Certificate Signing Request CSR (base64 encoded PKCS#10) to the following box and press "Submit" to generate certificate.

```

-----BEGIN CERTIFICATE REQUEST-----
MIICuDCCAACAQAwczELMAkGA1UEBhMCSEsxEjAQBgNVBAgTCUhhbmcgS29uZzES
MBAgA1UEBxMj05G9uZy5Lb25nMSEwHwYDVQQKEhhJbnR1cm51dCBXaWRnaXRzIFB0
eSBMdGQxSTAXBgNVBAMTERd3dySteXN1cn21c15jb20wggE1MA0GC5qGS1b3DQEB
AQUAA4IBDwAwggEKAoIBAQDw0zGIFJGKghXdWnuWerAMwdfKLsdJocXzM105zqm/
CTWCQwVT010PJfFHbe+01meIK1N97a9+17KVOLq3GVEwSv/ILg0+1dKW3ReBXsR
LX8+pirXC/e/rwLGA9NVJACjXVS082K02BmzjrgkbtzPVE/h2pppdFyfWnRYht8R
HXcaEmxsuerg/8NEEwFBVMt/pVD1NGCb12k1z88SaDC2FC1c26XjcgUoWke+WGN+
7fIm9XnzIrgKPV6DAX7/TxtsOThXK1PIa61YQRROASm2hascfkwUEcz07peKx2zd
LYwFR1FvezId89EPjYSJ4pJvBnQDF7LEVc3QF18wqf6FAGMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEAS/XNr0mYEcXoRUSPNk01MjkiBhOga78R64pYc3qZ+YJ5av
eQbMgHePvksFRmtaMOz2S1XSbO10gzkaTKzTs7u53pev9VWhRJe+bp2+UHSAOjT
4hNFO+DwubYemZmJPBypbGVWtwjFCMPUGxzXouhhNco2OKKjNnwhhS9rnc3cV
2epNxEtDH1HBP2rJoSTNpW4UA32dxGD/dun1NYf1HUKWTz7j517TinmmMNEg7qv5
n1c/MQ63PxLuGJ7z2pclTVo2pSFuwSzv6XBWxG51Sz7chgLkeqS3pFa+2qhEvsht
    
```

Below the text box is a 'Submit' button, which is highlighted with a red arrow.

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

The screenshot shows the 'Welcome to generate e-Cert e-Cert (Server)' page with the following details:

**The following is the information of this certificate**

<b>Subscriber Details</b>	
Server Name :	www.myserver.com
Additional Server Name(s) :	www.myserver2.com
Organization Name :	My Organization
Branch Name :	
Business Registration No. :	1234567890123456
Certificate of Incorporation / Certificate of Registration :	12345678
Others :	

**The following is the system generated information**

Subscriber Reference Number :	0000821069
e-Cert Type :	Hongkong Post e-Cert (Server)
Issued by :	Hongkong Post e-Cert CA 1 - 10
e-Cert Serial No. :	2E4594
e-Cert Validity Period :	27/04/2013 to 27/04/2014

Please click "Accept" to confirm acceptance of this certificate. Otherwise, please click "Reject" and state the reasons for rejecting the certificate.

(Note : Your personal data collected by Hongkong Post will be used for processing your e-Cert application. You have the right of access and correction with respect to personal data as provided for in the Personal Data (Privacy) Ordinance.)

At the bottom, there are three buttons: 'Accept', 'Reject', and 'Cancel'. A red arrow points to the 'Accept' button.

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.*

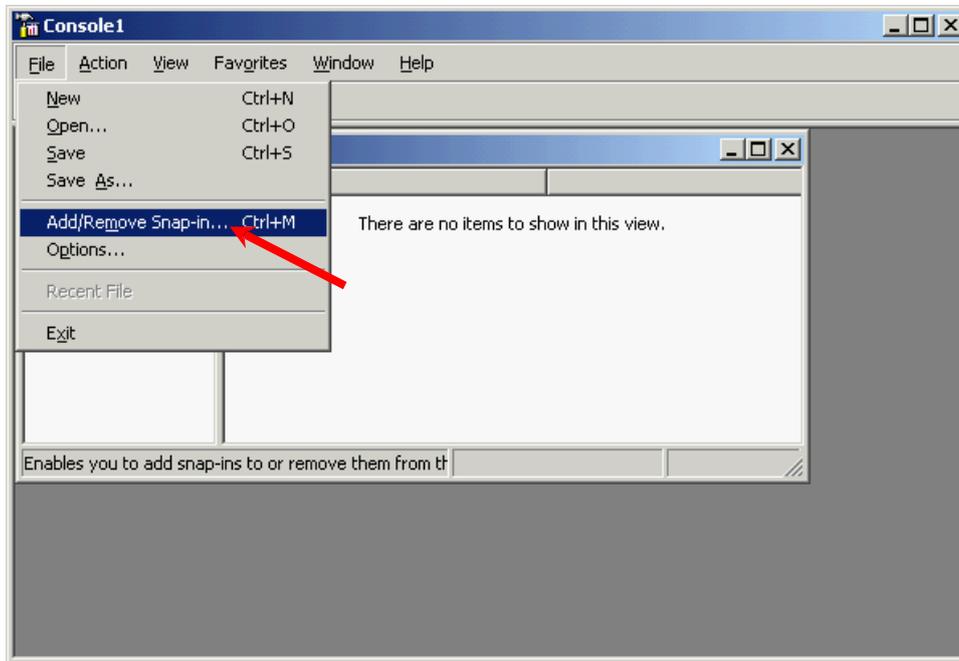
<http://www.hongkongpost.gov.hk/en/sc>

*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.*

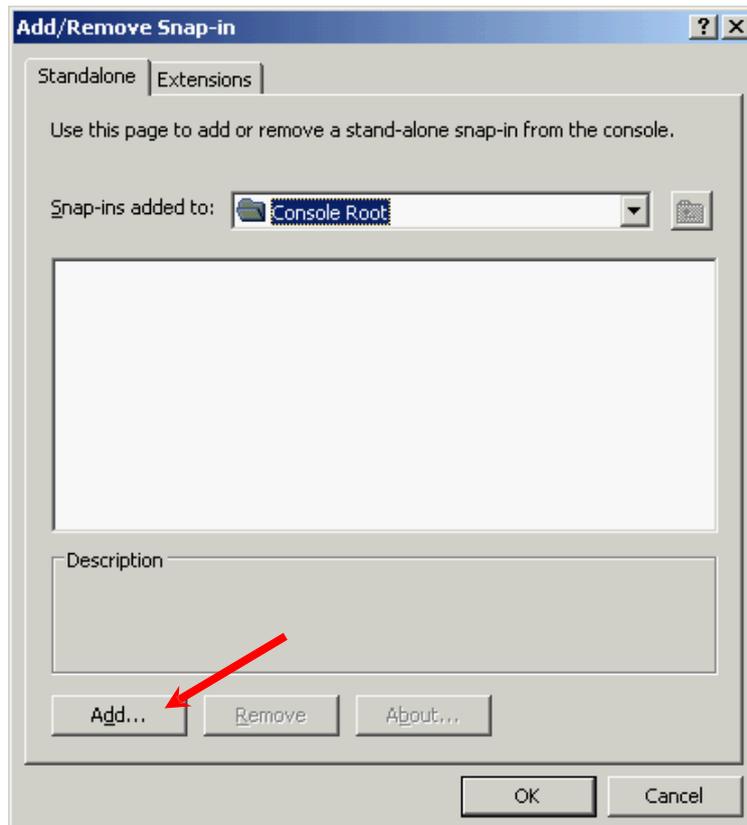
The screenshot shows the Hongkong Post e-Cert (Server) generation interface. The header includes the Hongkong Post e-Cert logo and the tagline 'The solution for e-Security'. The main heading is 'Welcome to generate e-Cert e-Cert (Server)'. A red box highlights the 'You may now:-' section, which lists three items: 'Download the “Hongkong Post e-Cert (Server)” certificate', 'Download the “Hongkong Post e-Cert CA 1 - 10” certificate', and 'Download the “Hongkong Post Root CA 1” certificate'. Below this, a note states: 'Please note that the new CA certificate (Hongkong Post e-Cert CA 1 - 10) is in effect from 26 February 2010 for issuing e-Cert (Server). If you have not installed this new CA certificate in your server, please install it now before the installation of your new e-Cert (Server)'. The page footer includes '2007 © | Important Notices | Privacy Policy'.

## D. Installing Hongkong Post Root CA Certificate

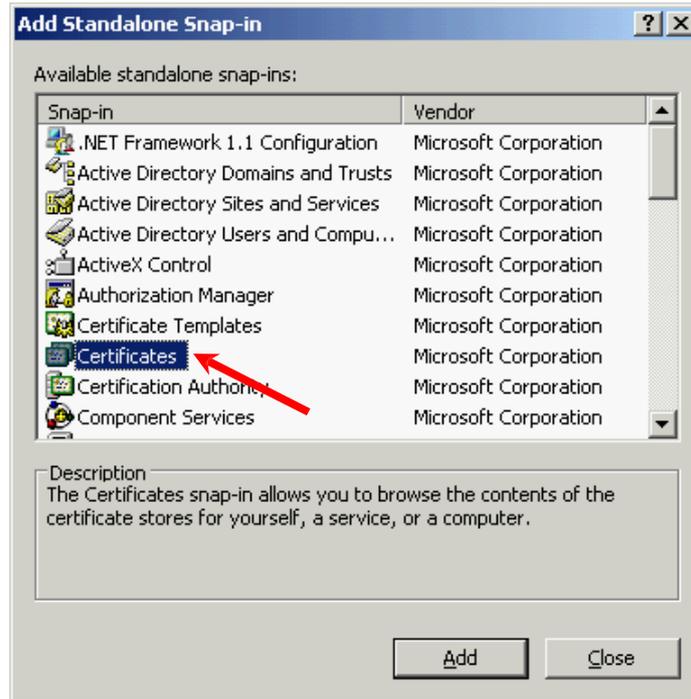
1. Start Microsoft Management Console (MMC) by clicking “Start” > “Run”, type “mmc” and click OK, and then select “Add/Remove Snap-in” from the “File” / “Console” menu.



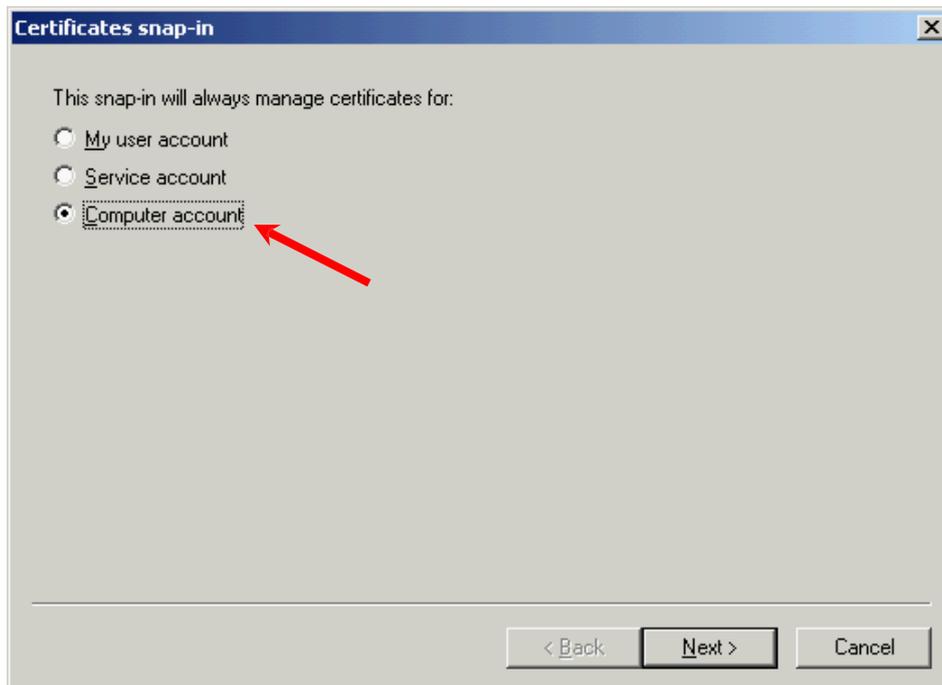
2. Click “Add”.



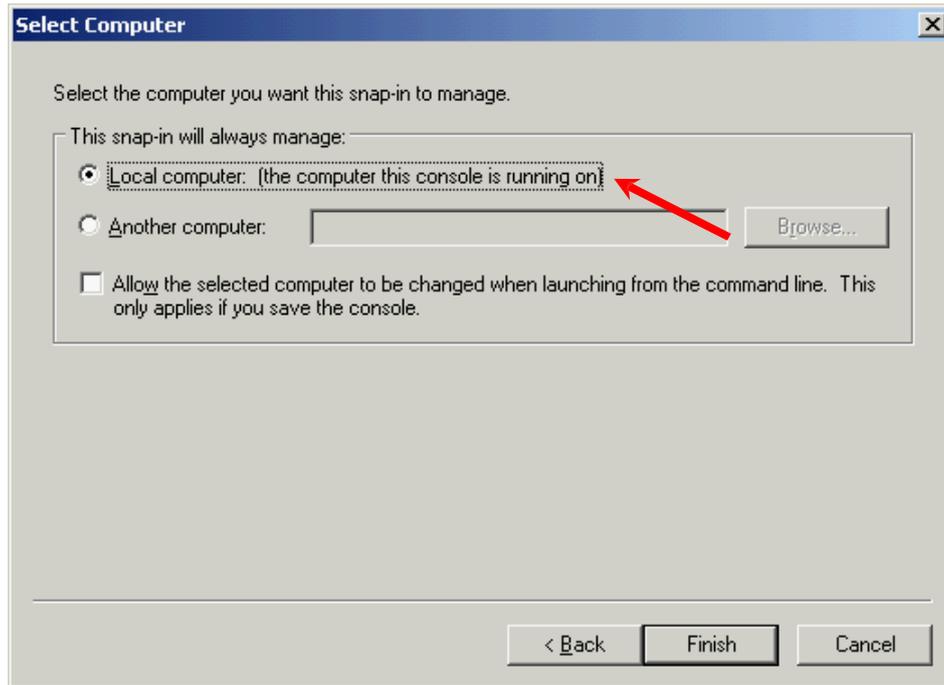
3. Select “Certificates”, and then click “Add”.



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



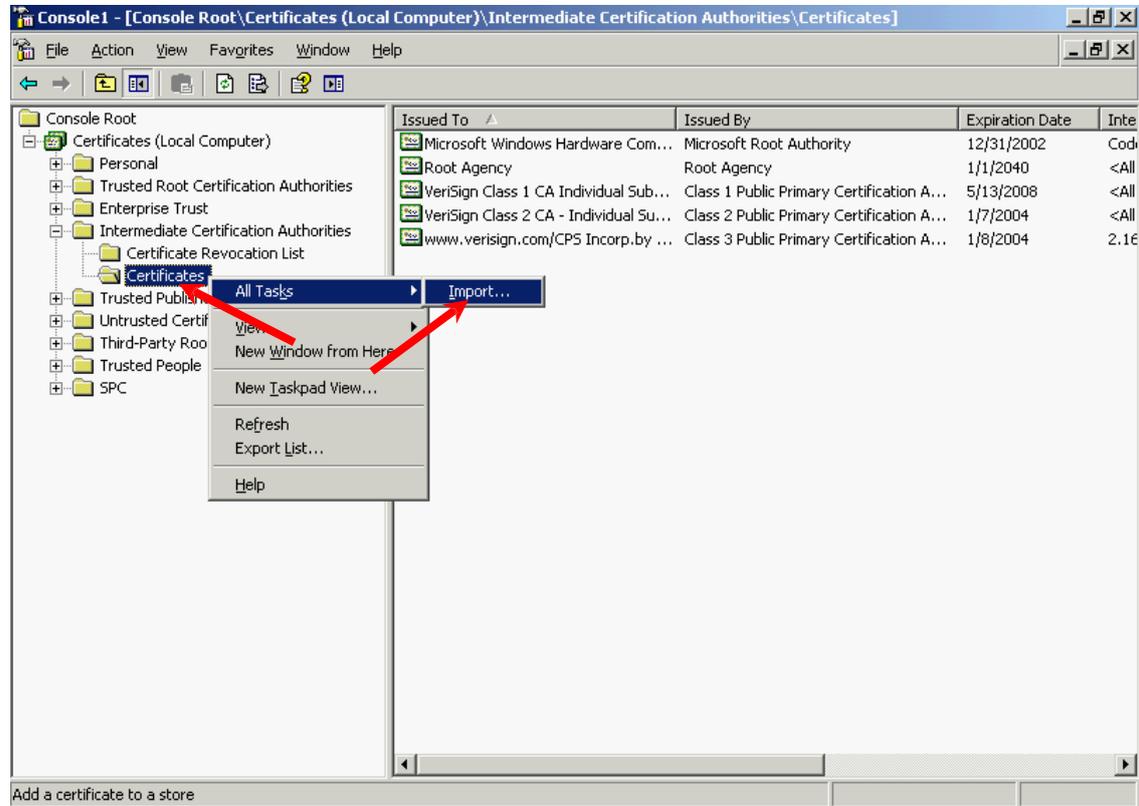
5. Select “Local computer”, and then click “Finish”.



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**

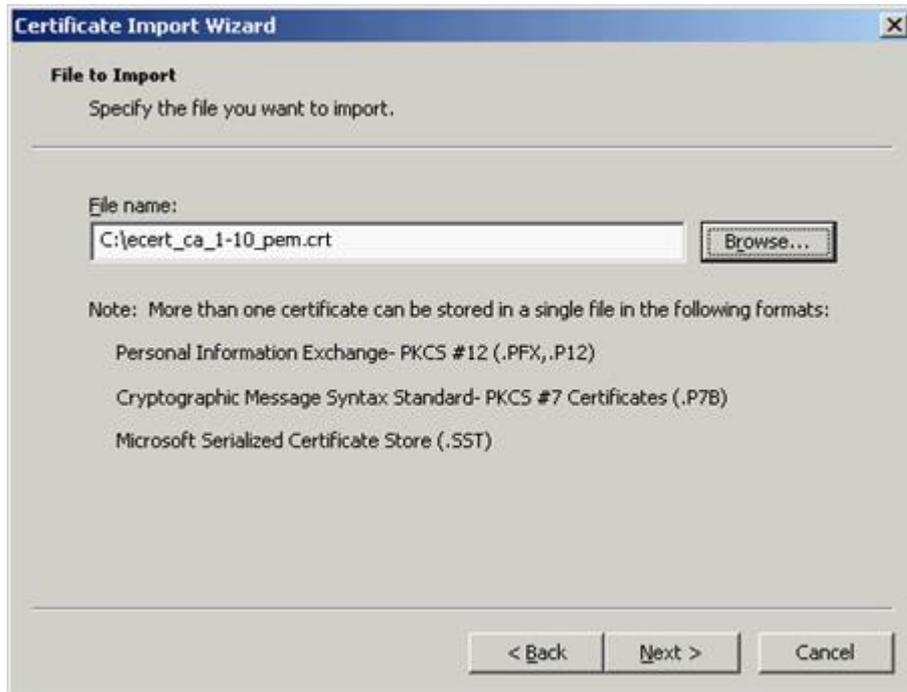
- Expand “Intermediate Certification Authorities” and right-click “Certificates”, and then select “All Tasks” > “Import”.



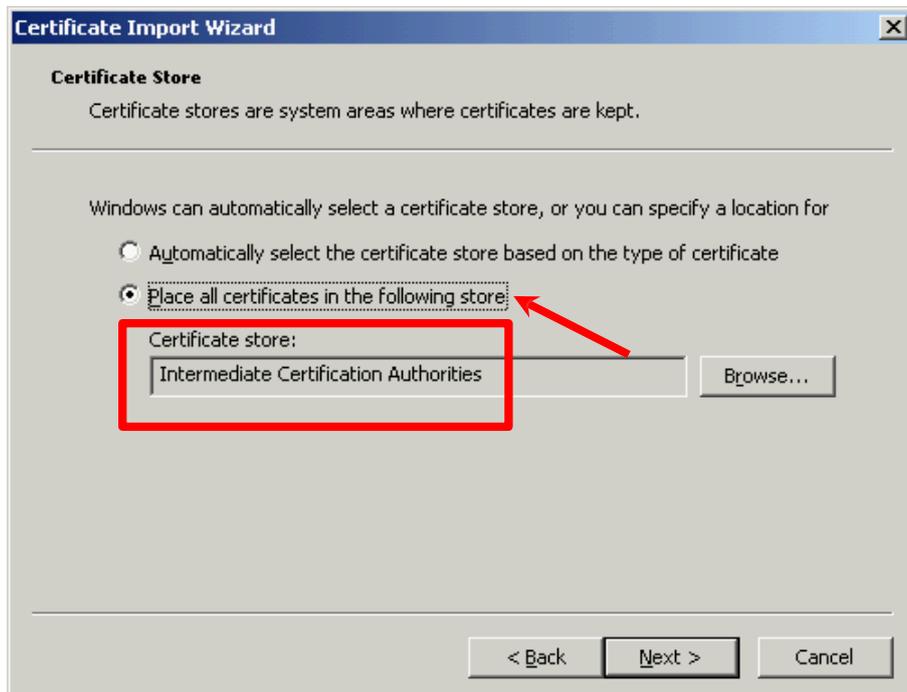
- In the “Certificate Import Wizard”, click “Next” to continue.



- 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”.



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



11. Click “Finish” to close the wizard.



12. Click “OK” to complete.

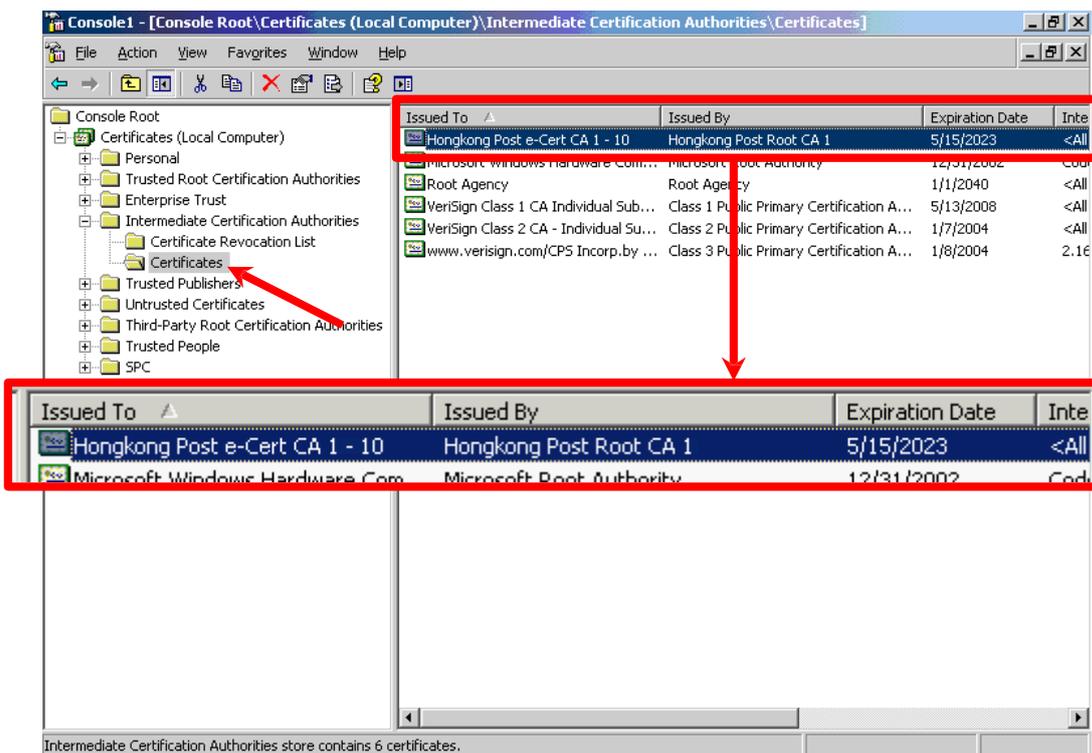
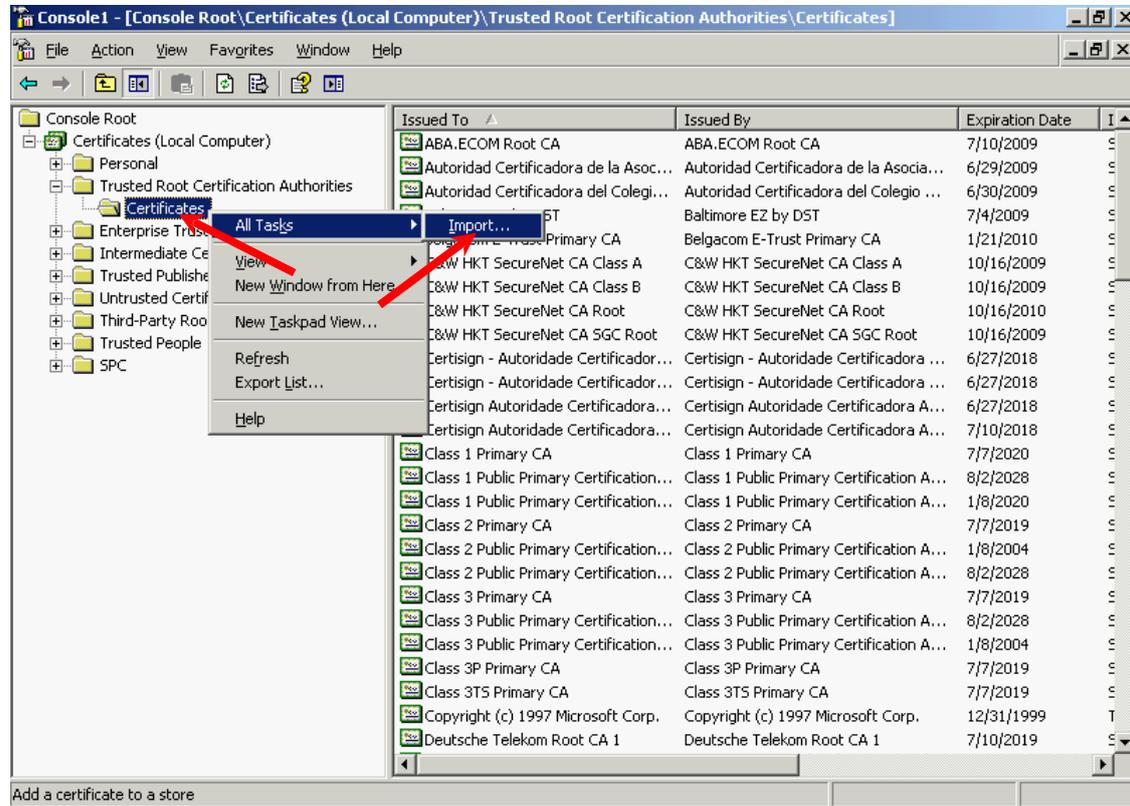


Figure 1: “Hongkong Post e-Cert CA 1 - 10” certificate has been successfully installed

## **Installing the “Hongkong Post Root CA 1” Certificate**

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



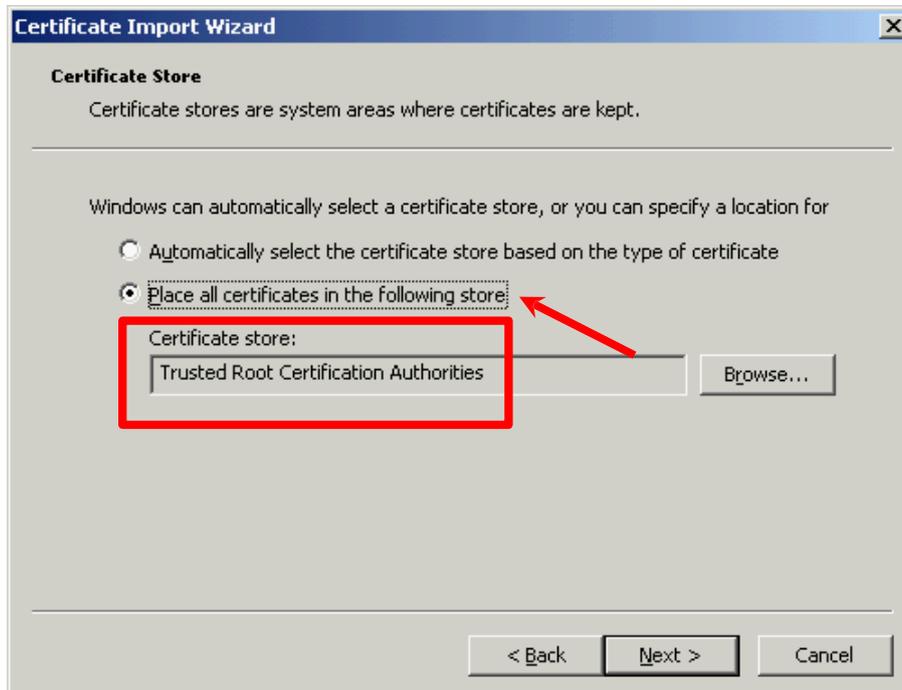
- In the “Certificate Import Wizard”, click “Next” to continue.



- 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”.



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



17. Click “Finish” to close the wizard.



18. Click “OK” to complete.

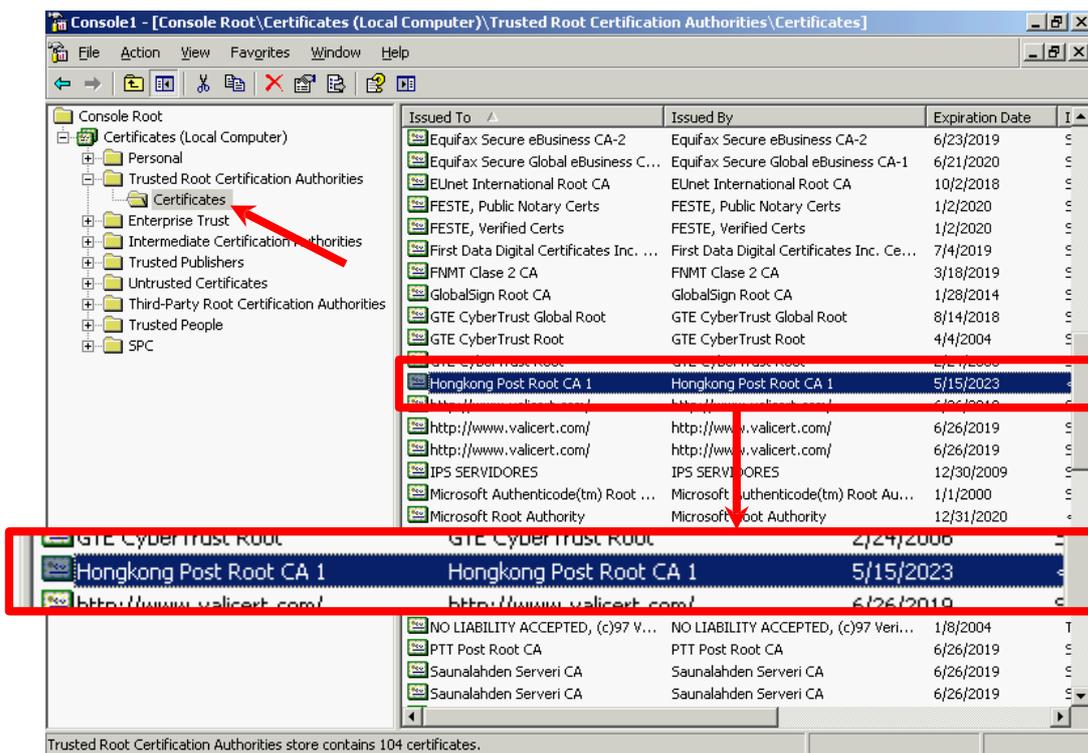
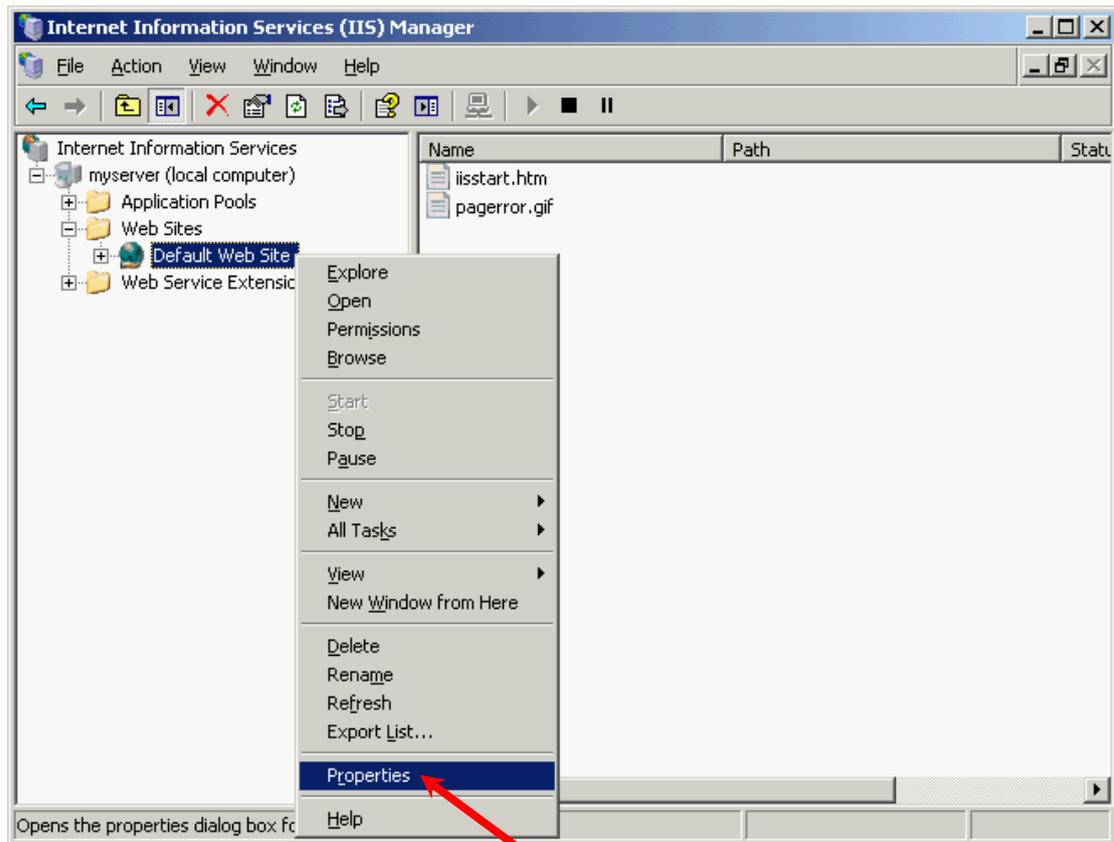


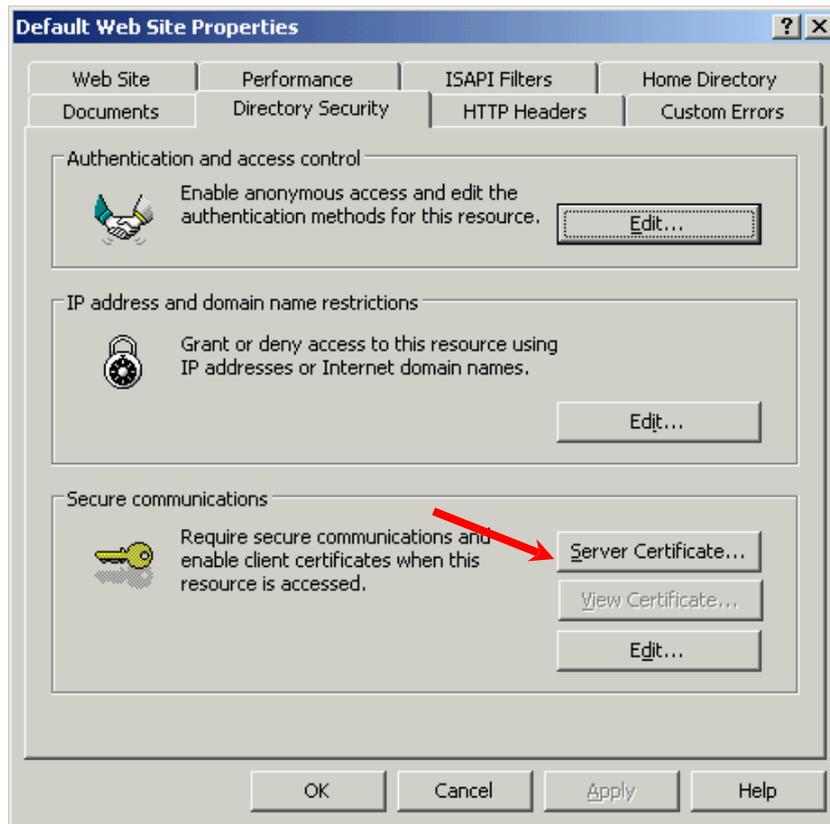
Figure 2: “Hongkong Post Root CA 1” certificate has been successfully installed

## 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”.



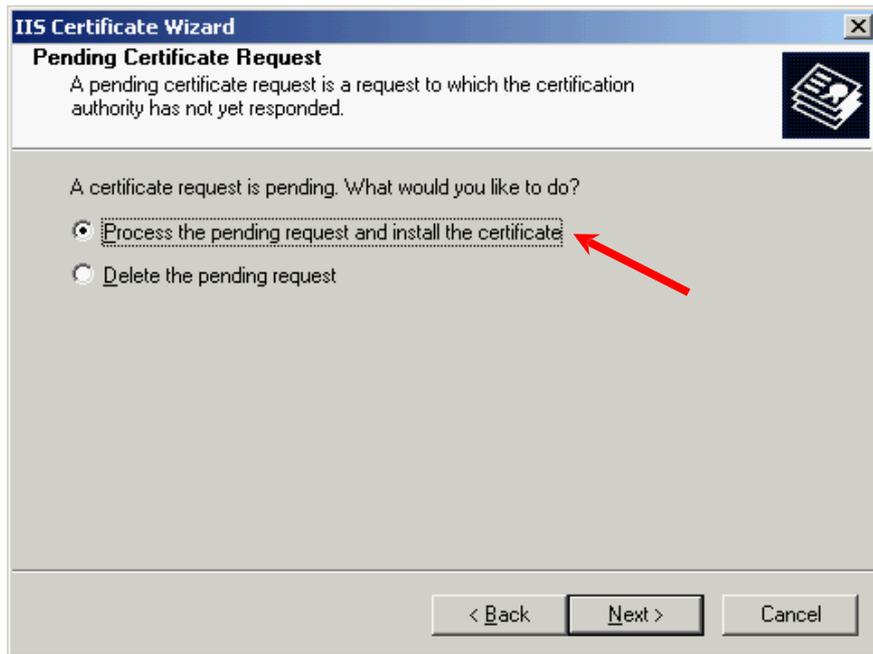
3. In the “Directory Security” tab, Click “Server Certificate”.



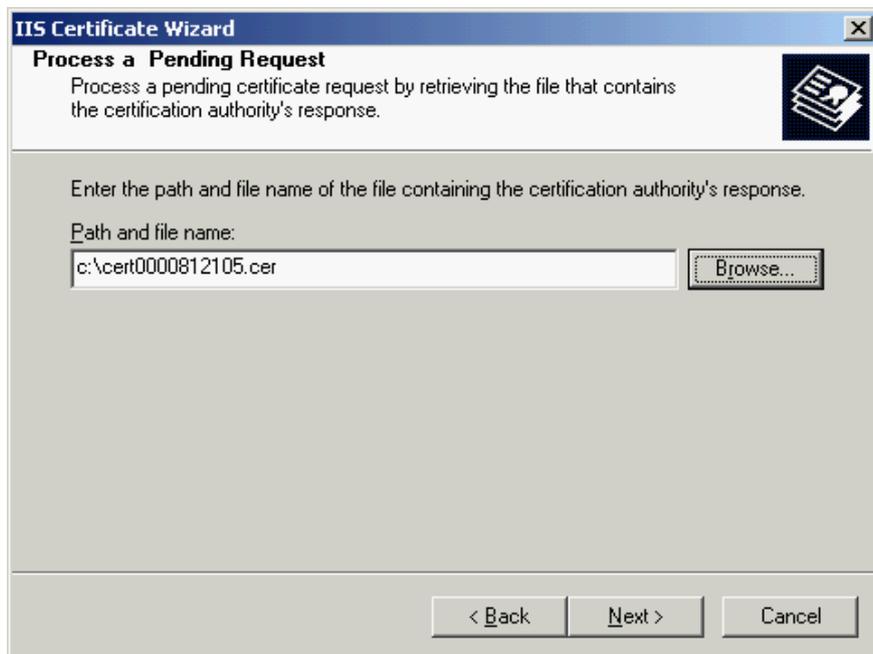
4. In the “Web Server Certificate Wizard”, click “Next” to continue.



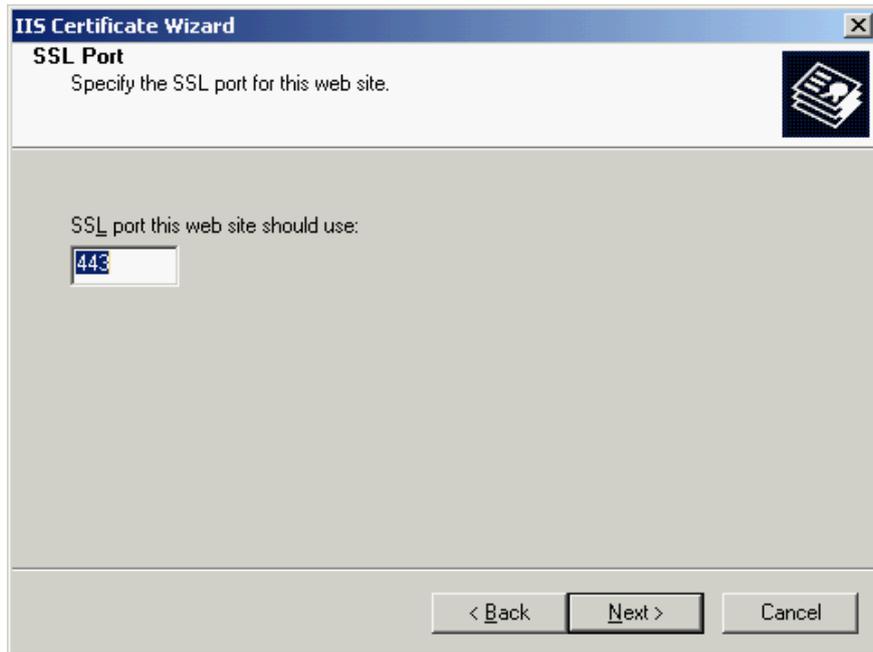
5. Select “Process the pending request and install the certificate”, and then click “Next”.



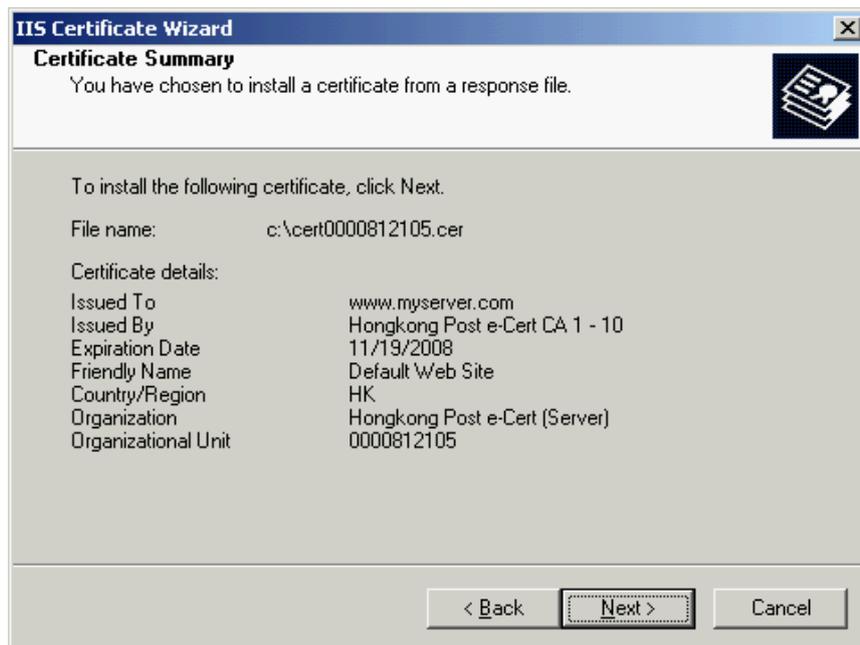
6. Click “Browse” to locate the “Hongkong Post e-Cert (Server)” certificate that you downloaded in Part C Step 7, and then click “Next”.



- 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)



- Click “Next”.



9. Click “Finish” to close the wizard.



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

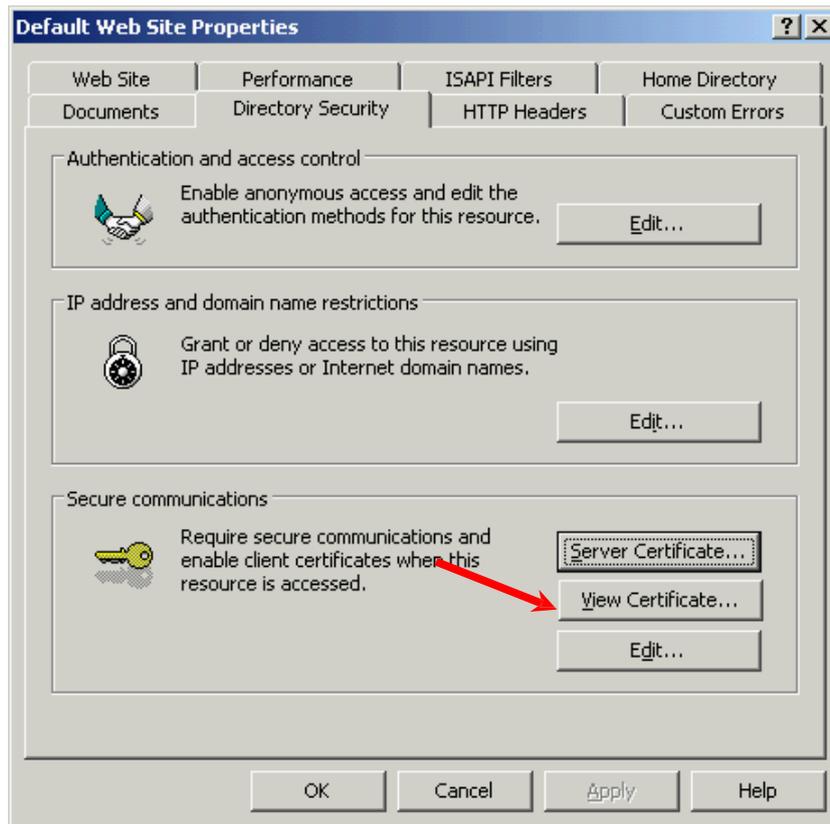
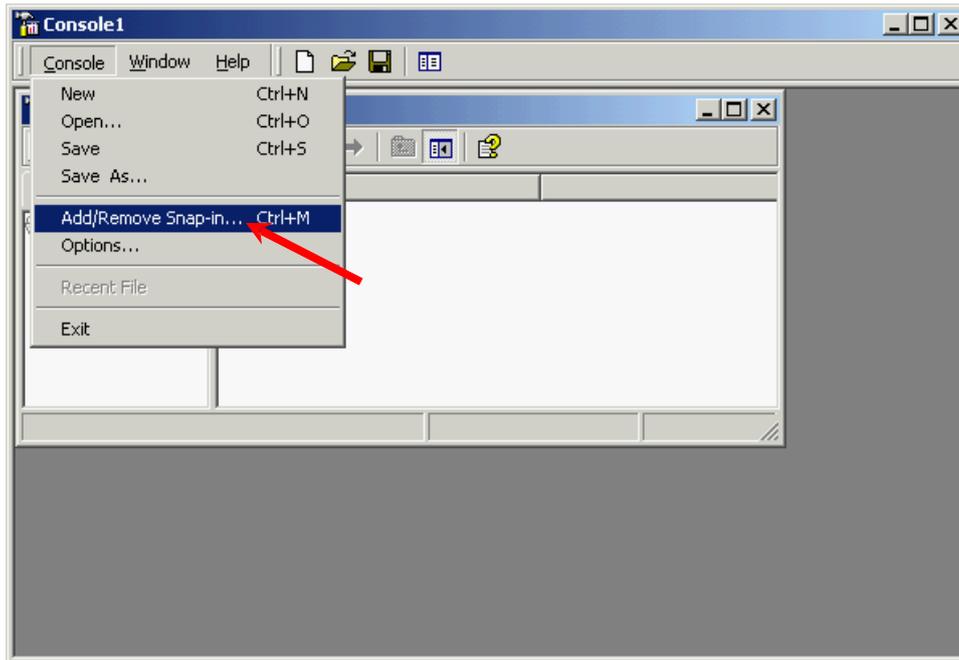


Figure 3: “Hongkong Post e-Cert (Server)” certificate has been successfully installed

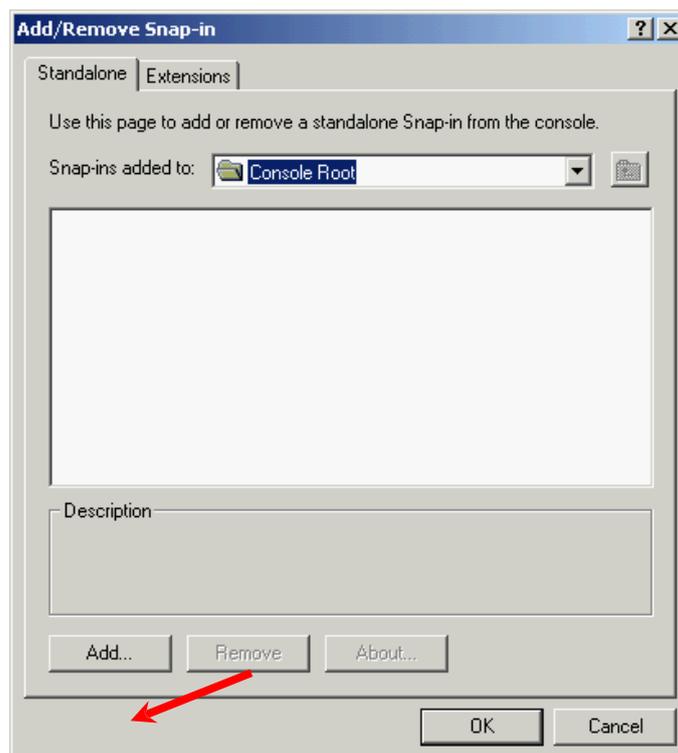
## F. Backing up the Private Key

### Backing up the Private Key for IIS 5.0

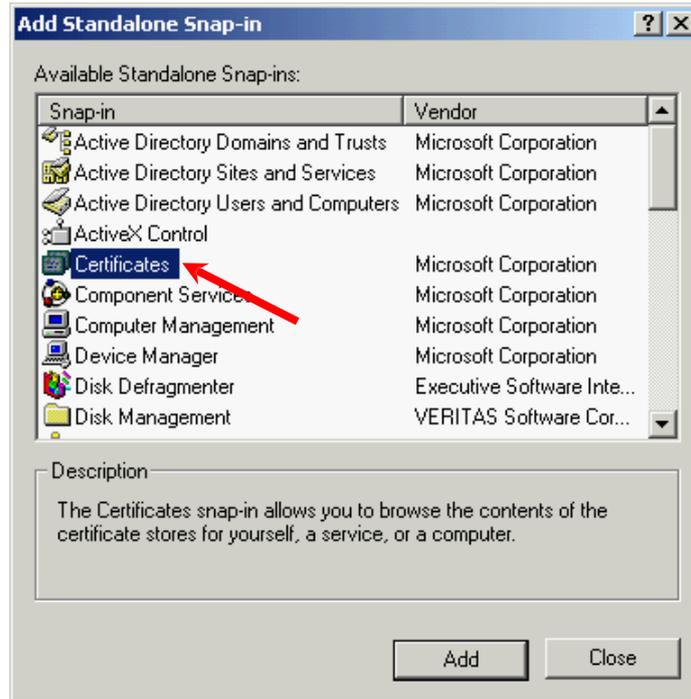
1. Start Microsoft Management Console (MMC) by clicking “Start” > “Run”, type “mmc” and click OK, and then select “Add/Remove Snap-in” from the “Console” menu.



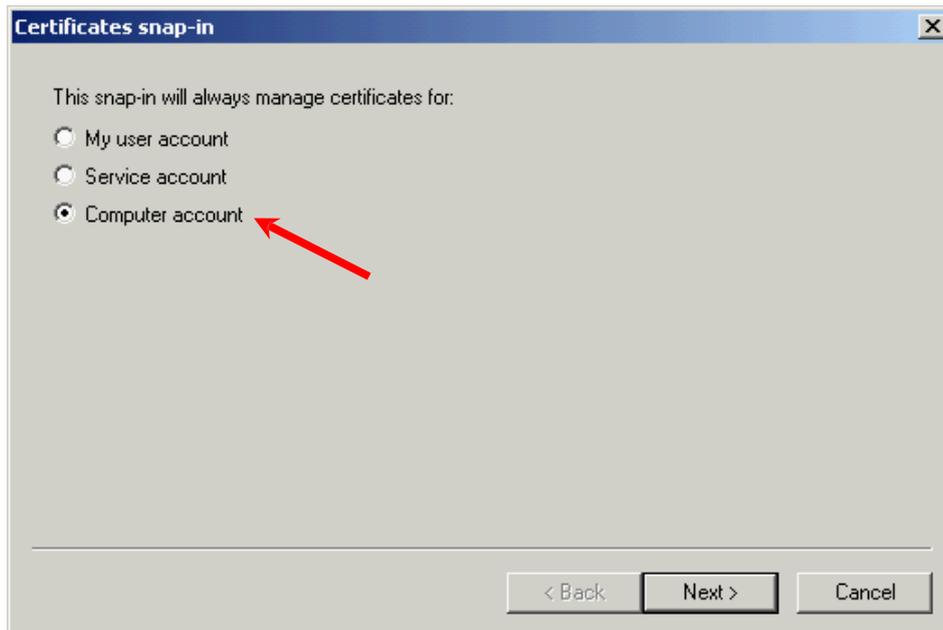
2. Click “Add”.



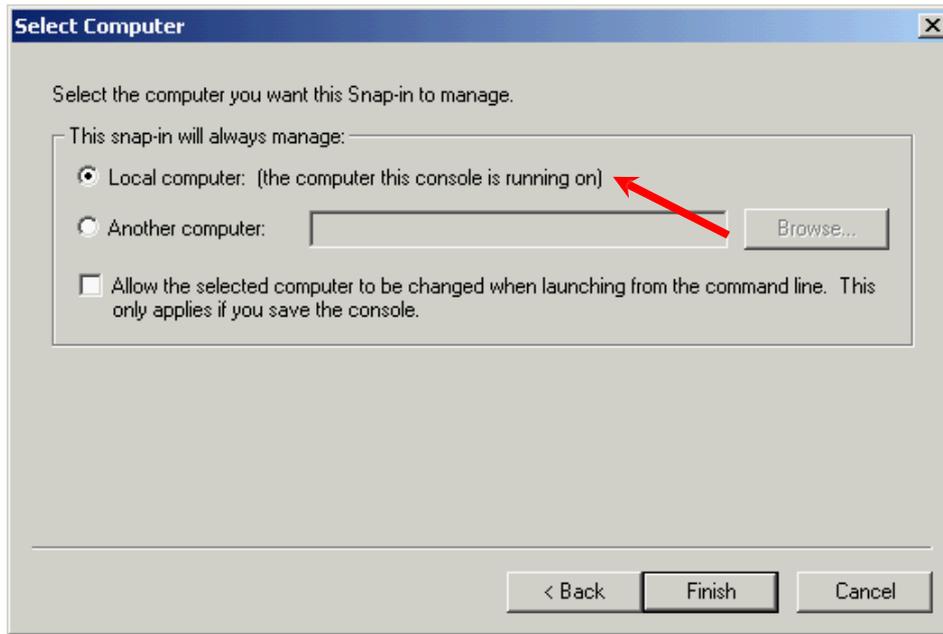
3. Select “Certificates”, and then click “Add”.



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

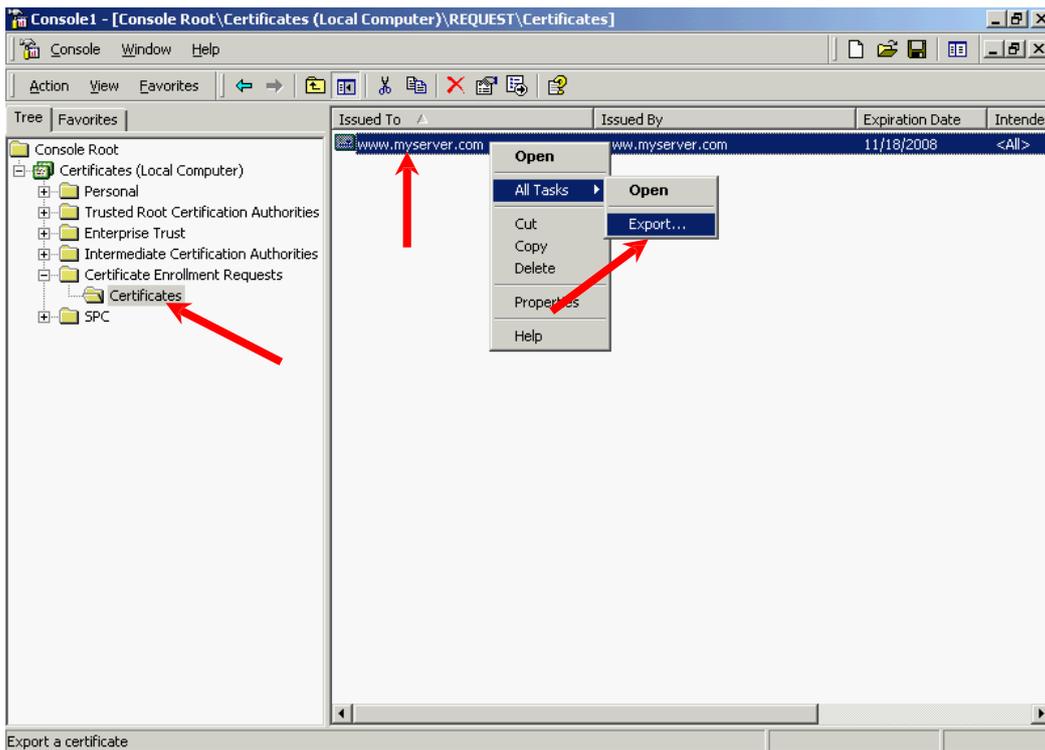


5. Select “Local computer”, and then click “Finish”.

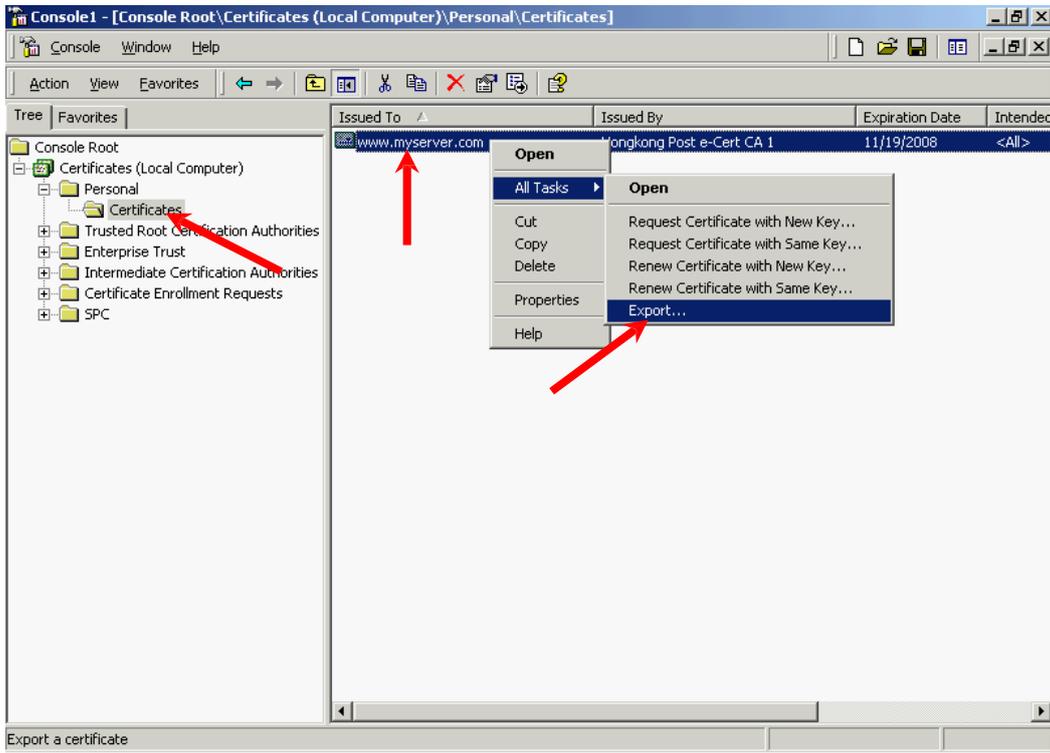


6. Close the “Add Standalone Snap-in” dialog box, and then click “OK” to close the “Add/Remove Snap-in” dialog box.

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”.



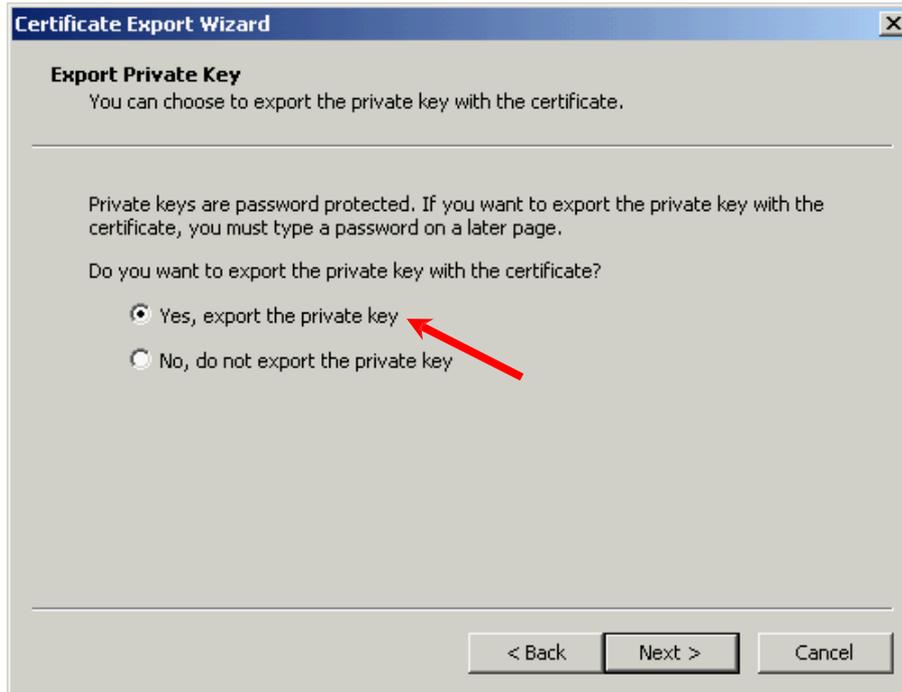
- To backup the private key of an existing certificate, expand “Personal” and select “Certificates”, select the certificate that you would like to make a backup, right-click and then select “All Tasks” > “Export”.



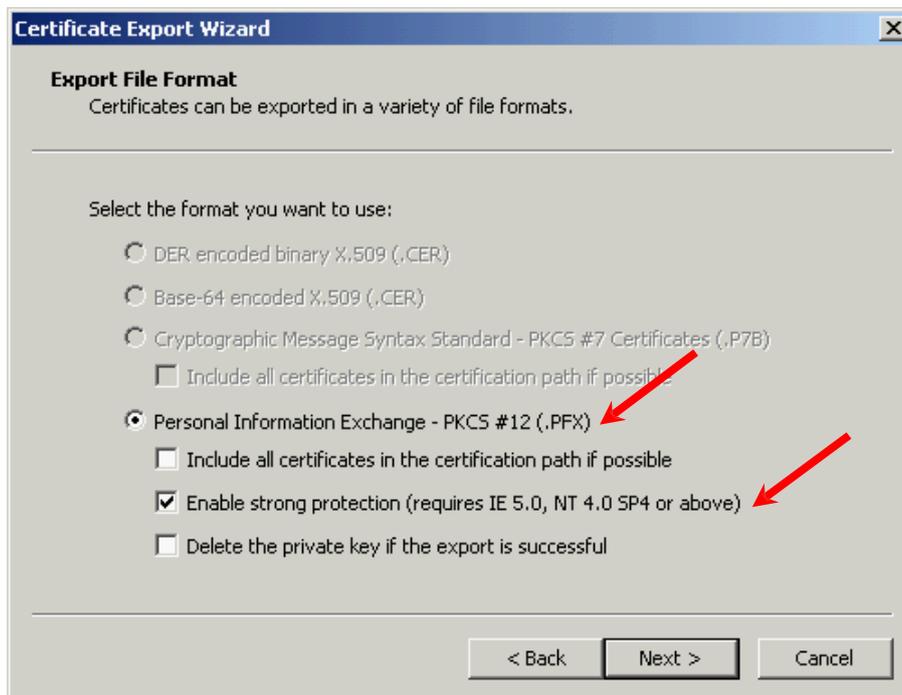
8. In the “Certificate Export Wizard”, click “Next” to continue.



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.

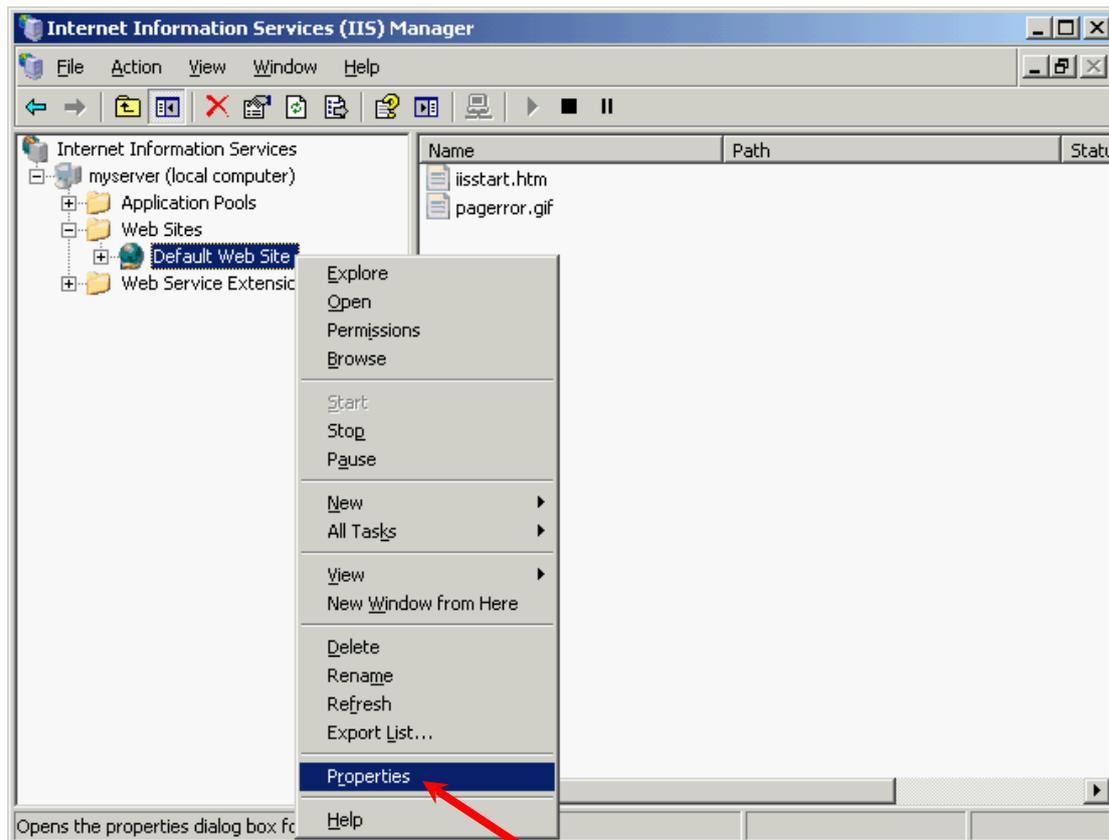


14. Click “OK” to complete.

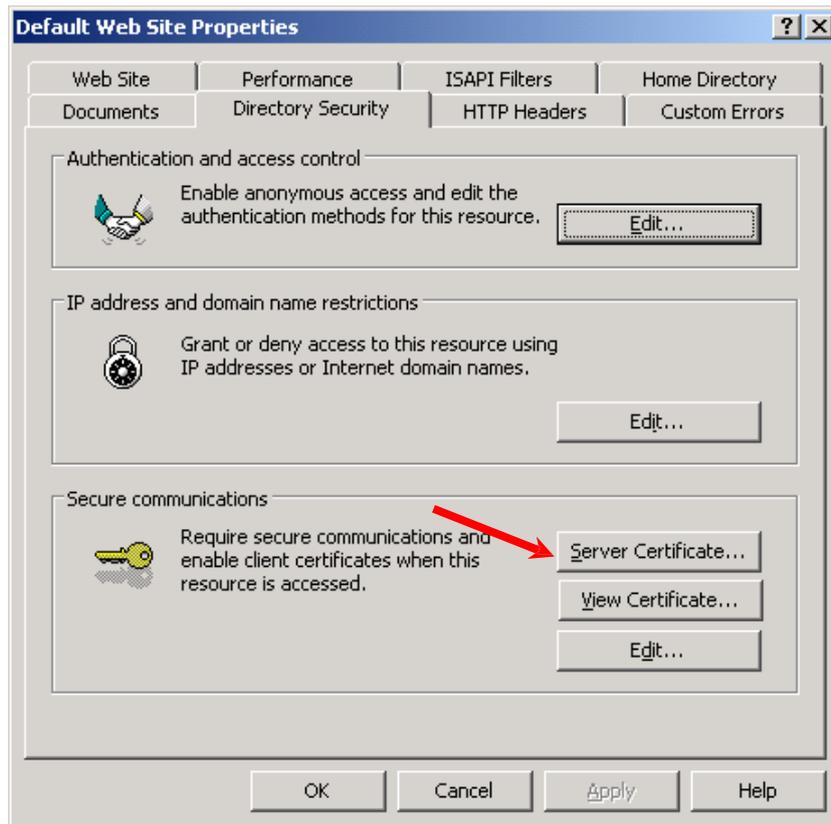


## **Backing up the Private Key for IIS 6.0**

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”.



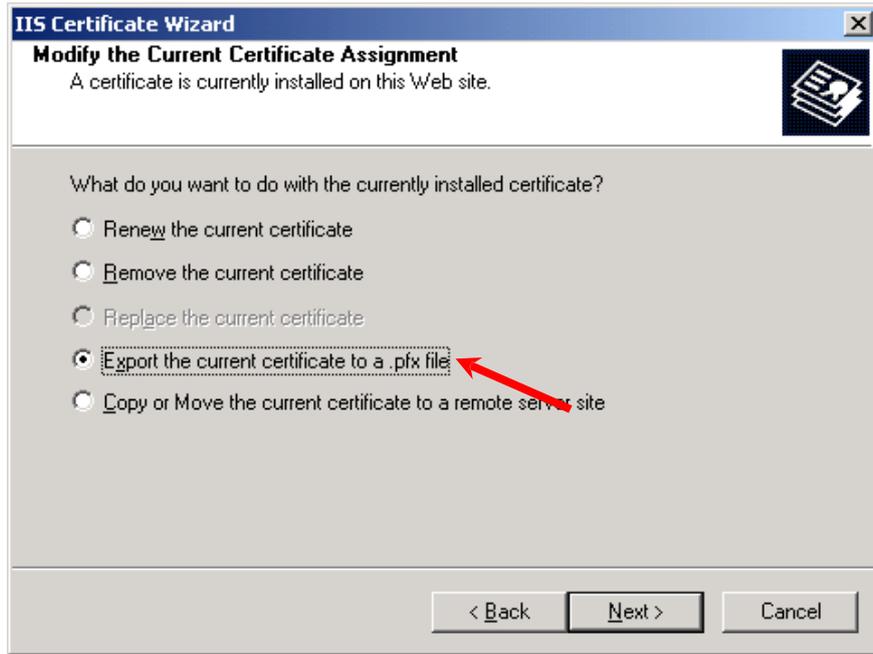
3. In the “Directory Security” tab, click “Server Certificate”.



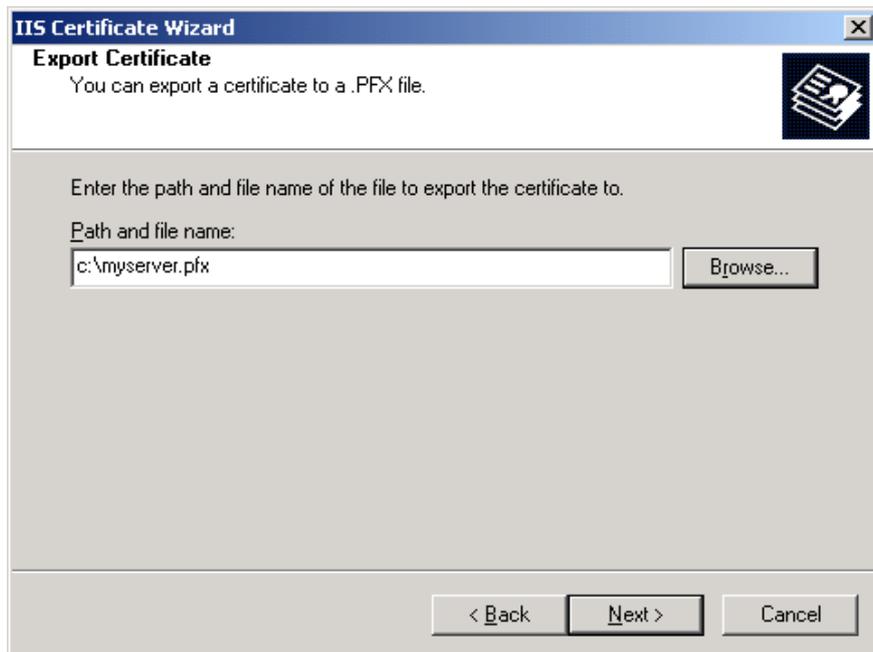
4. In the “Web Server Certificate Wizard”, click “Next” to continue.



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

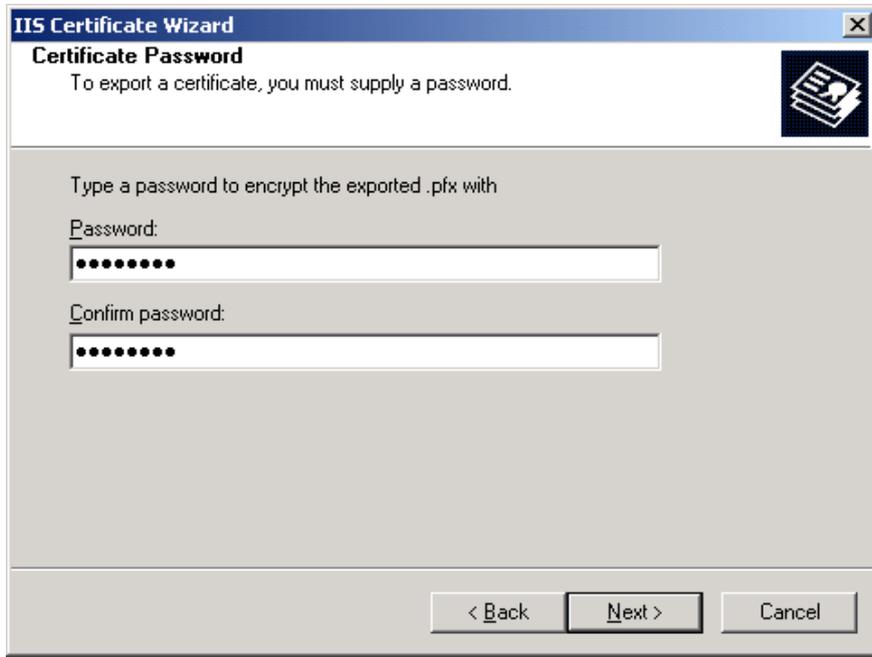


6. Enter the path and file name of the file to export the certificate to, and then click “Next”.

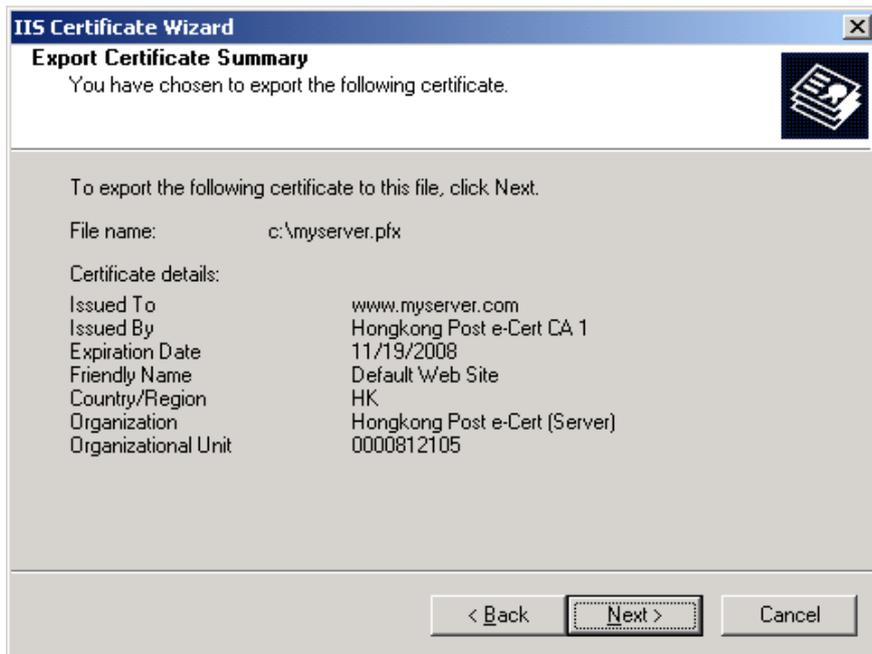


7. Type and confirm a password to encrypt the exported .pfx with, and then click “Next”.

*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”.



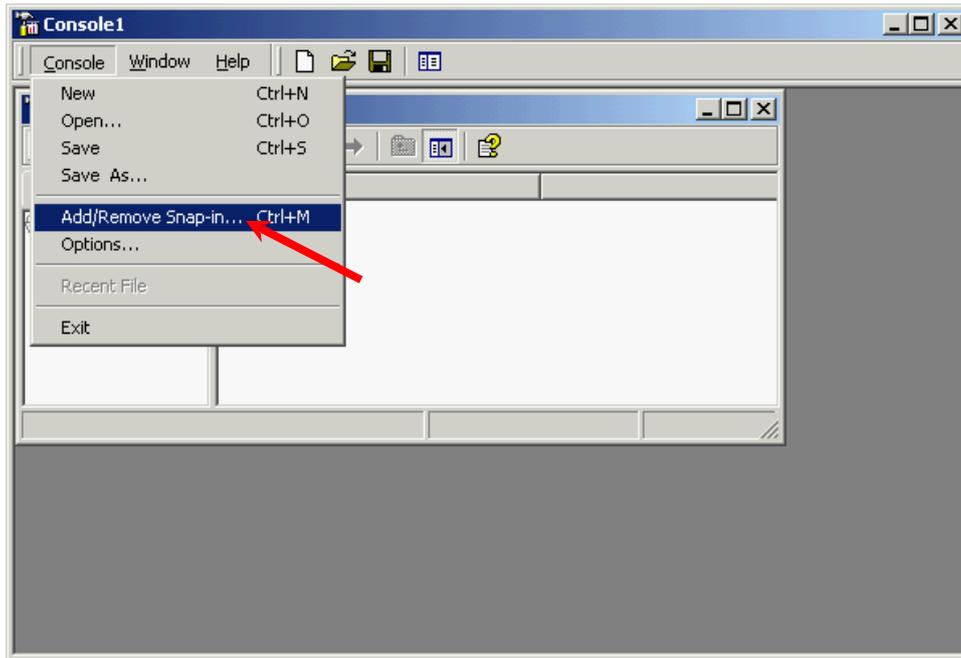
9. Click “Finish” to close the wizard.



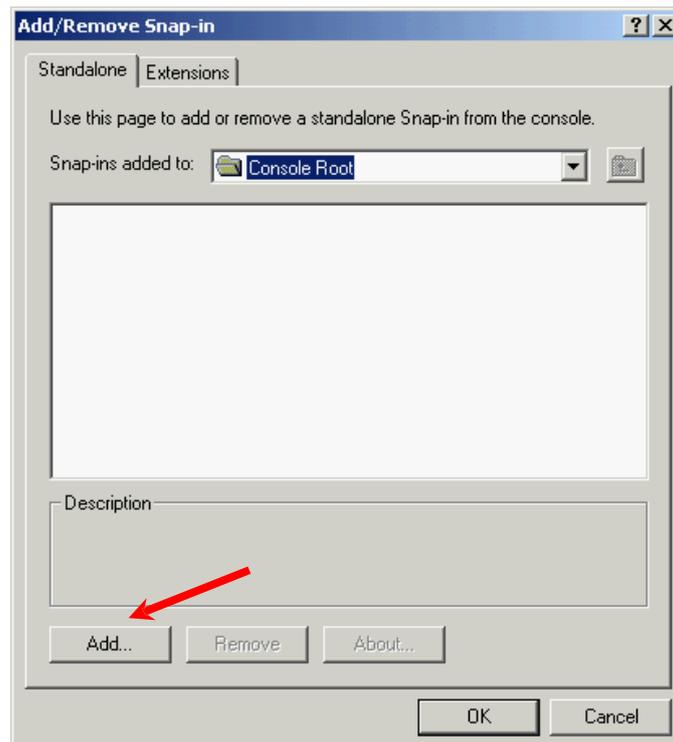
## G. Restoring the Private Key

### 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.



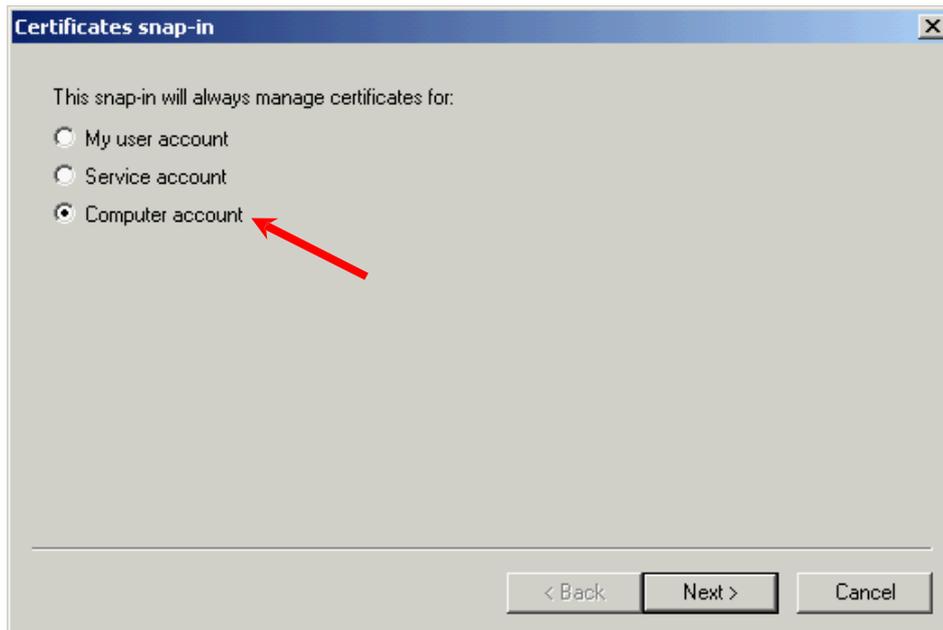
2. Click “Add”.



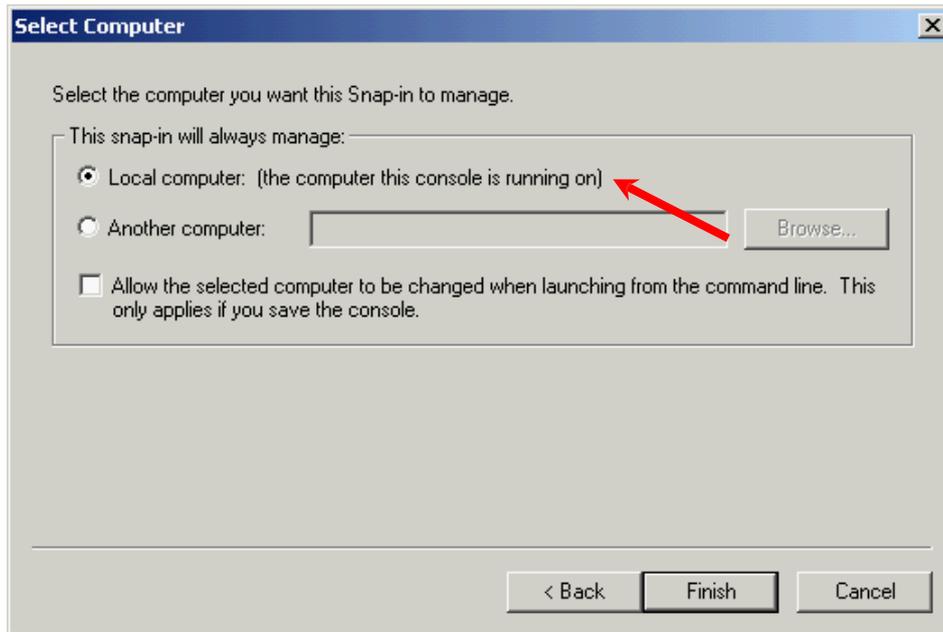
3. Select “Certificates”, and then click “Add”.



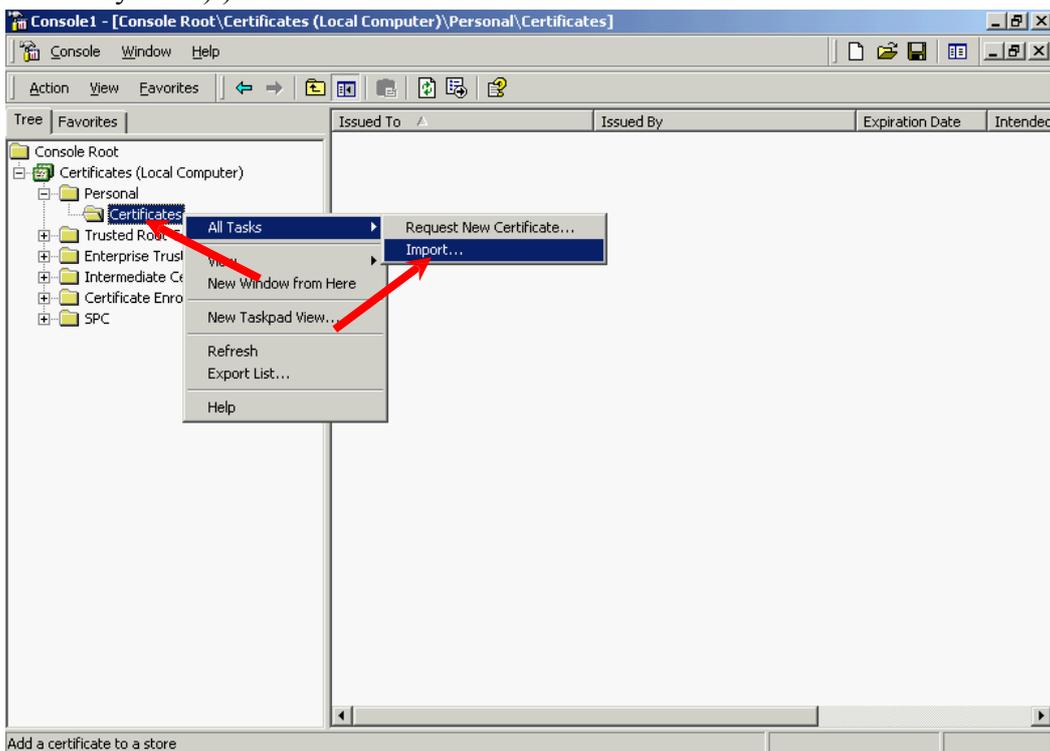
4. Select “Computer account”, and then click “Next”.



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



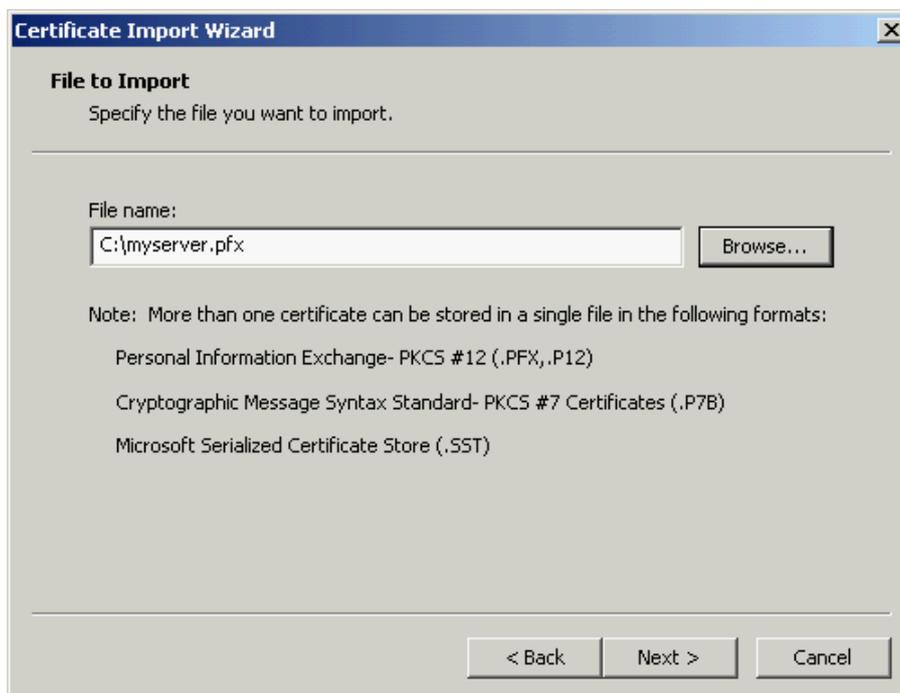
6. Close the “Add Standalone Snap-in” dialog box, and then click “OK” to close the “Add/Remove Snap-in” dialog box.
7. Expand “Personal” and select “Certificates”, right-click and then select “All Tasks” > “Import”. (To restore the private key of a pending request, expand “Certificate Enrollment Requests” (or named “REQUESTS” in some systems).)



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

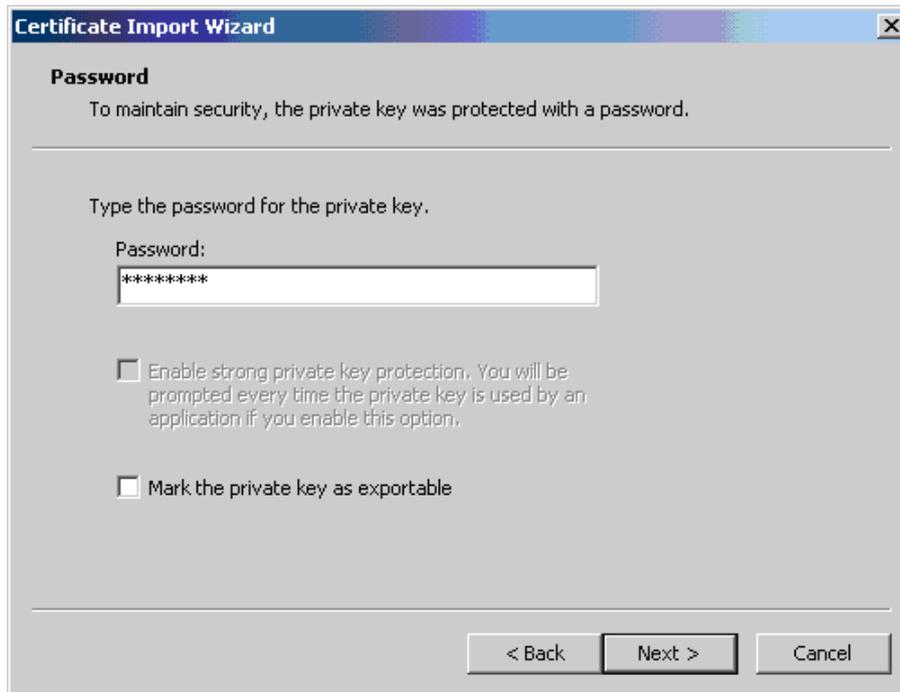


9. Click “Browse” to locate the backup file of your private key, and then click “Next”.

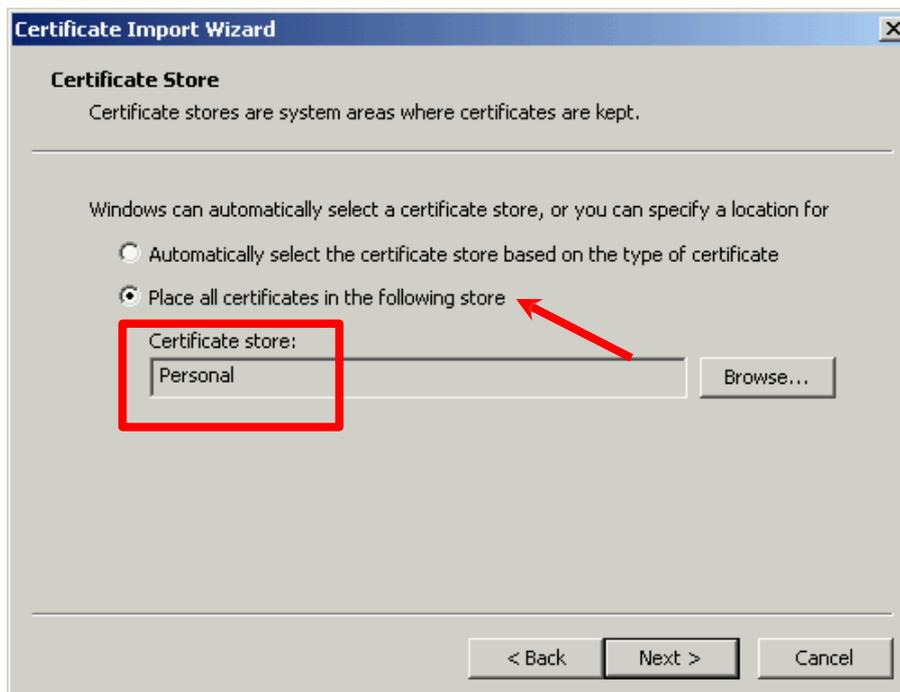


10. Type the password for the private key and then click “Next”.

*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.

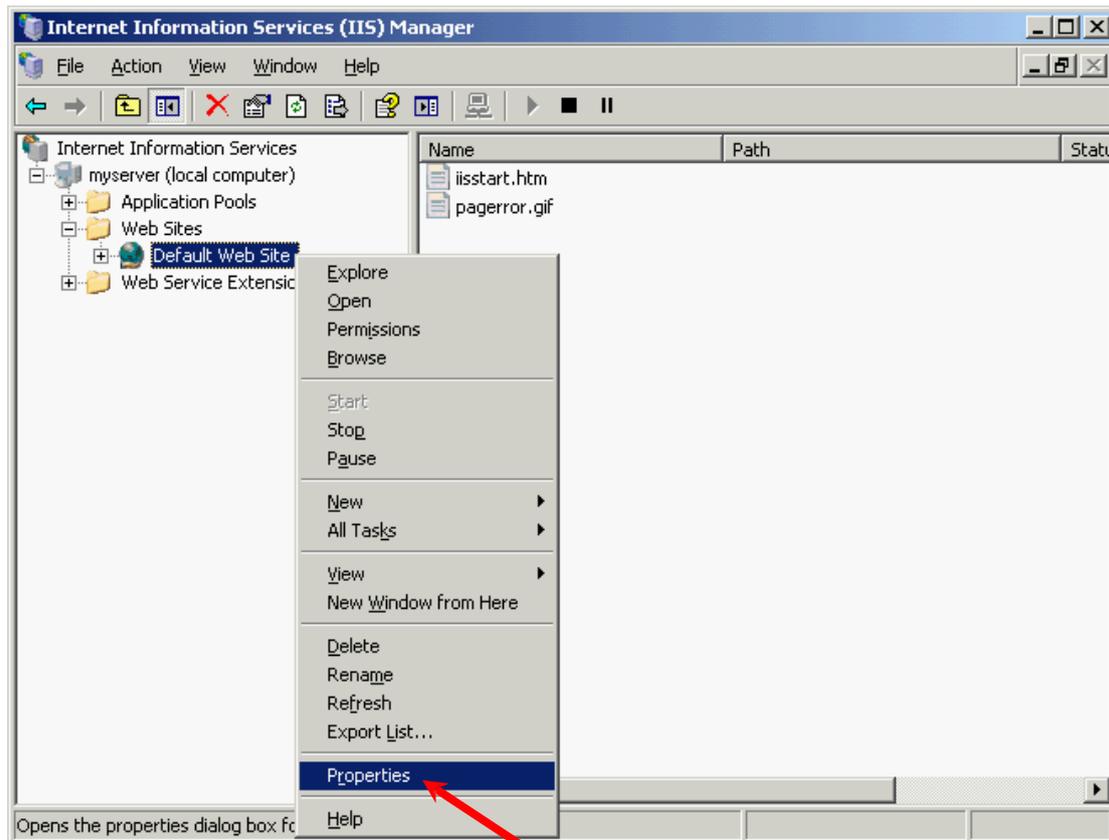


13. Click “OK” to complete.

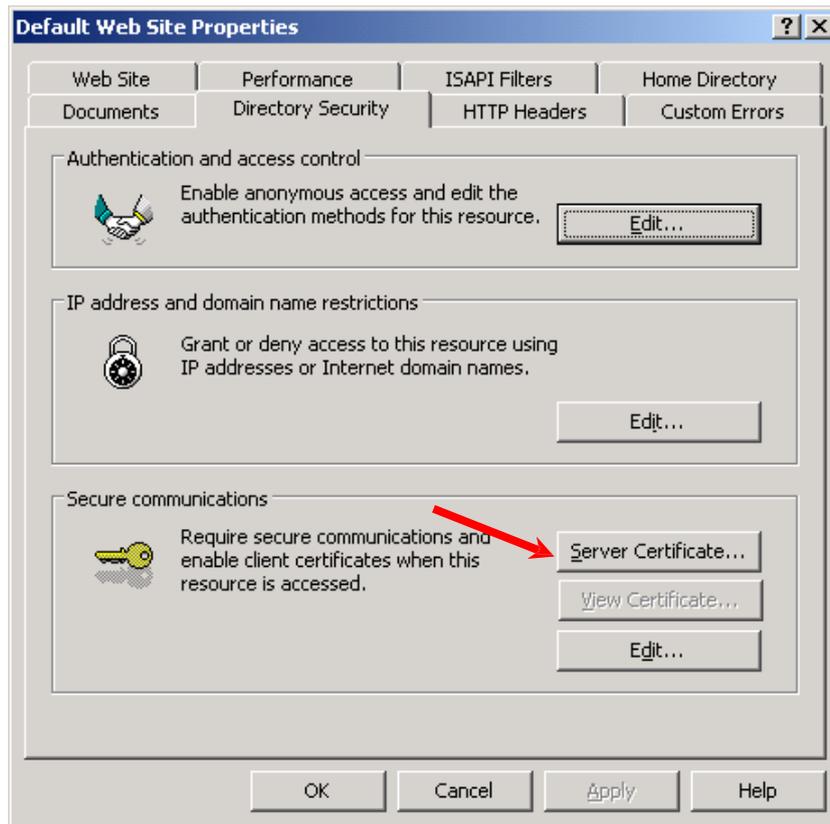


## **Restoring the Private Key for IIS 6.0**

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”.



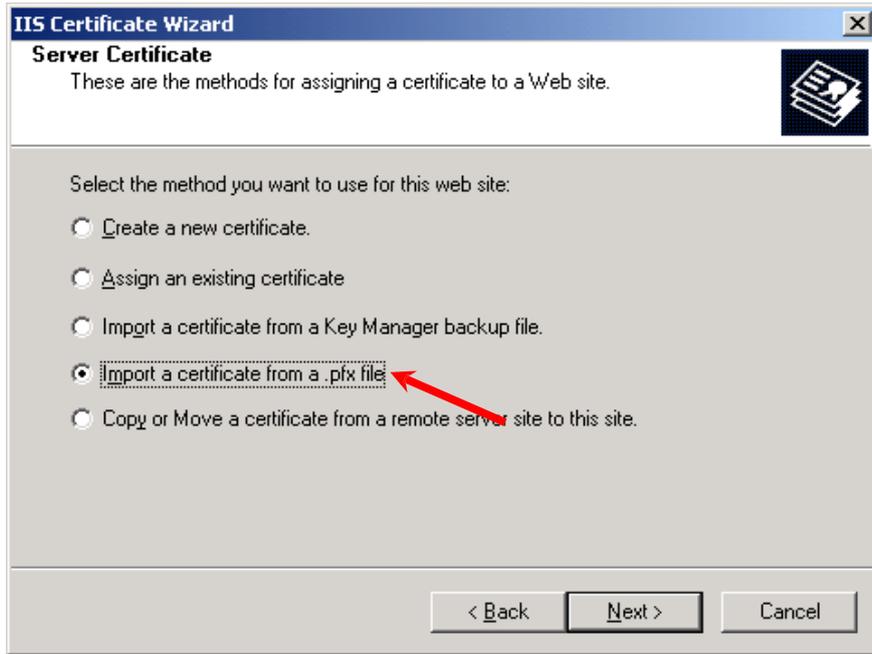
3. In the “Directory Security” tab, click “Server Certificate”.



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

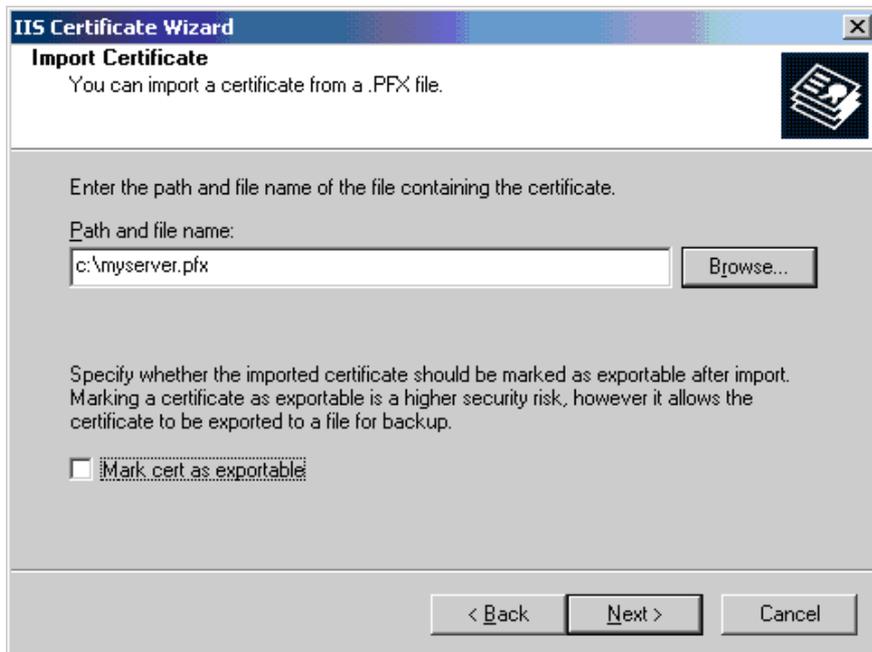


5. Select “Import a certificate from a .pfx file”, and then click “Next”.

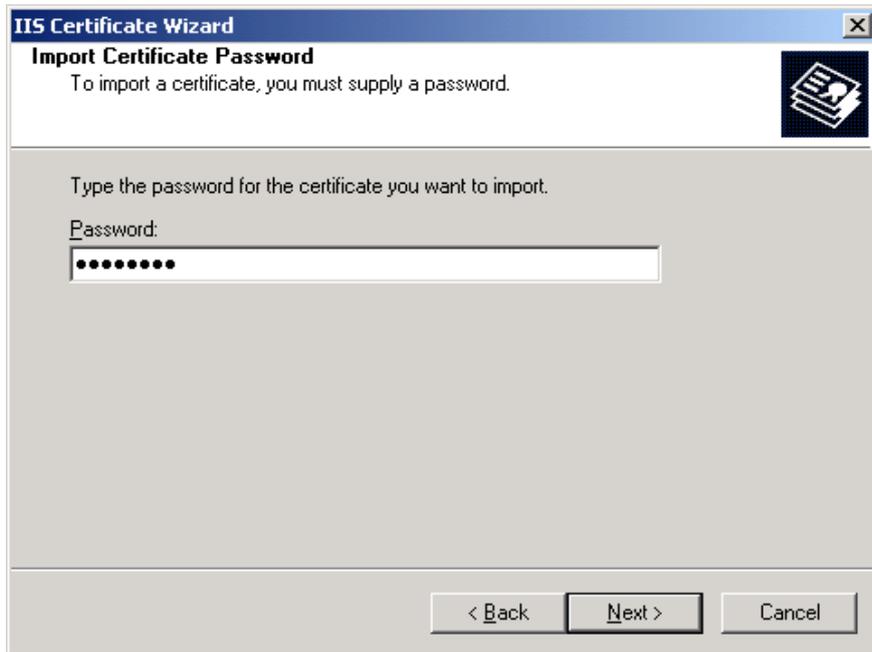


6. Enter the path and file name of the file containing the certificate and then click “Next”.

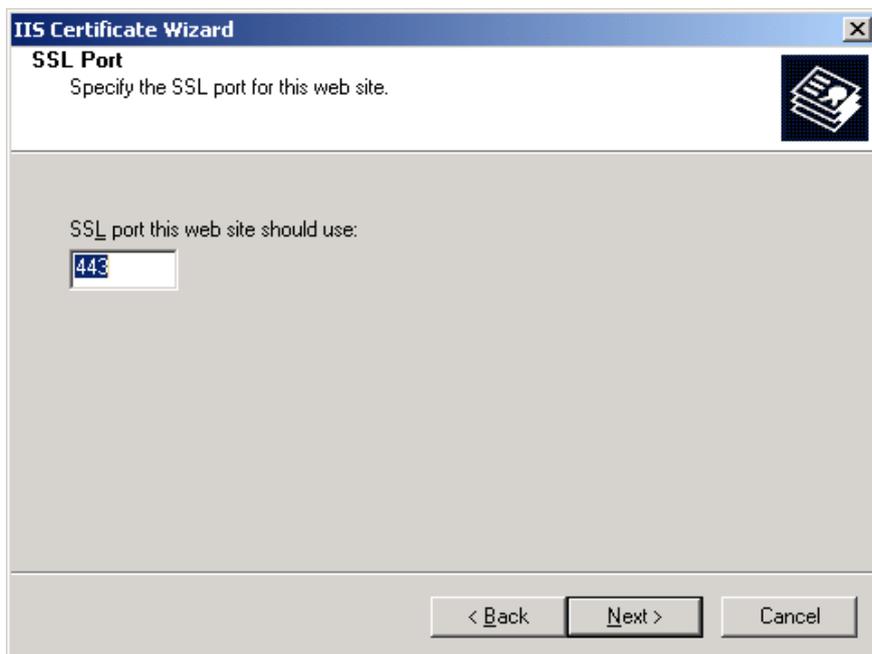
*Note: To allow you to back up or transport your certificate at a later time, you may mark this certificate as exportable.*



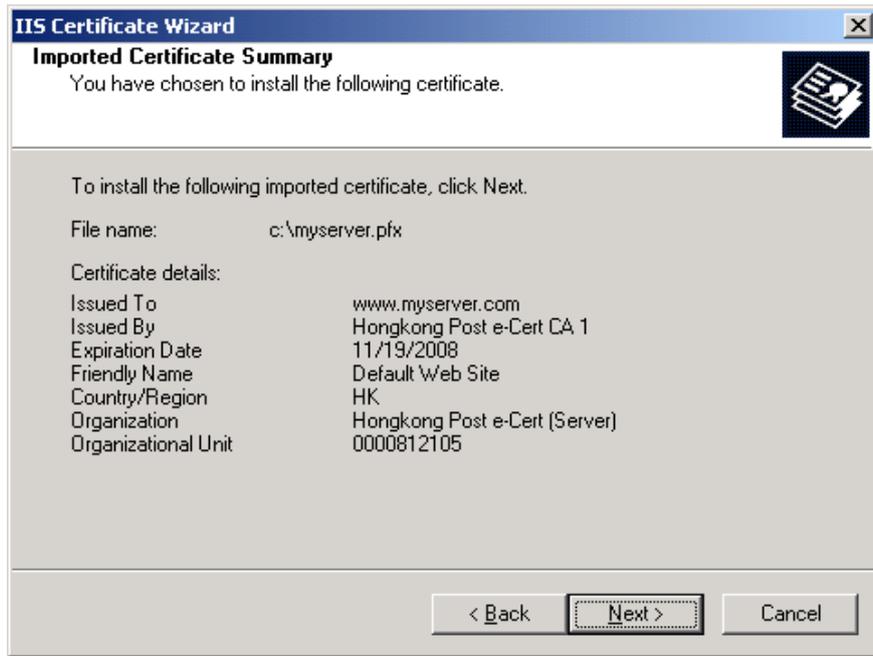
7. Type the password for the certificate you want to import, and then click “Next”.



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.

