



e-Cert (Server) User Guide

For Microsoft IIS 10.0

Contents

A.	Guidelines for e-Cert (Server) Applicant.....	2
	New and Renew Application	3
B.	Generating Certificate Signing Request (CSR)	4
C.	Submitting Certificate Signing Request (CSR)	9
D.	Installing Sub CA / Cross Certificate	13
	Remove Old Sub CA Certificate (if applicable).....	15
	Installing Sub CA / Cross Certificate	16
E.	Installing Server Certificate	20
F.	Backing up the Private Key	23
G.	Restoring the Private key.....	30

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 Authorized Representative to submit the CSR at the Hongkong Post CA website.

This user guide is for reference by applicants of e-Cert (Server) in generating their key pair and Certificate Signing Request (CSR) using Microsoft Internet Information Server (IIS) 10.0. 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	23
G.	Restoring the Private key	30

New and Renew Application

Please follow the instructions as described in the following sections for a new or renew application for e-Cert (Server):

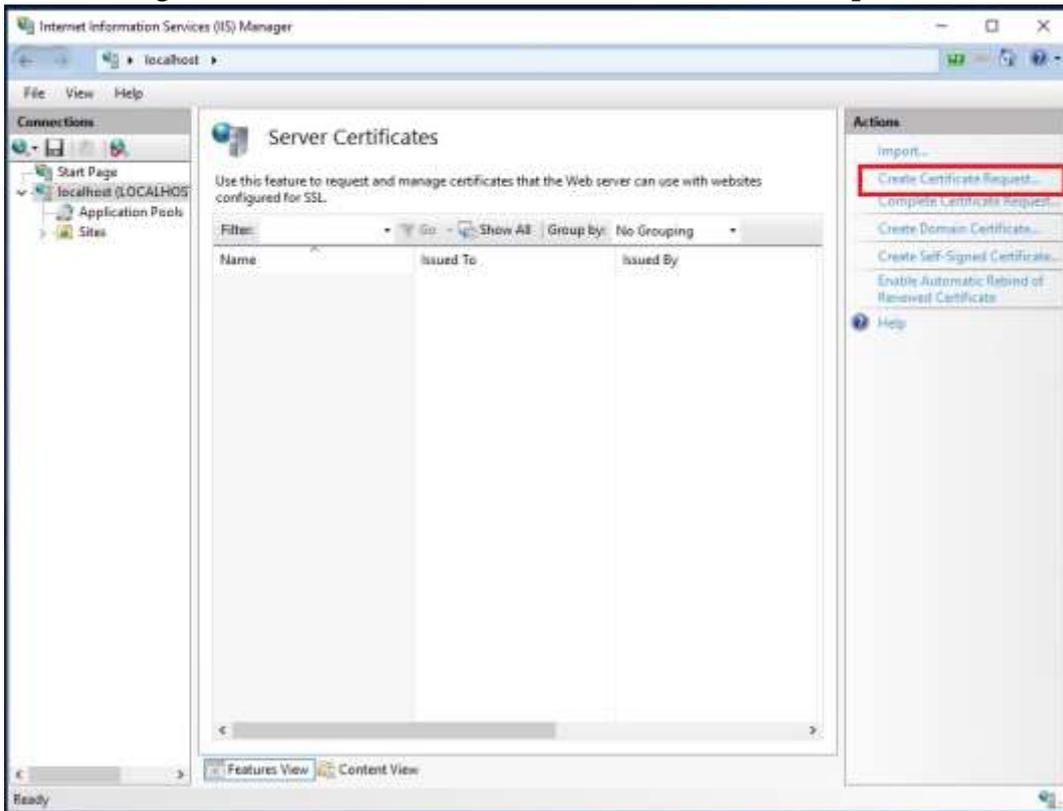
B.	Generating Certificate Signing Request (CSR)	4
C.	Submitting Certificate Signing Request (CSR)	9
D.	Installing Sub CA / Cross Certificate	13
	Remove Old Sub CA Certificate (if applicable).....	15
	Installing Sub CA / Cross Certificate	16
E.	Installing Server Certificate	20

B. Generating Certificate Signing Request (CSR)

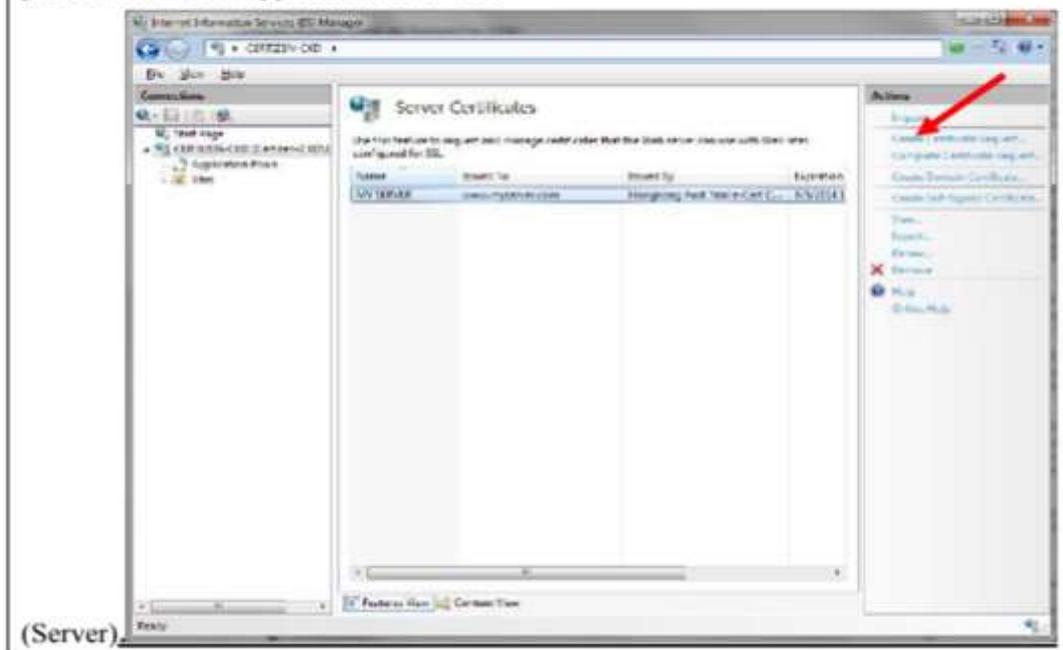
1. Start menu, “Administrative Tools”, and click on “Internet Information Services (IIS) Manager”.
2. In “Internet Information Services (IIS) Manager”, select your web site, and then double-click “Server Certificates”.



- 3 At the right column "Actions", select "Create Certificate Request".



Note : For renew of e-Cert (Server) application, please do not click "Renew" option to renew the certificate. Please click "Create Certificate Request" as the same procedures as new application for e-Cert



(Server)

- 4 Type the common name (i.e. server name) for your site, organization’s name and your organizational unit, select “**HK**” for the “**Country/Region**”. Type “**Hong Kong**” for both “**State/province**” and “**City/locality**”, and then 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.

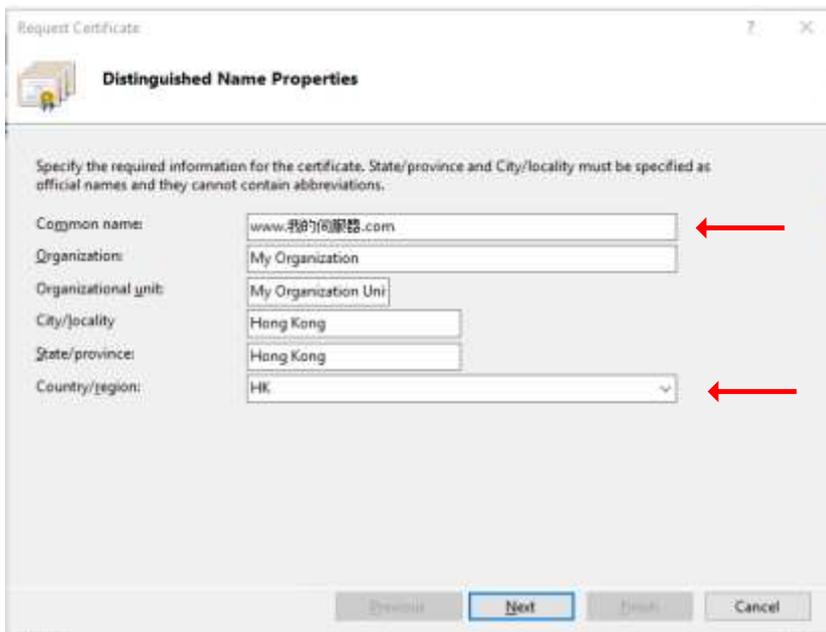
Note: For application of e-Cert (Server) with “Multi-domain” feature or EV e-Cert (Server) with “Multi-domain” feature, please input the “Common Name” field with “Server name used as Subject Name in the Certificate” being filled in the application form. It is not necessary to specify any “Additional 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.*

Note: For application of e-Cert (Server) with Chinese Domain Name

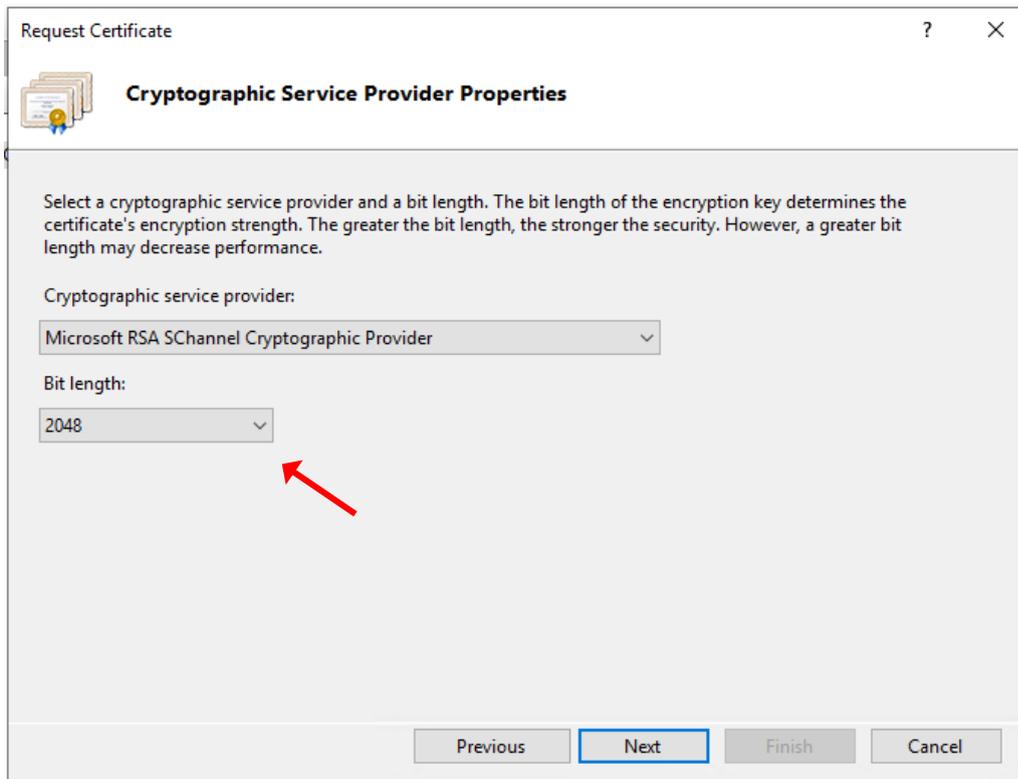
Option 1: please input the “Common Name” field with “Server name used as Subject Name in the Certificate” being filled in the application form.

Option 2: Use of IDN conversion tool to convert Chinese Domain Name into ASCII characters and input of the converted name in the “Common Name” field is also supported.

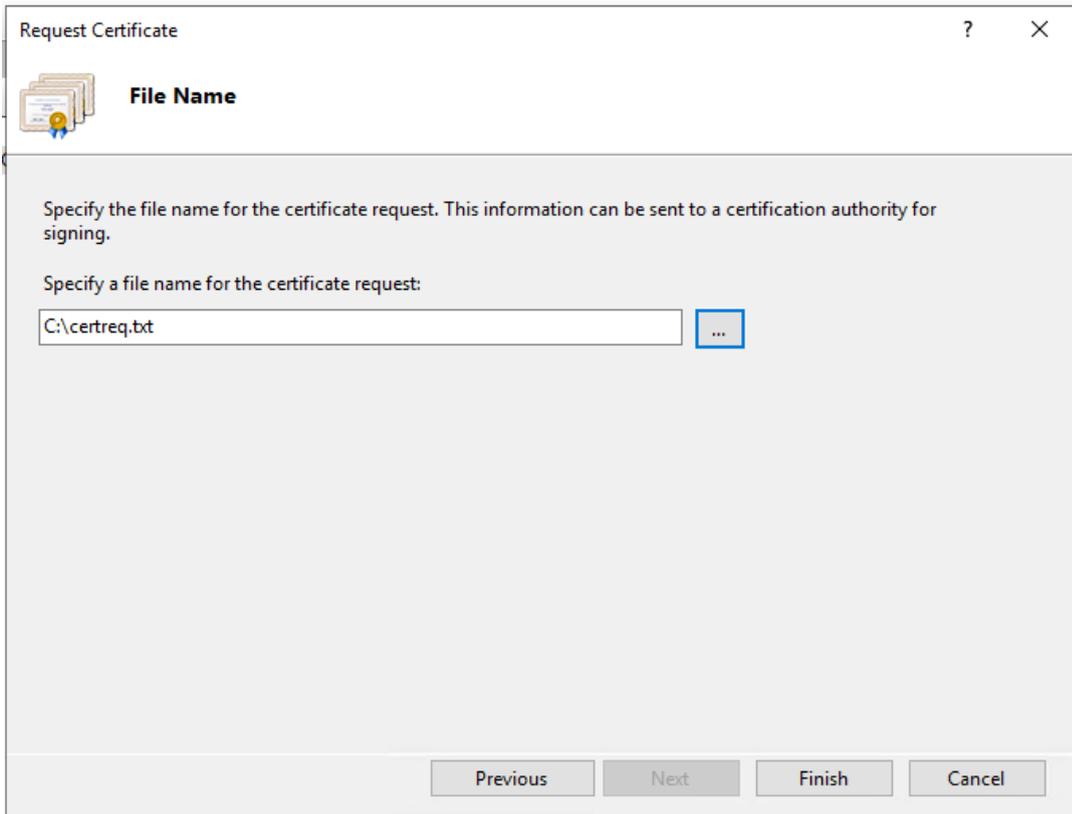


5. Choose “**Microsoft RSA SChannel Cryptographic Provider**” for the “Cryptographic service provider”, and “**2048**” for the “Bit length”, and then click “**Next**”.

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.



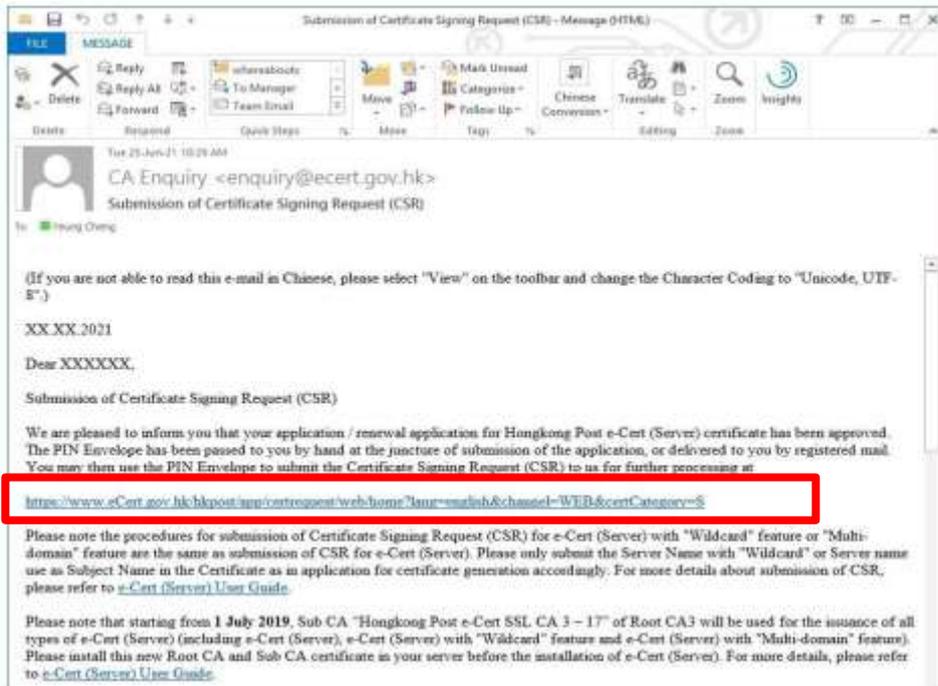
6. Enter a file name for the certificate request, and then click **“Finish”**.



The screenshot shows a Windows dialog box titled "Request Certificate" with a question mark icon and a close button (X) in the top right corner. On the left side, there is an icon of three certificates and the text "File Name". The main area of the dialog contains the following text: "Specify the file name for the certificate request. This information can be sent to a certification authority for signing." Below this, it says "Specify a file name for the certificate request:" followed by a text input field containing "C:\certreq.txt" and a blue ellipsis button "...". At the bottom of the dialog, there are four buttons: "Previous", "Next", "Finish", and "Cancel".

C. Submitting Certificate Signing Request (CSR)

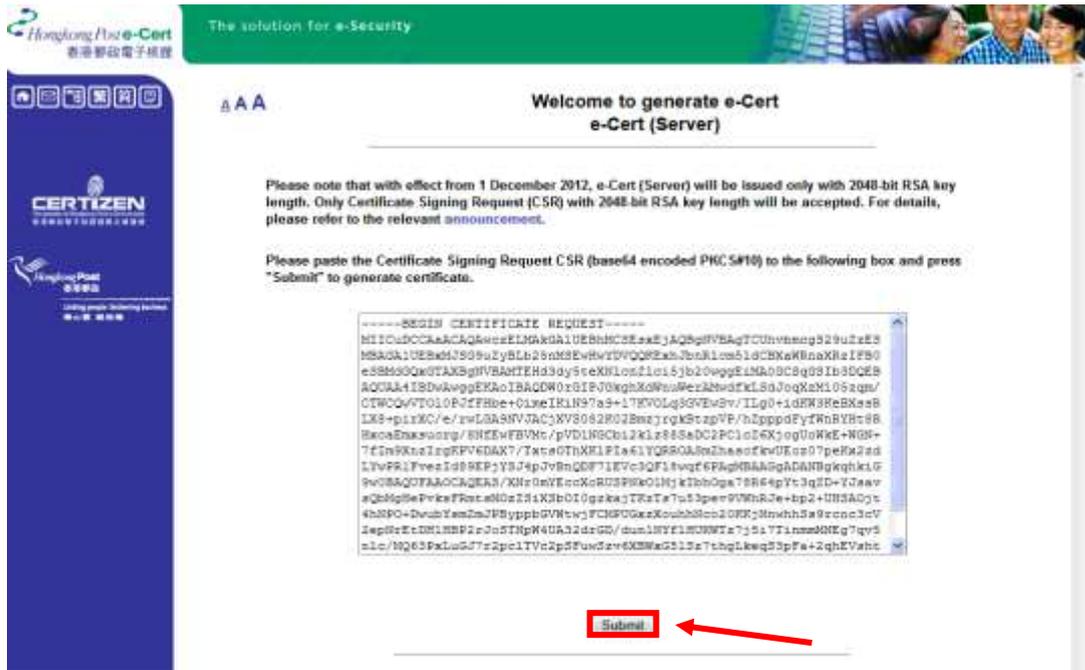
1. Click on the hyperlink in the e-mail with subject “**Submission of Certificate Signing Request (CSR)**” sent from Hongkong Post Certification Authority to access the Hongkong Post CA web site.



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**”.



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 **Hongkong Post e-Cert (Server)**.



Note:

1. You can also download your e-Cert (Server) from the Search and Download Certificate web page.

<https://www.ecert.gov.hk/en/sc/index.html>

2. Starting from 1 July 2019, Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" of Root CA3 will be used for the issuance of all types of e-Cert (Server). Subscribers with e-Cert (Server) certificates issued on or after 1 July 2019 is required to conduct the following so that their websites installed with e-Cert (Server) under Root CA3 will continue to be trusted by common web browsers: Install the Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" issued by Root CA3. Click the following link to download:

http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt

Install the cross-certificate "Hongkong Post Root CA 3" issued by "GlobalSign Root CA - R3". Click the following link to download:

http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

3. Starting from 21 January 2022, Sub CA "Hongkong Post e-Cert EV SSL CA 3 - 17" of Root CA3 will be used for the issuance of all types of EV e-Cert (Server). Subscribers with EV e-Cert (Server) certificates issued on or after 21 January 2022 is required to conduct the following so that their websites installed with EV e-Cert (Server) under Root CA3 will continue to be trusted by common web browsers:

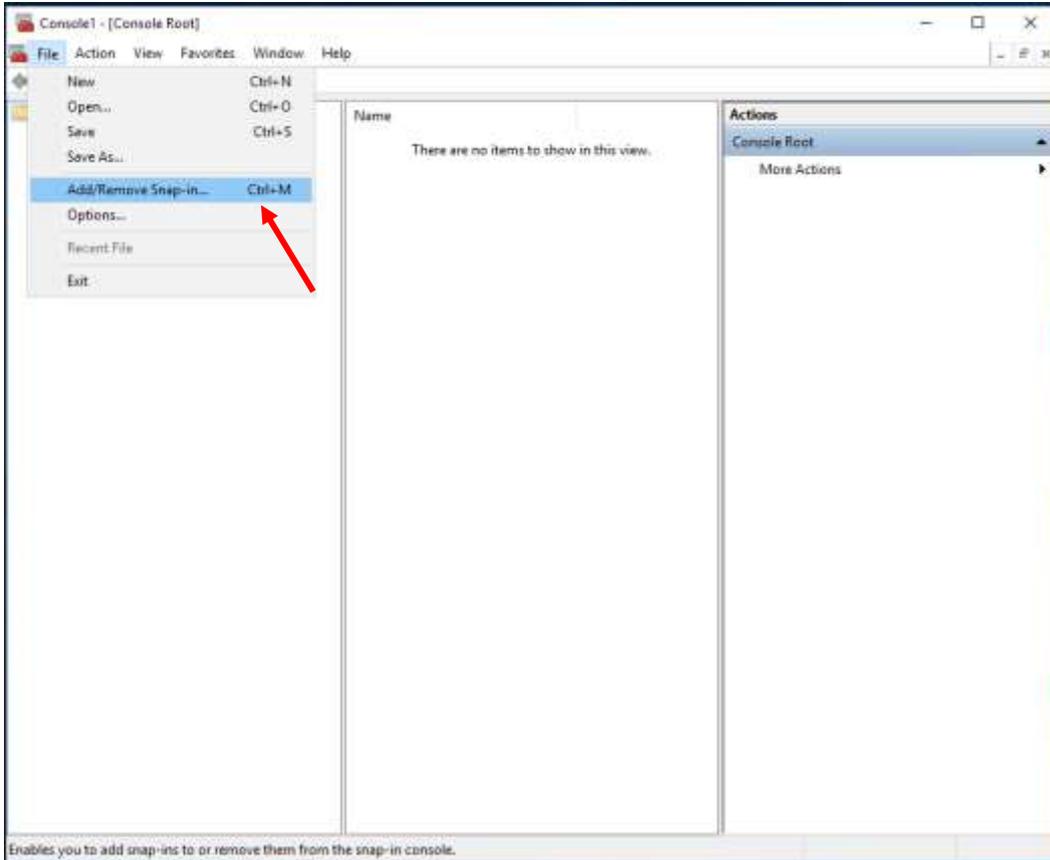
Install the Sub CA "Hongkong Post e-Cert EV SSL CA 3 - 17" issued by Root CA3. Click the following link to download:

Install the cross-certificate "Hongkong Post Root CA 3" issued by "GlobalSign Root CA - R3". Click the following link to download:

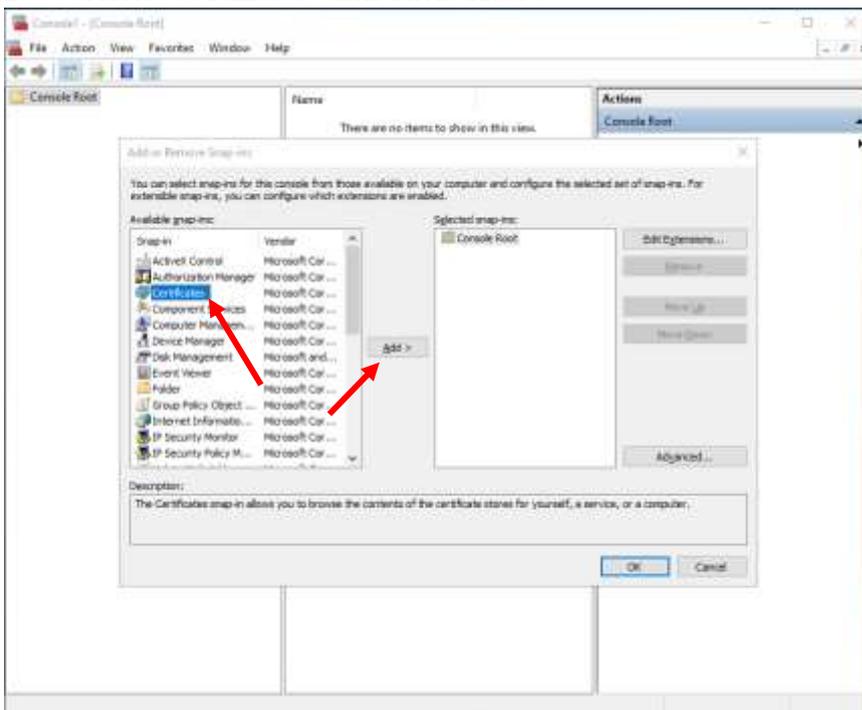
http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

D. Installing Sub CA / Cross Certificate

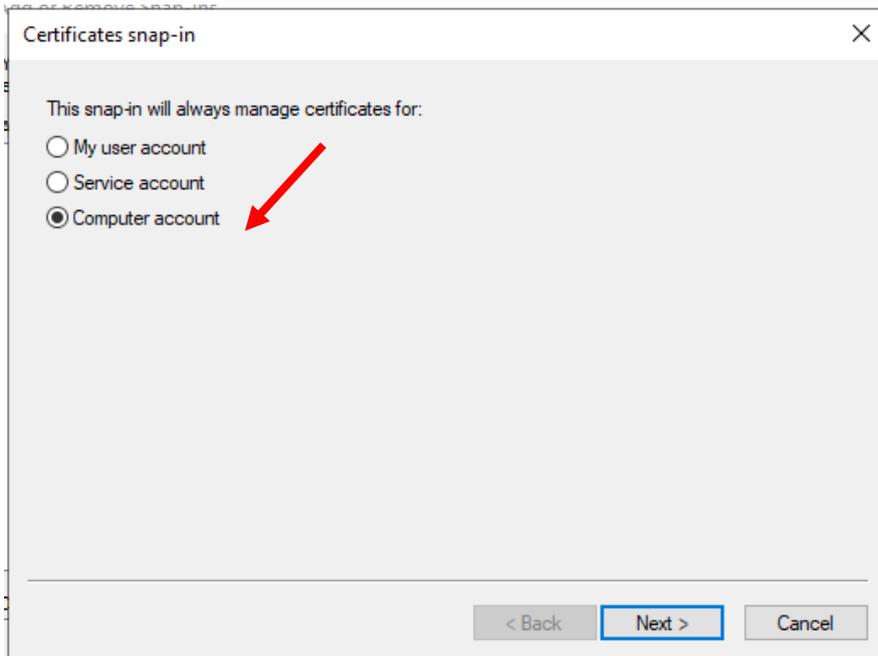
1. Start **Microsoft Management Console (MMC)** by clicking “**Start**” > “**Run**”, type “**mmc**” and click **OK**, and then select “**Add/Remove Snap-in**” from the “**File**” menu.



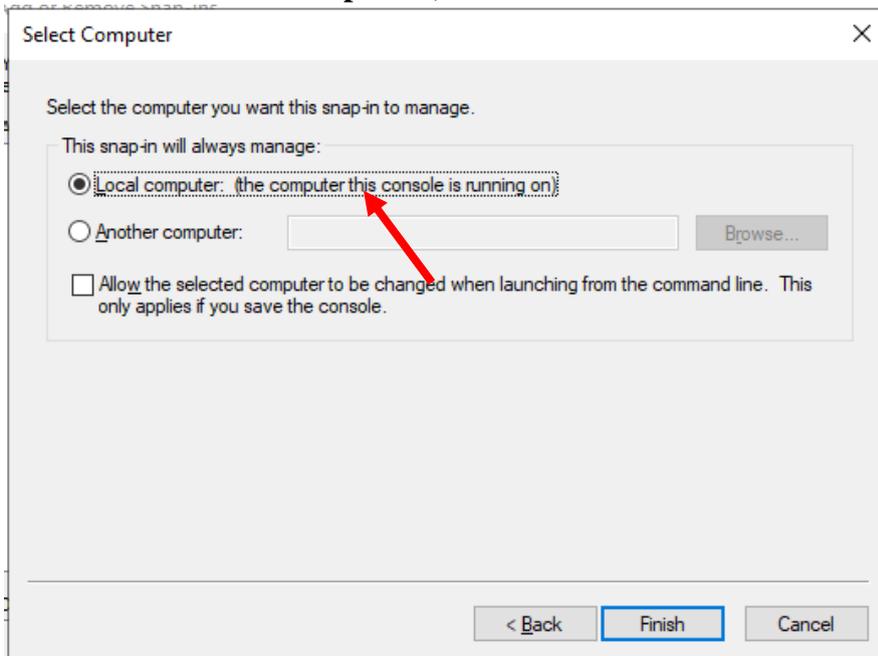
2. Select “**Certificate**” then Click “**Add**”.



3. Select “**Computer account**”, and then click “**Next**”.



4. Select **“Local computer”**, and then click **“Finish”**.

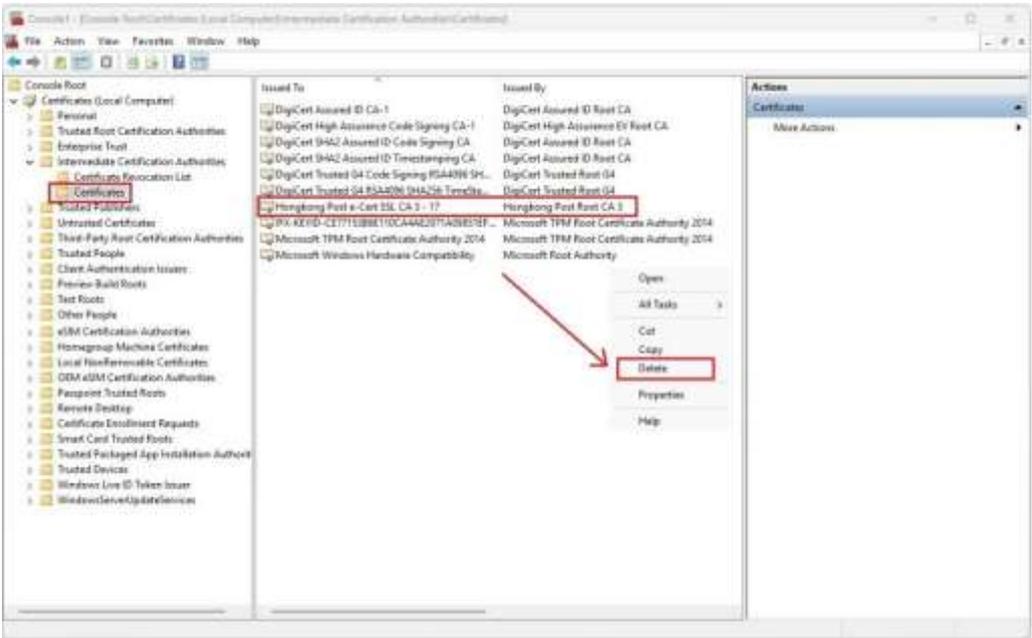


The following uses the “**Hongkong Post e-Cert SSL CA 3 - 17**” Sub CA certificate as example.

Note:
Starting from **1 May 2025**, new Sub CA certificates will be used to issue e-Cert (Server). When installing an e-Cert (Server) issued on or after 1 May 2025, **please first remove the old Sub CA certificate, if applicable, and then install the new Sub CA certificate on your server.**

Remove Old Sub CA Certificate (if applicable)

Expand the “Intermediate Certification Authorities” and select “Certificates” Highlighted the Old “Hongkong Post e-Cert SSL CA3-17” then right click & select “Delete”.



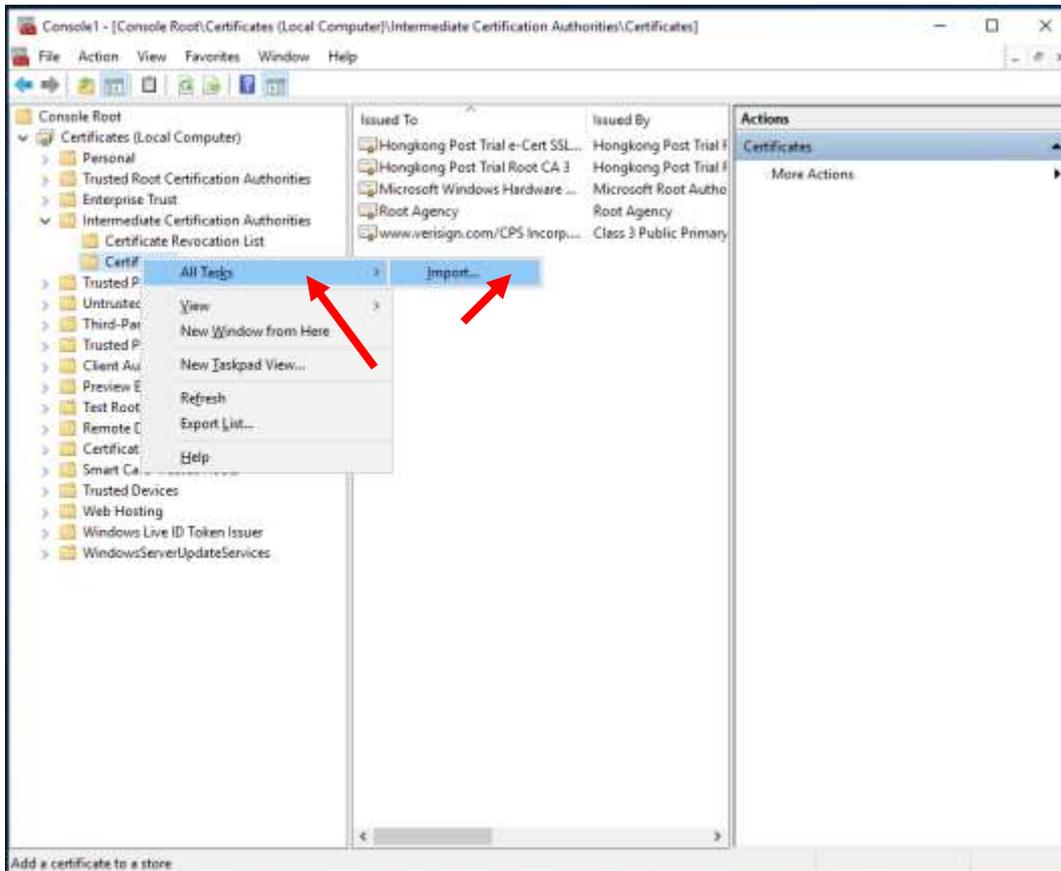
Click “Yes” to delete.



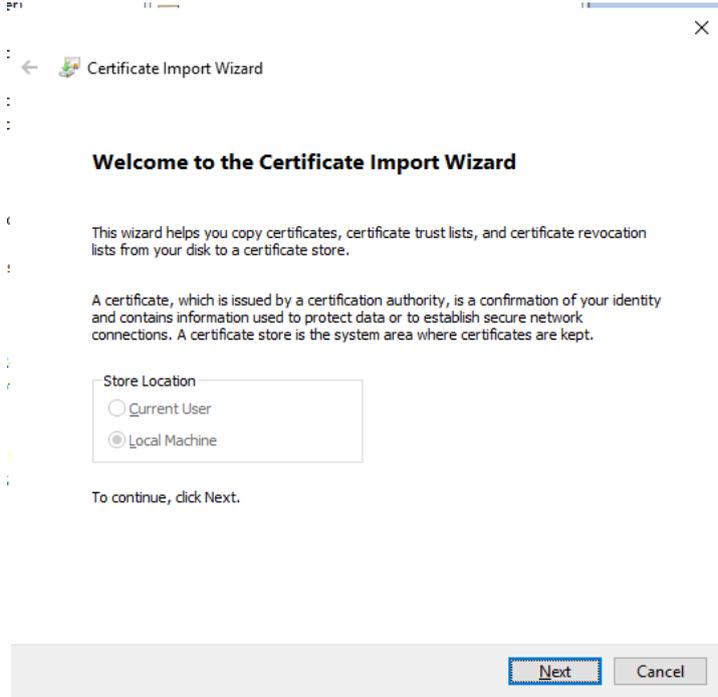
The following uses the “**Hongkong Post e-Cert SSL CA 3 - 17**” Sub CA certificate as example.

Installing Sub CA / Cross Certificate

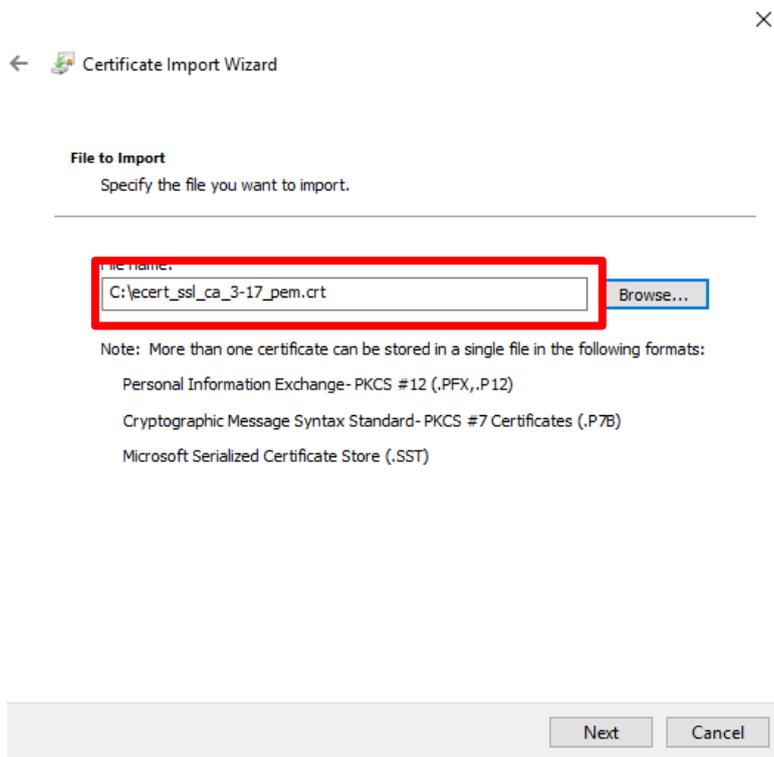
5. Expand “**Intermediate Certification Authorities**” and right-click “**Certificates**”, and then select “**All Tasks**” > “**Import**”.



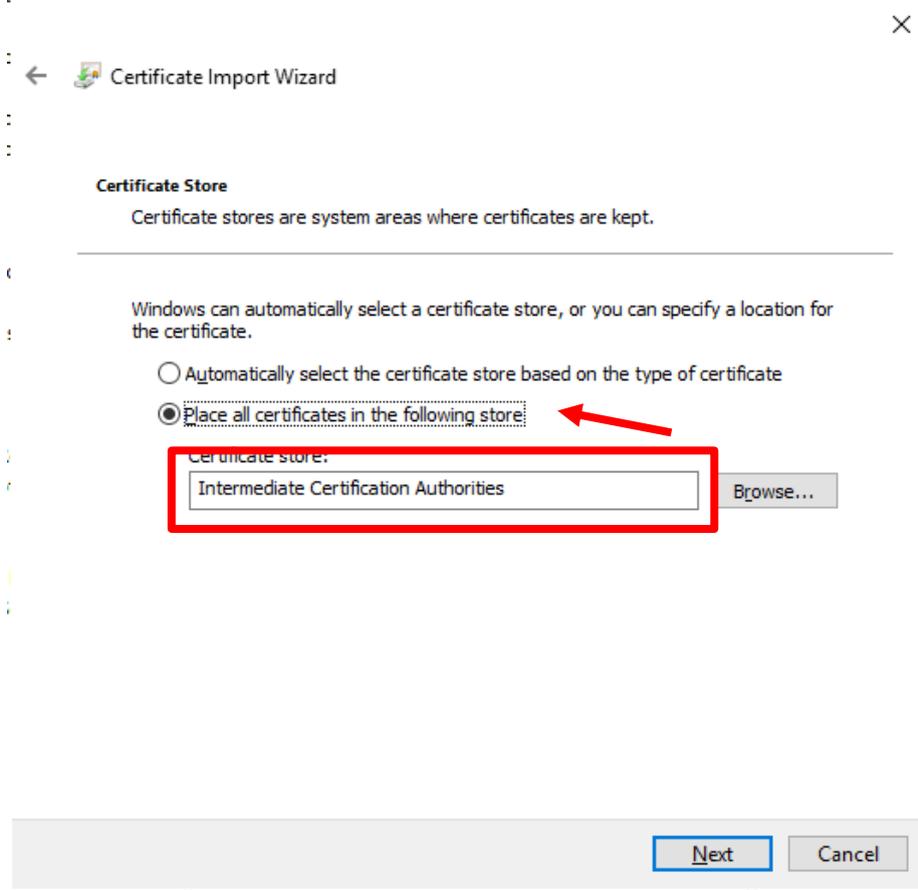
6. In the “**Certificate Import Wizard**”, click “**Next**” to continue.



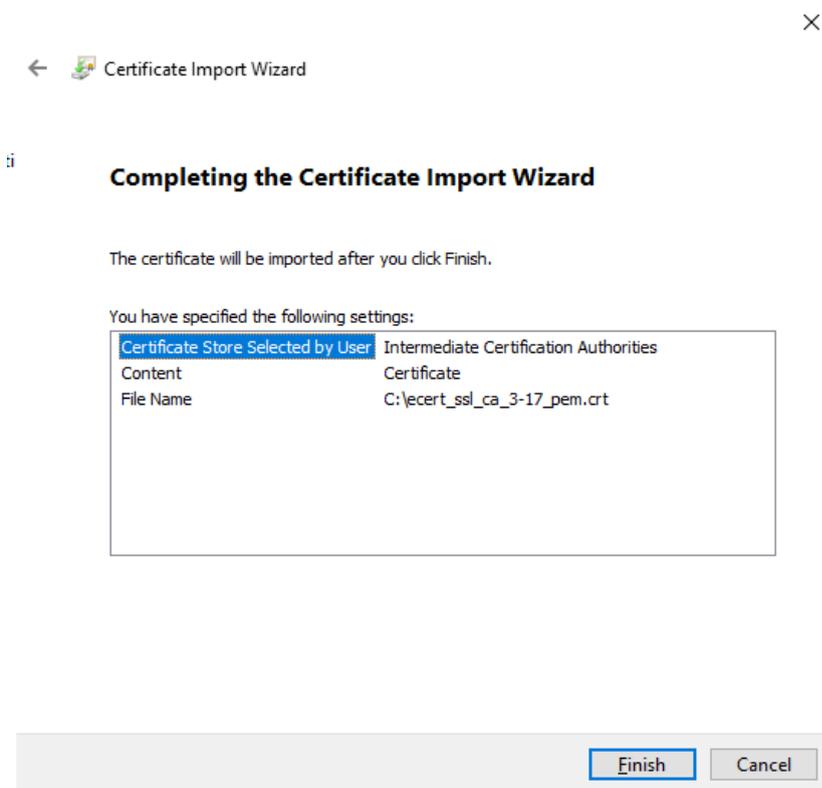
7. Click “**Browse**” to locate the “**Hongkong Post e-Cert SSL CA 3 - 17**” certificate that you downloaded in Part C Step 7 (ecert_ssl_ca_3-17_pem.crt), and then click “**Next**”.



8. Select **“Place all certificates in the following store”**, make sure **“Intermediate Certification Authorities”** has been selected as **“Certificate store”**, and then click **“Next”**.



9. Click **“Finish”** to close the wizard.



10. Click “OK” to complete.

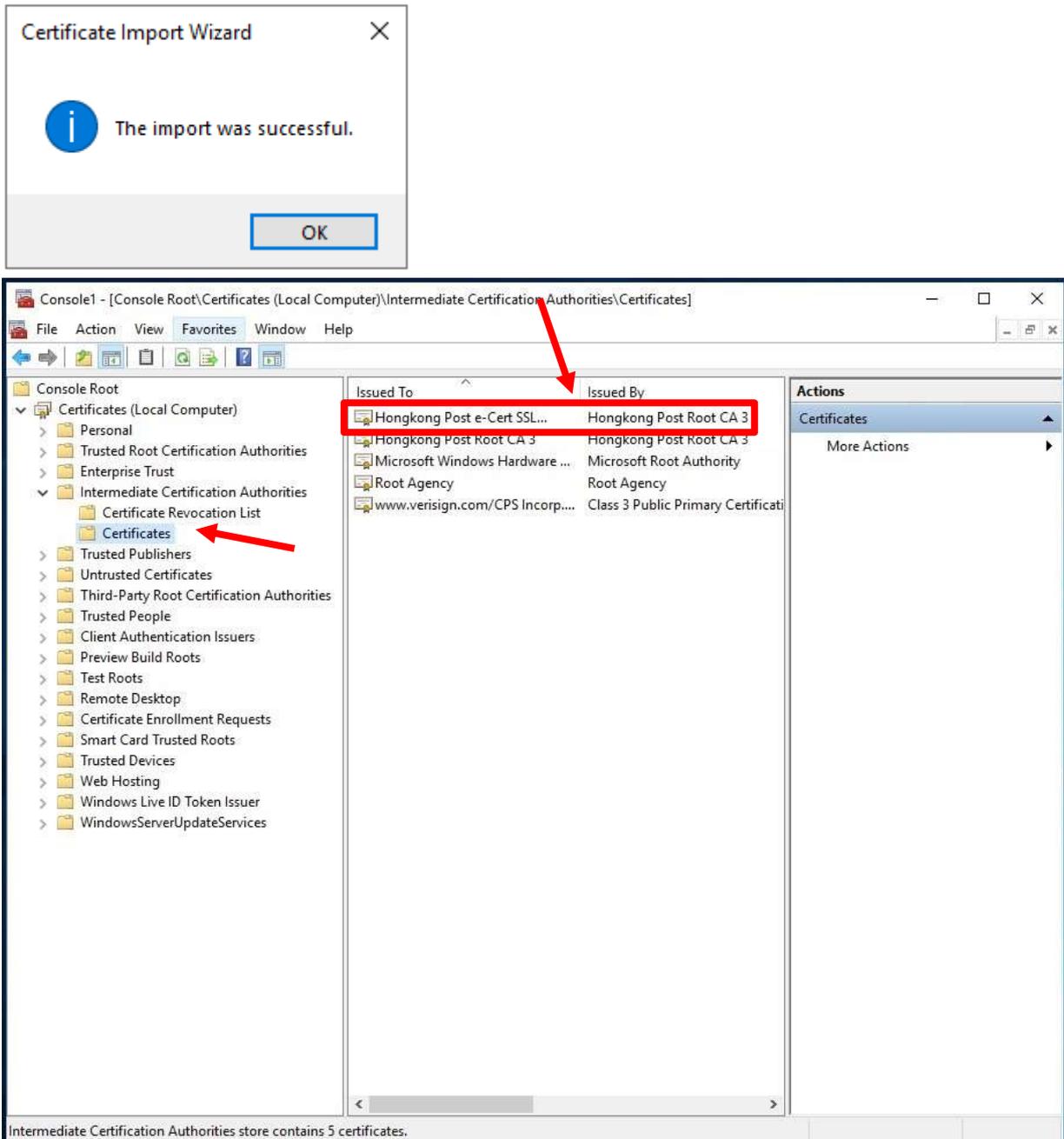
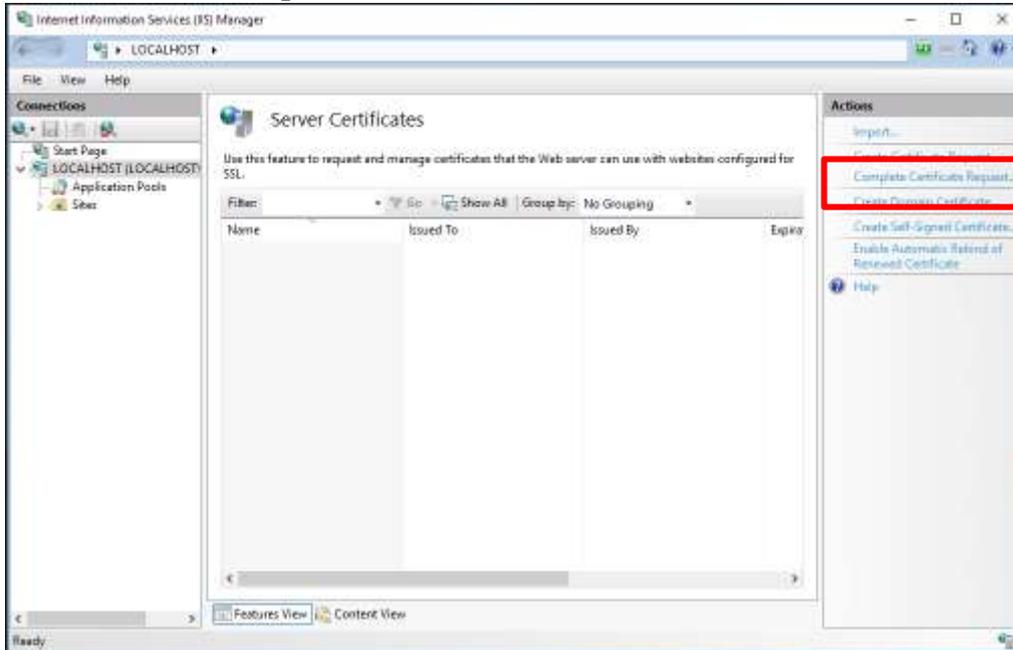


Figure 1: “Hongkong Post e-Cert SSL CA 3 - 17” certificate has been successfully installed

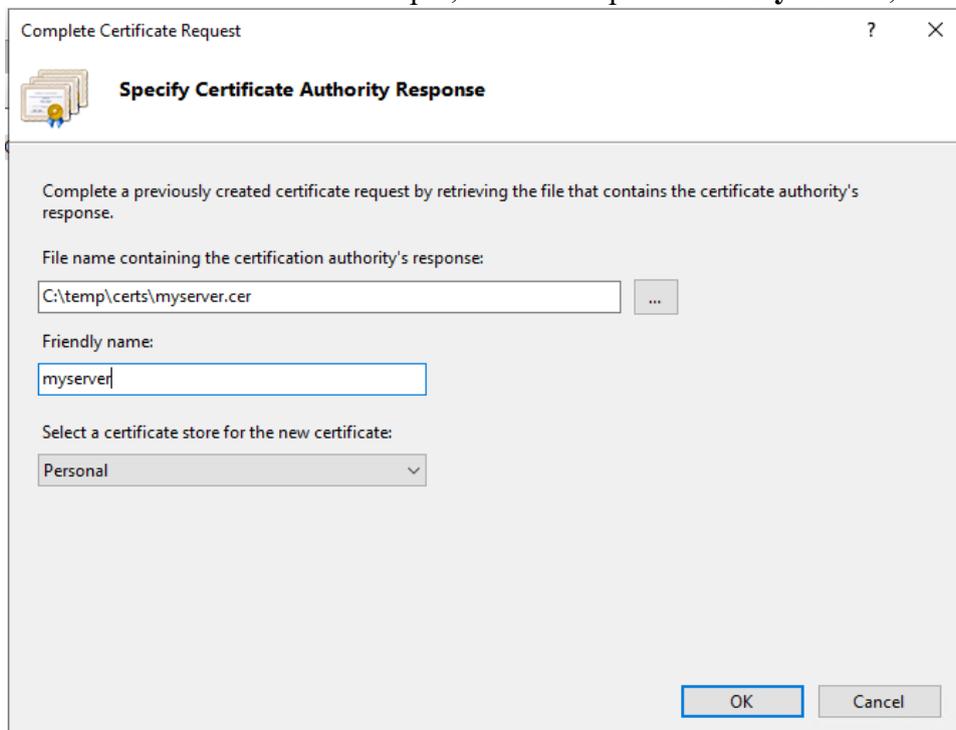
Repeat step 5 to step 10 for installation of cross-cert (root_ca_3_x_gsca_r3_pem.crt) which was downloaded in Section C step 7.

E. Installing Server Certificate

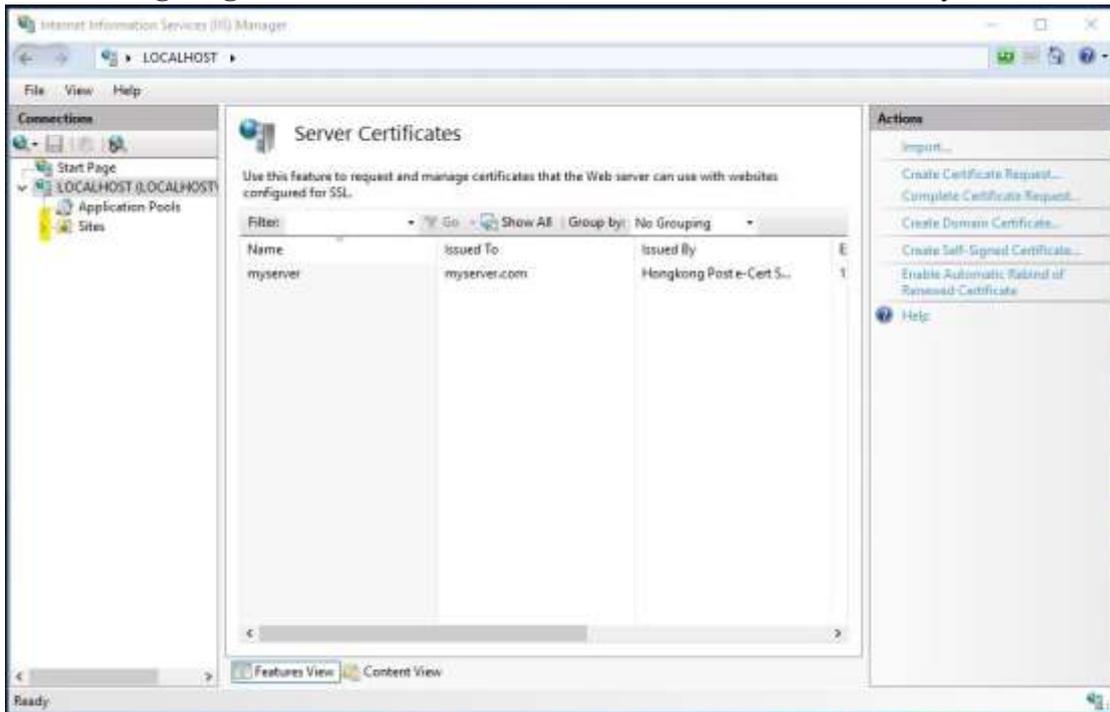
1. In “**Internet Information Services (IIS) Manager**”, select your web site, and then double-click “**Server Certificates**”. At the right column "Actions", select “**Complete Certificate Request**”.



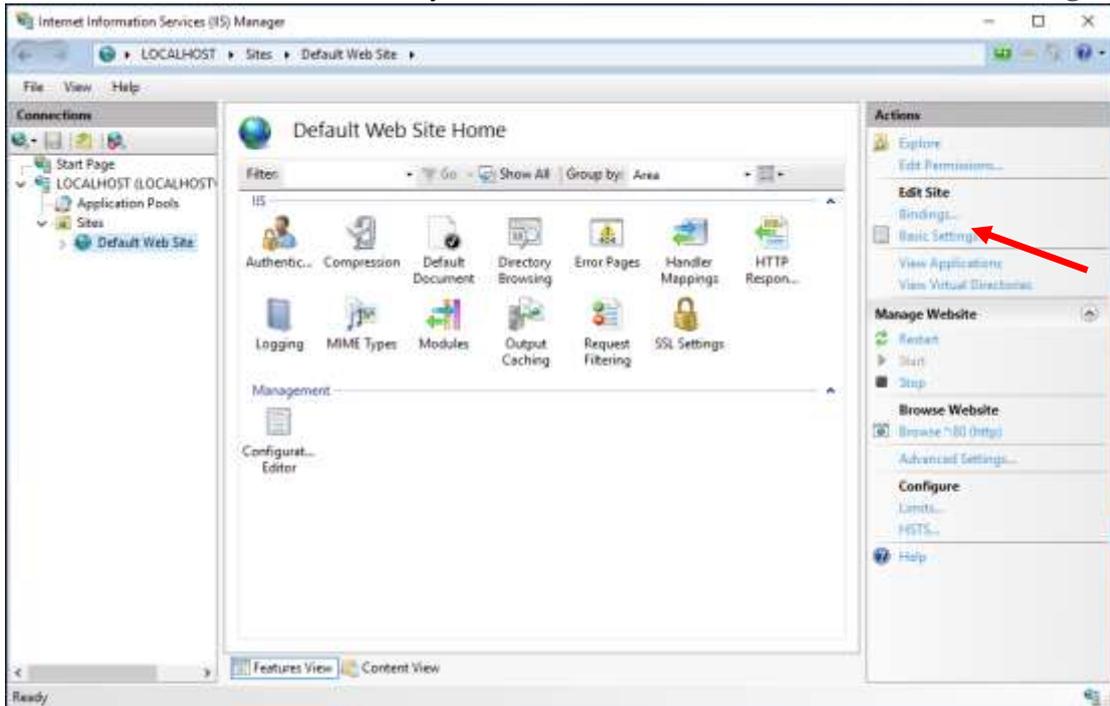
2. Click “**Browse**” to locate the “**Hongkong Post e-Cert (Server)**” certificate that you downloaded in Part C Step 7, and then input “**Friendly name**”, click “**OK**”.



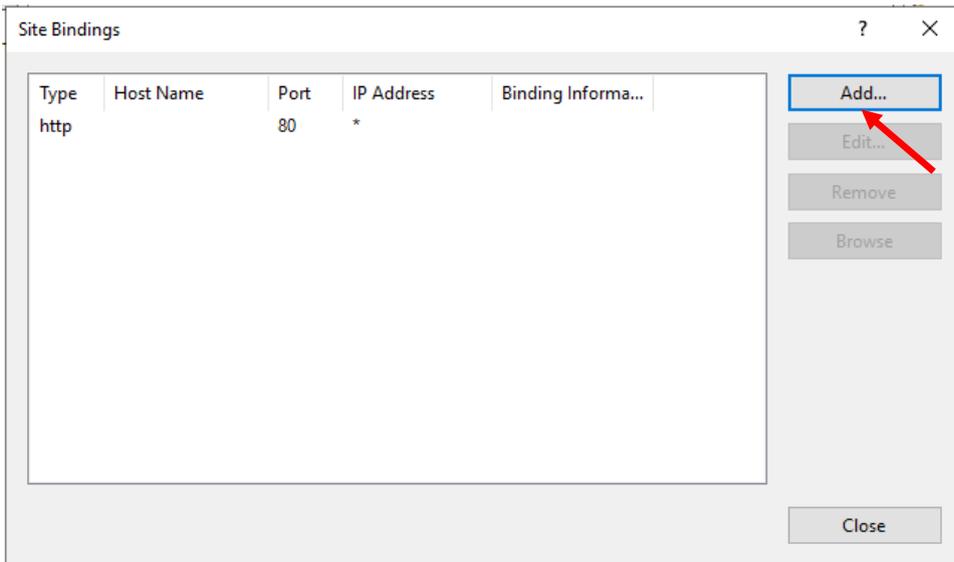
3. “Hongkong Post e-Cert (Server)” certificate has been successfully installed.



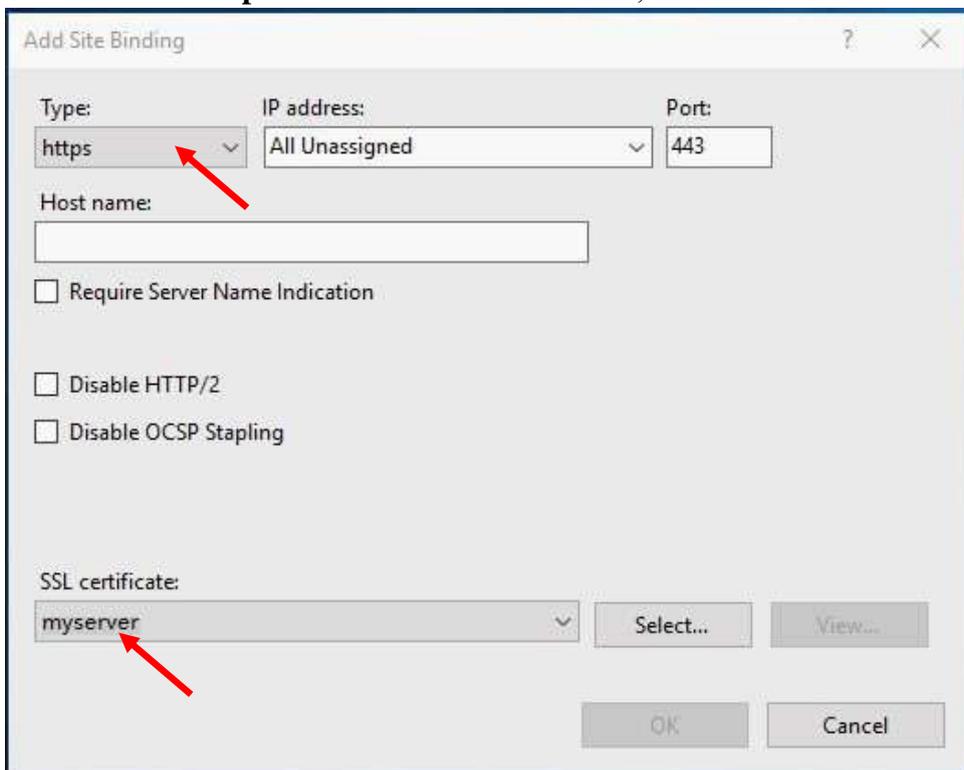
4. Click on the website that you want to bind the certificate to. Click “**Bindings**”.



5. click “Add...”.

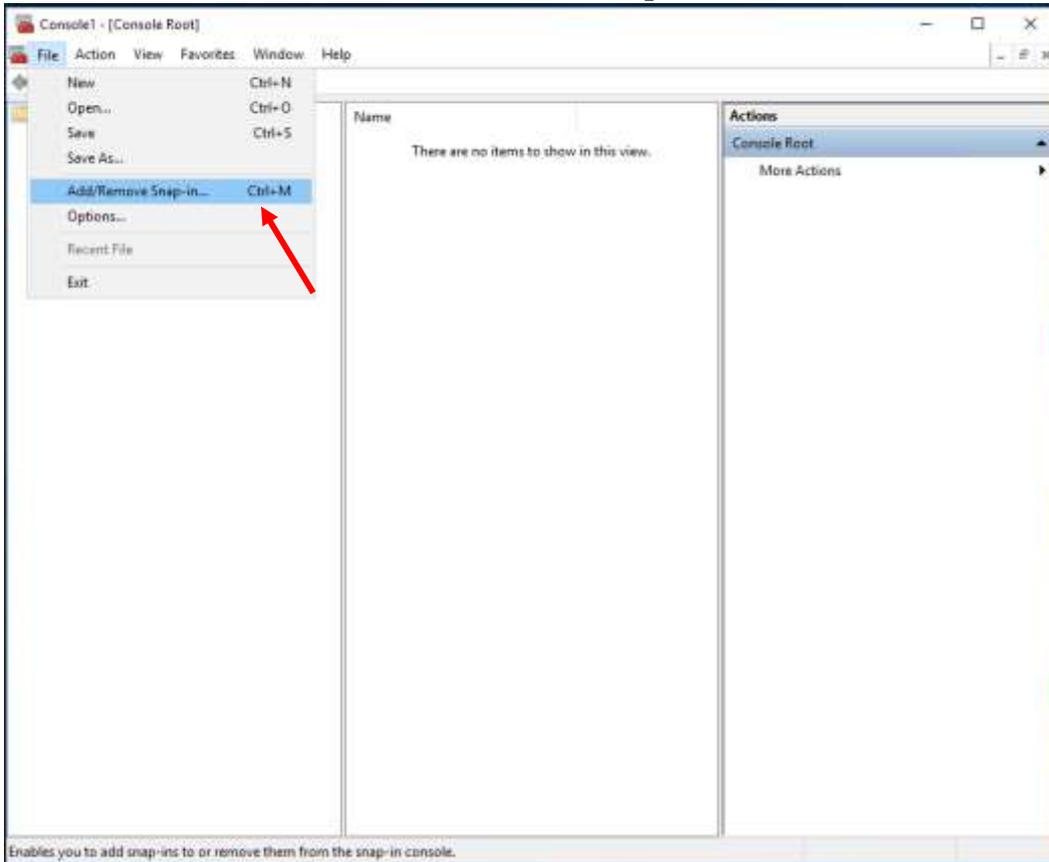


6. Select “https” and related SSL certificate, then click “OK” to confirm.

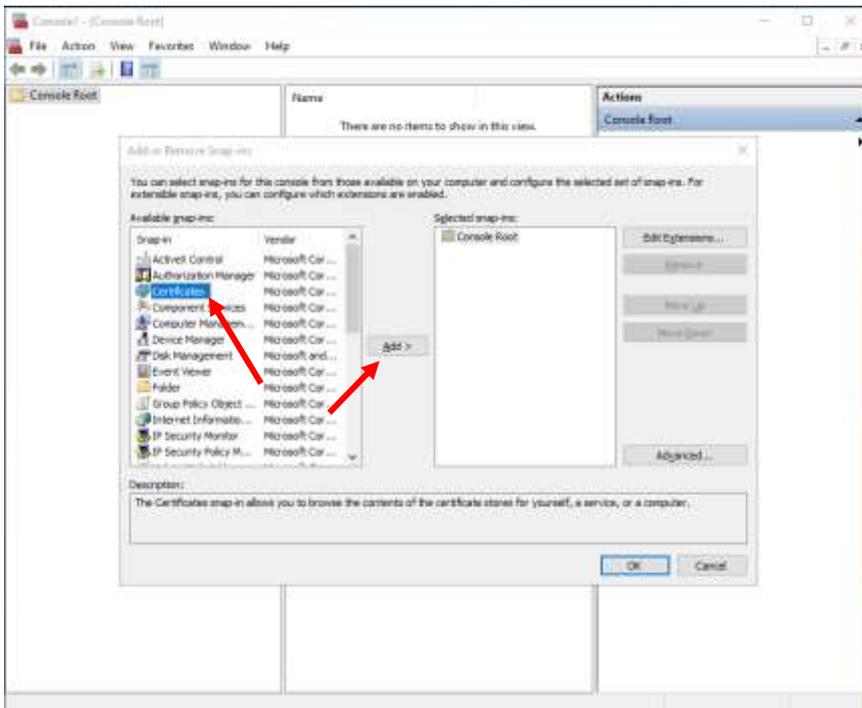


F. Backing up the Private Key

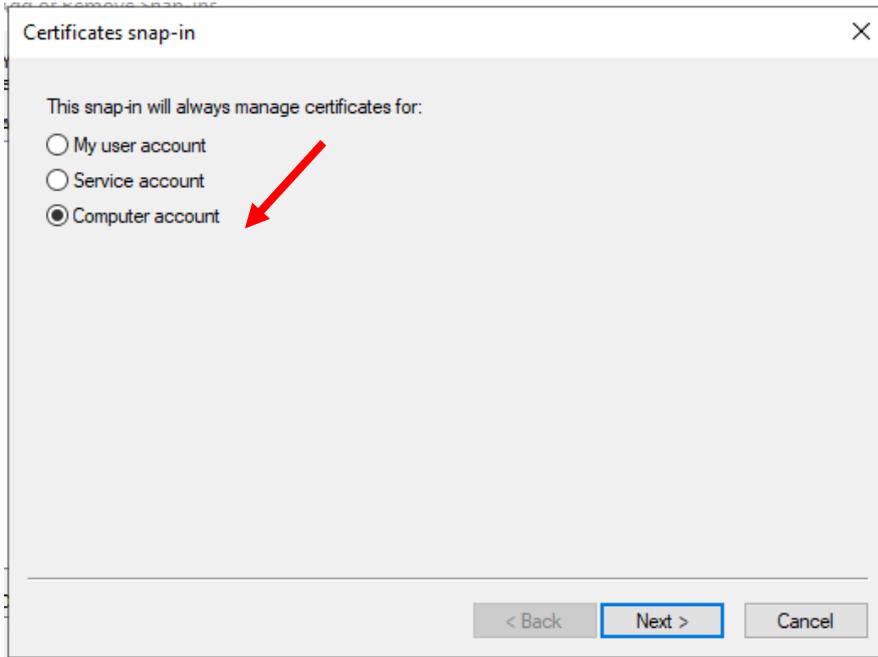
1. Start Microsoft Management Console (MMC) by clicking **“Start”** > **“Run”**, type **“mmc”** and click OK, and then select **“Add/Remove Snap-in”** from the **“File”** menu.



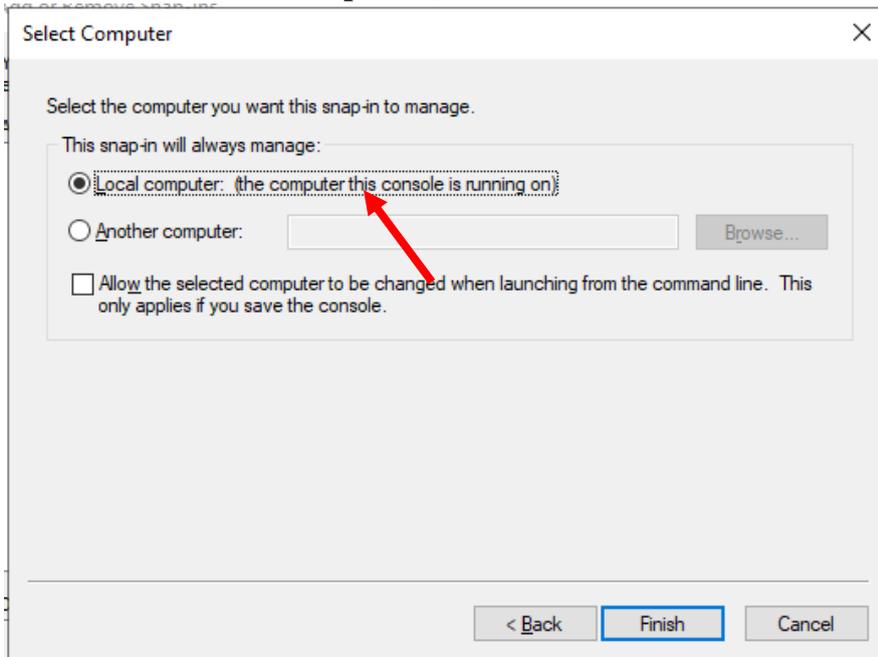
2. Select **“Certificate”** then Click **“Add”**.



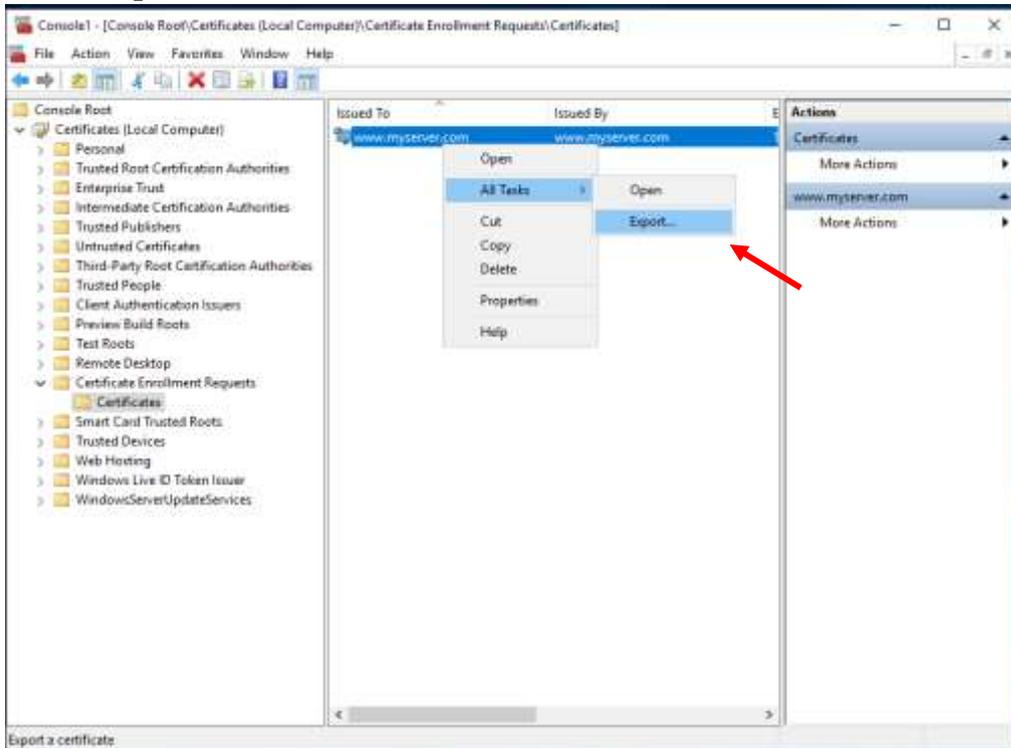
3. Select “**Computer account**”, and then click “**Next**”.



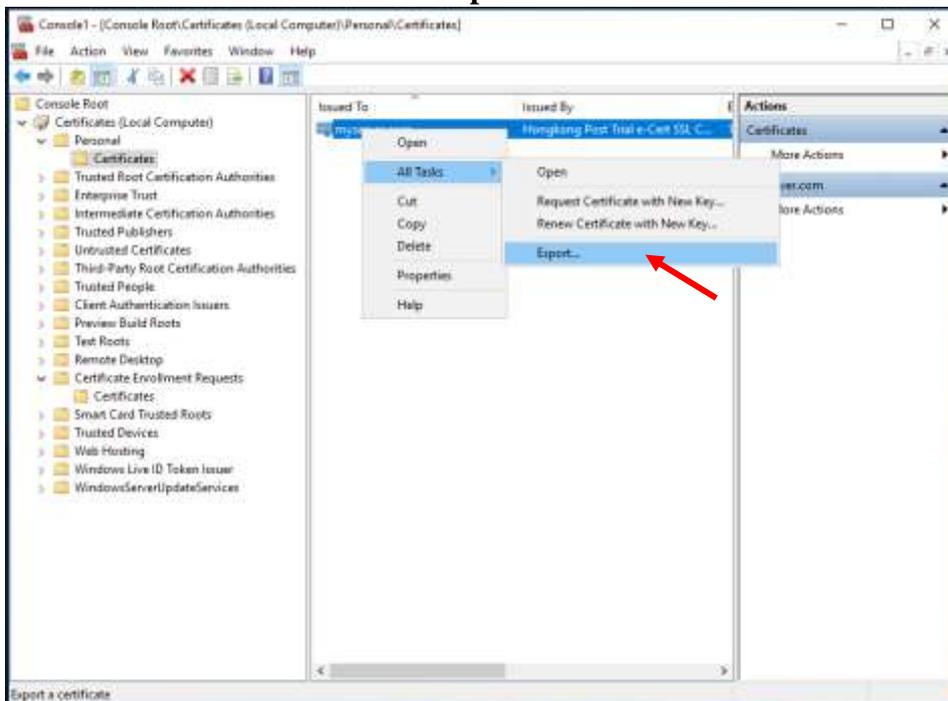
4. Select “**Local computer**”, and then click “**Finish**”.



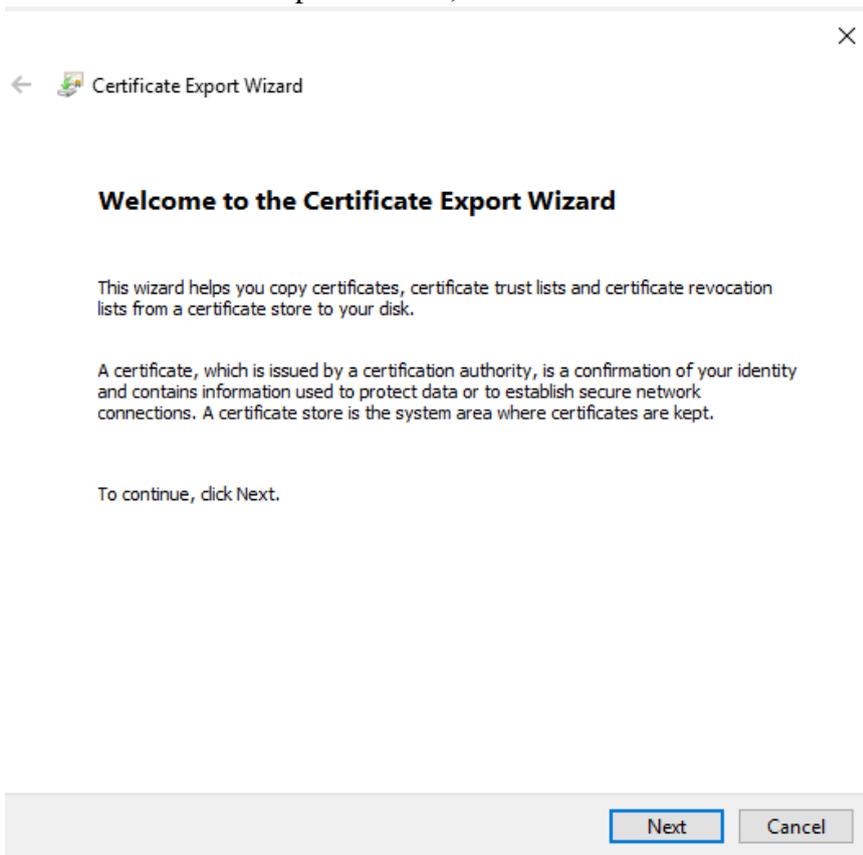
5. Backup the private key:
 - To backup the private key of a pending request, expand “**Certificate Enrollment Requests**” (or named “**REQUESTS**” in some systems) and select “**Certificates**”, select the pending request that you just created, right-click and then select “**All Tasks**” > “**Export**”.



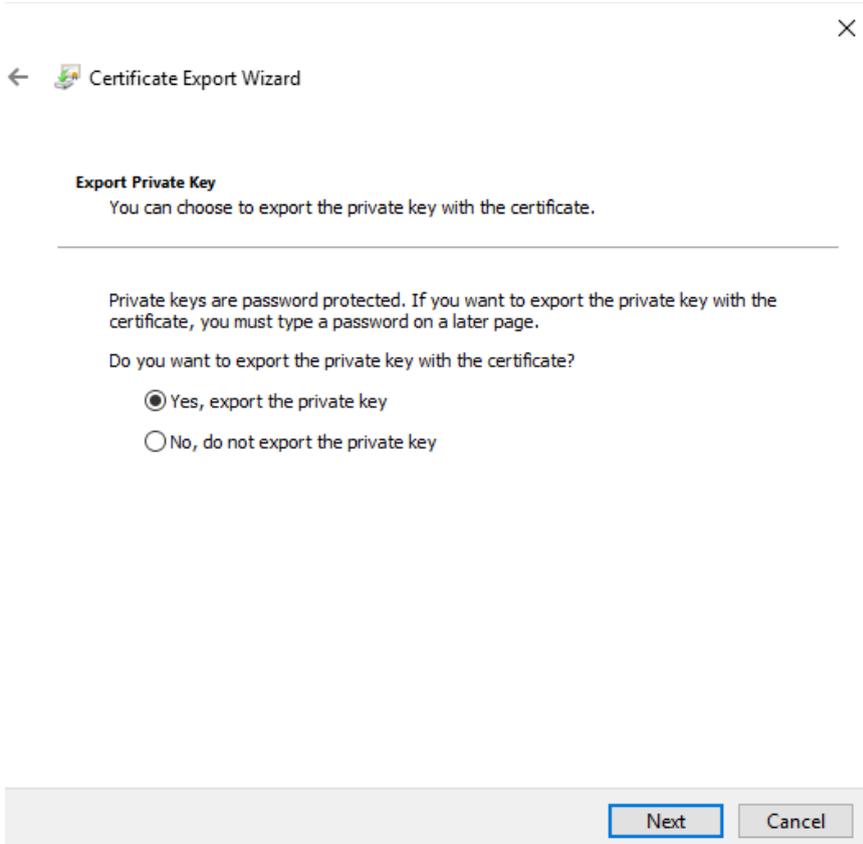
- To backup the private key of an existing certificate, expand “**Personal**” and select “**Certificates**”, select the certificate that you would like to make a backup, right-click and then select “**All Tasks**” > “**Export**”.



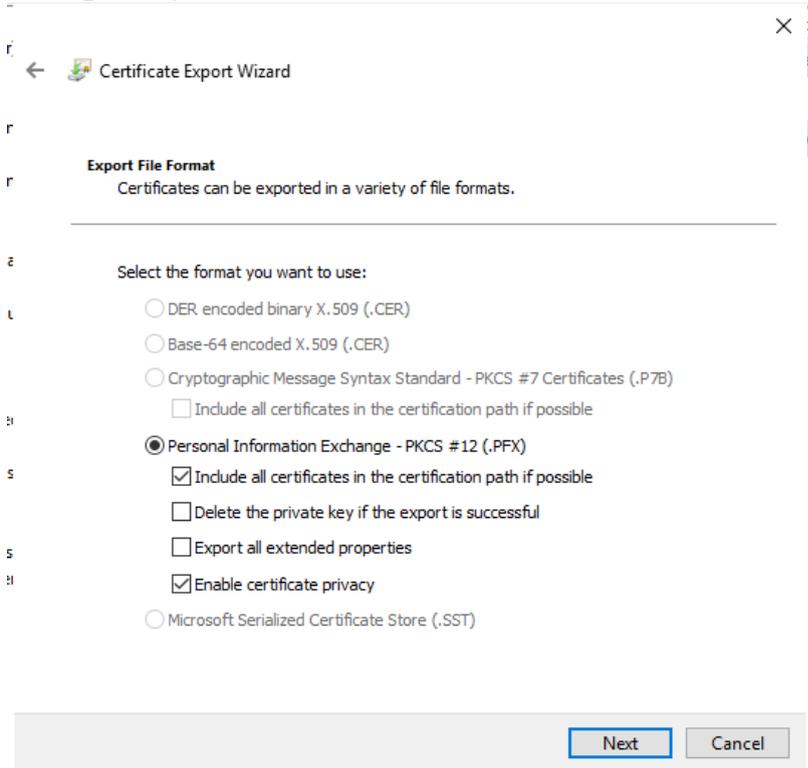
6. In Certificate Export Wizard, choose “Next”.



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

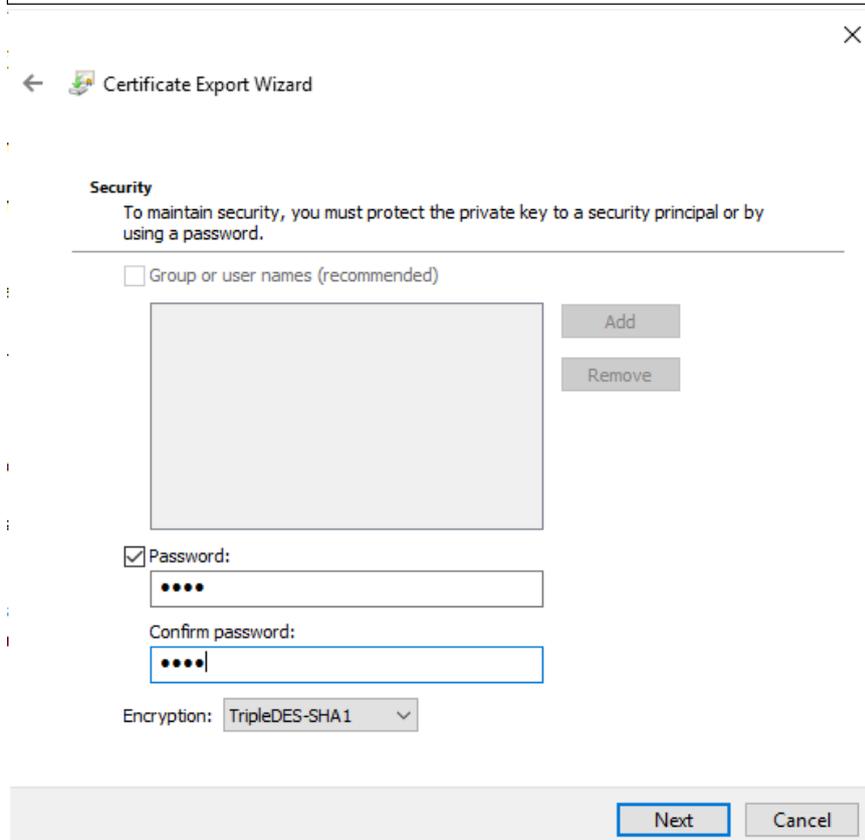


8. Select **“Personal Information Exchange - PKCS #12 (.PFX)”** and check the boxes **“Include all certificates in the certificate path if possible”** and **“Enable certificate privacy”** while leave the other boxes unchecked, and then click **“Next”**

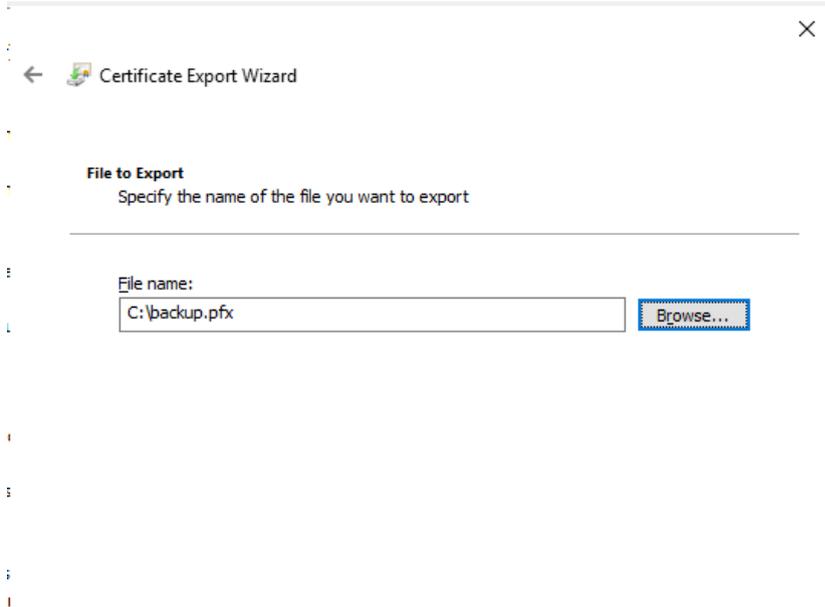


9. Type and confirm a password for the private key, and then click **“Next”**.

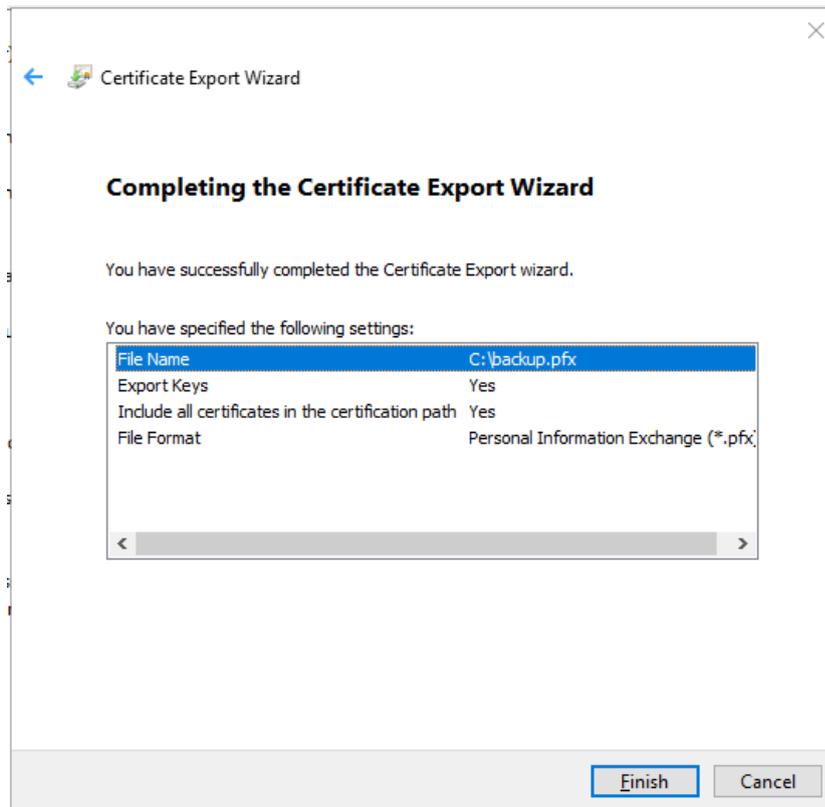
Note: It is very important that you remember this password. If you forget it, you will be unable to restore your private key.



- 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.)



- Click “**Finish**” to close the wizard.

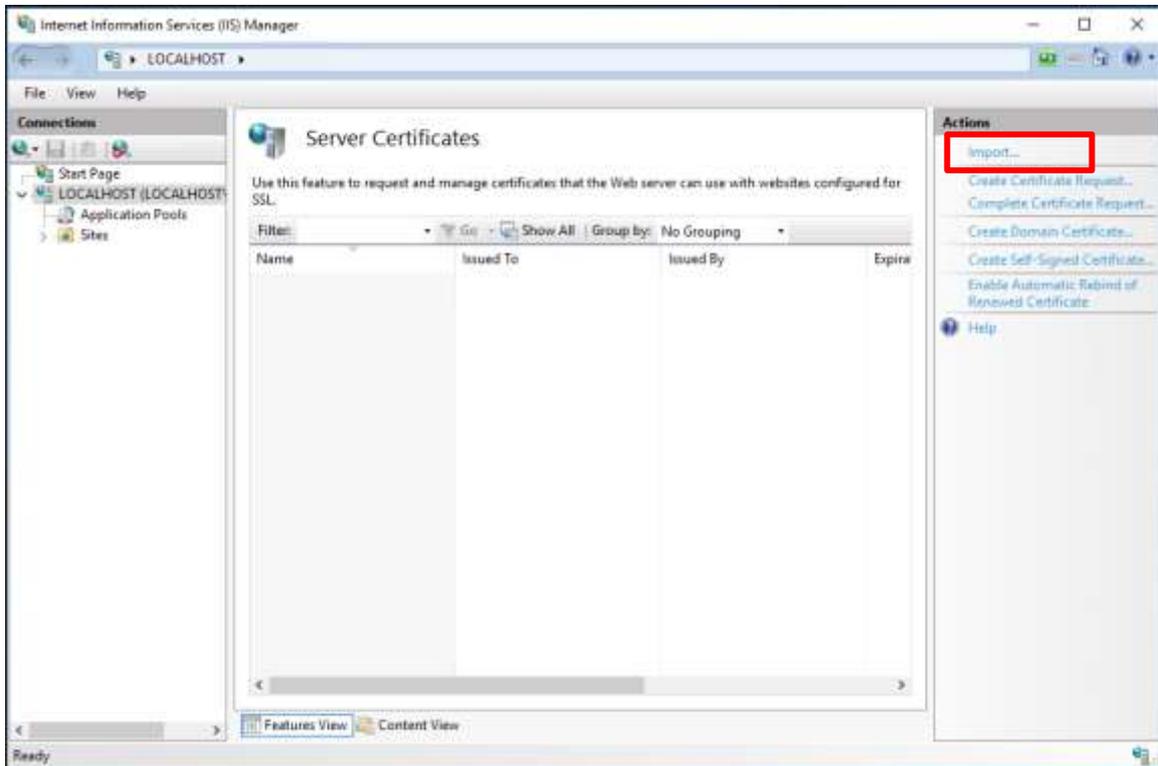


12. Click **“OK”** to complete



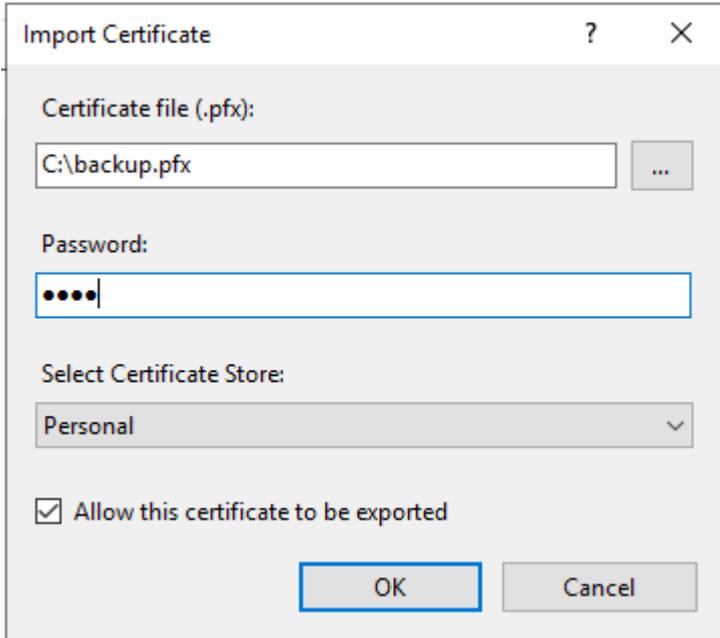
G. Restoring the Private key

1. Start menu, “**Administrative Tools**”, and click on “**Internet Information Services (IIS) Manager**”.
2. Select your web site, and then double-click “**Server Certificates**”.
3. At right column “**Actions**”, select “**Import**”



4. Enter the path and file name of the file containing the certificate, and password, then click “OK”.

Note: You may uncheck the box “Allow this certificate to be exported” to not allow the certificate to be exported. Or to allow you to back up or transport your certificate at a later time, you may check the box “Allow this certificate to be exported”.



5. “Hongkong Post e-Cert (Server)” certificate has been successfully restored.

