e-Cert (Server) User Guide

For Microsoft Exchange Server 2010

Revision Date: January 2026

Contents

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 Exchange Server 2010. 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 and Renew Application

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

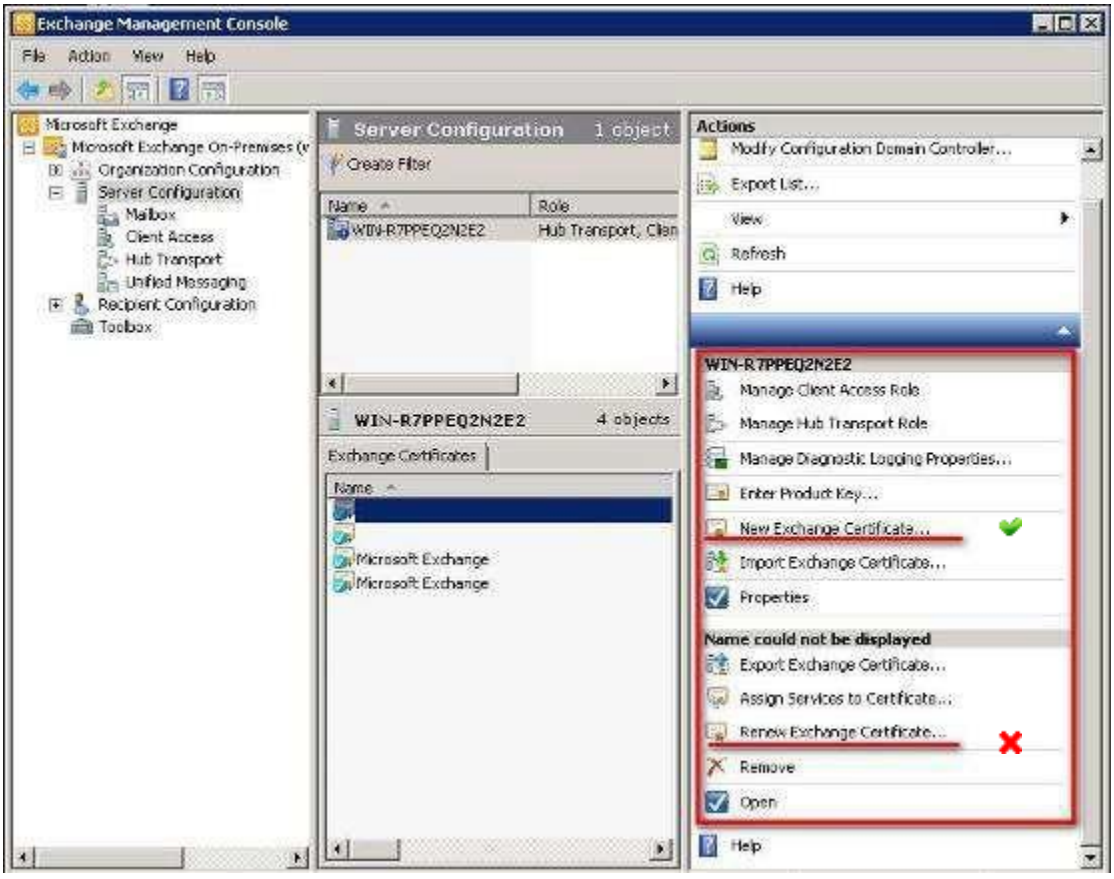
B. Generating Certificate Signing Request (CSR)

1 Start the **Exchange Management Console** by selecting **Start**, **All Programs**, **Microsoft Exchange Server 2010**, and then **Exchange Management Console**.

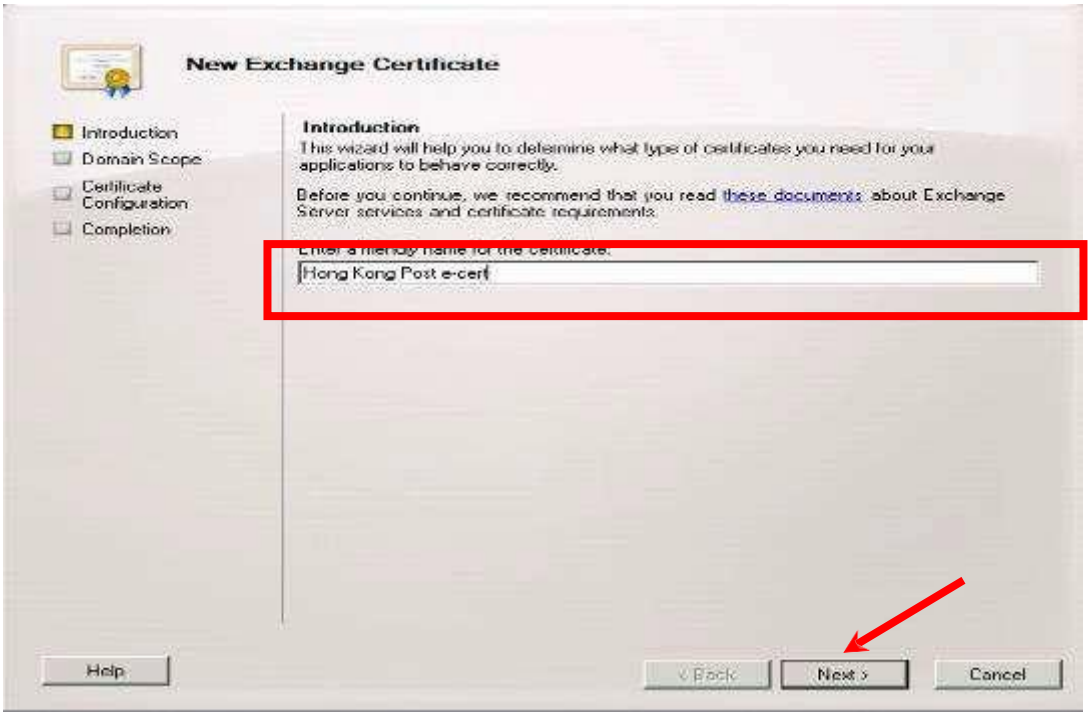
2 In Exchange Management Console, click + next to **Microsoft Exchange On-Premises** to expand the list of services.

3 Select **Server Configuration**, and then select **New Exchange Certificate** (in the right side of the screen).

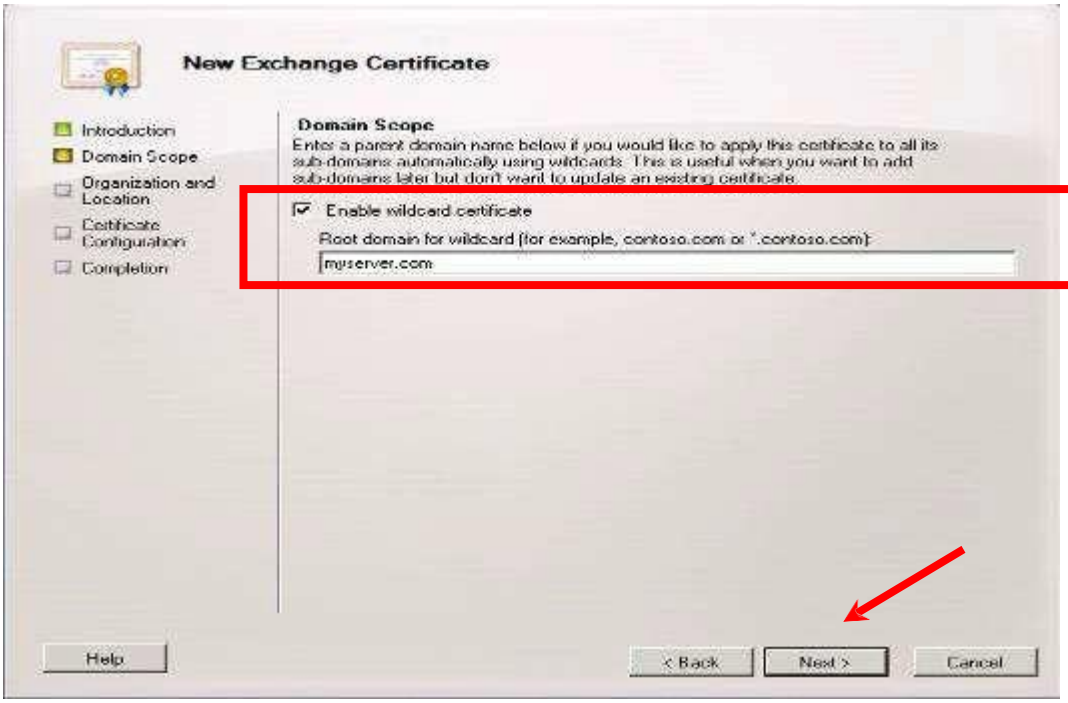
*Note : For renew of e-Cert (Server) application, please do not click "Renew" option to renew the certificate. Please click "**Create Certificate Request**" as the same procedures as new application for e-Cert (Server).*



4 Enter a friendly name to identify this certificate (e.g. Hong Kong Post e-cert), and then click **Next**.



5 In the Domain Scope section,



- If your CSR is for a wildcard certificate, select Enable wildcard certificate, enter the root domain name for your wildcard certificate, and then click **Next**. And directly follow step 6.

Note: *Please make sure that* ***root domain for wildcard*** *is filled with* ***Server Name with Wildcard*** *(both the names with or without wildcard component, i.e. the asterisk '*' are acceptable).*

- If your CSR is not for a wildcard certificate (both **Normal** and **Multi-domain** feature), click **Next** without selecting anything, and follow the 5.1 and 5.2.

5.1 In the Exchange Configuration section, select the services then click **Next**:

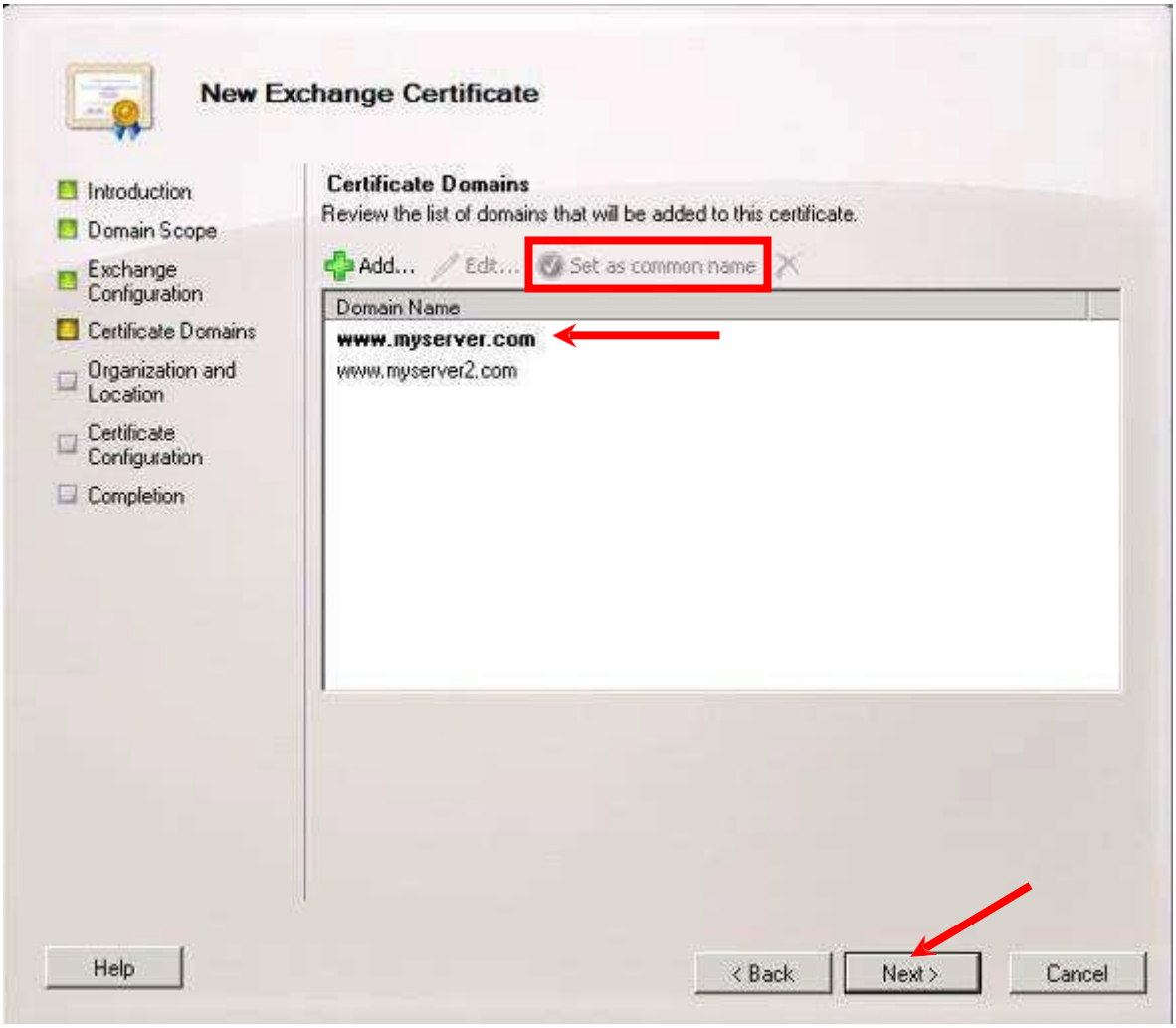
Note: *You need to know exactly how your server is configured to select the services you need to run, e.g. Client Access server (Outlook Web App).* ***This example is a multi-domain server certificate.***

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

Option 1: please input the domain name with "Server name used as Subject Name in the Certificate" being filled in the application form.

Option 2: please use IDN conversion tool to convert Chinese Domain Name into ASCII characters and input the converted name in the domain name field.

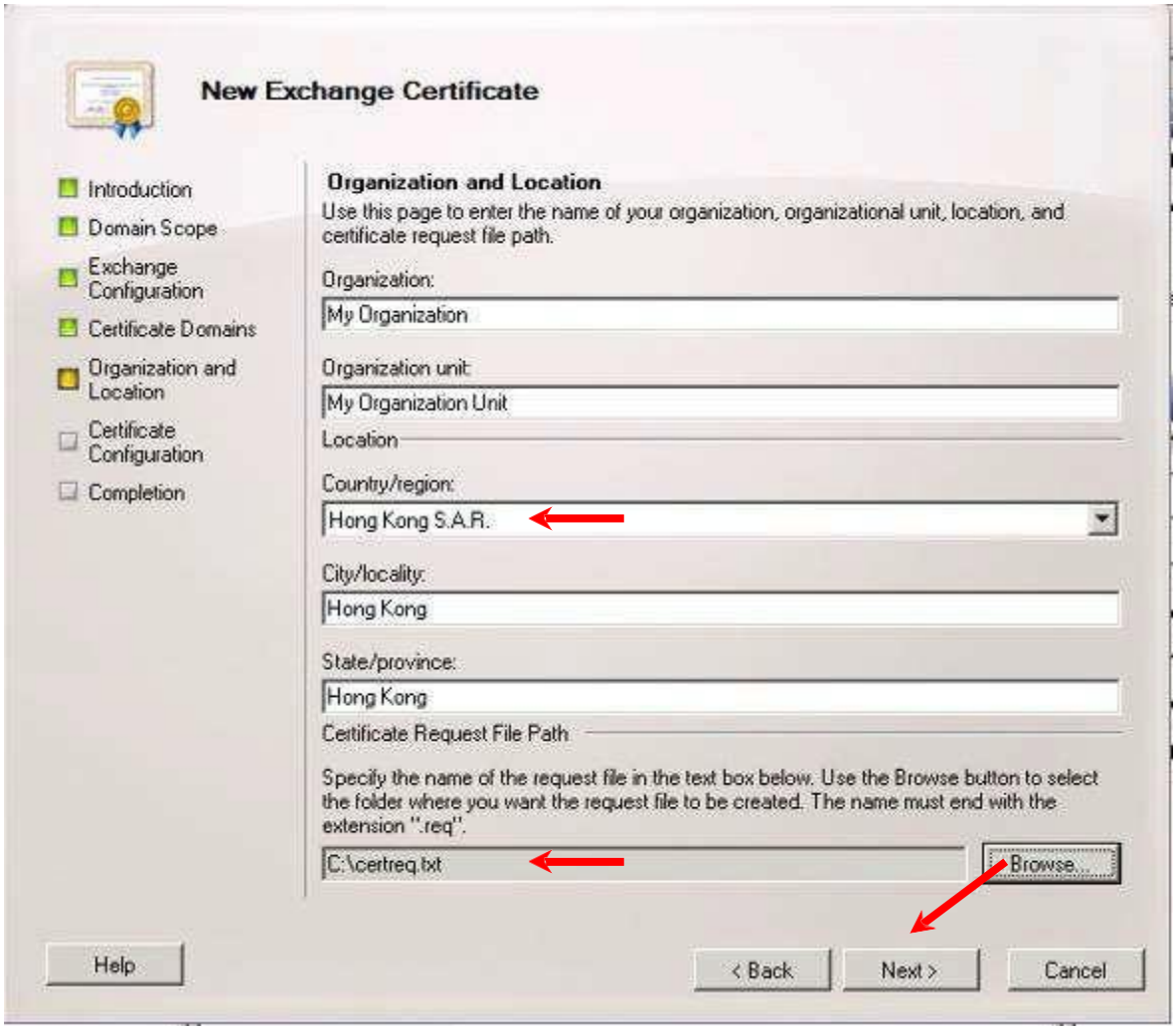
5.2 Select the **common name** (**Server name**), click **Set as common name**, and then click **Next**. (The bold name means the one set as common name)



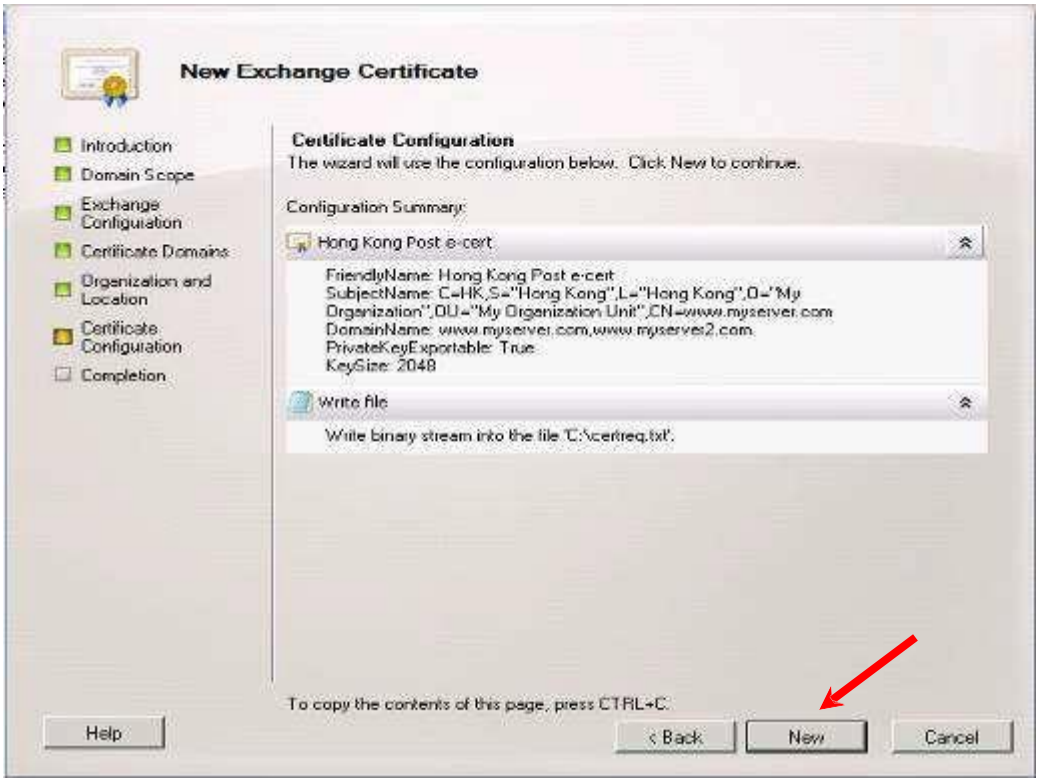
***NOTE: For application of e-Cert (Server) with Multi-domain feature or EV e-Cert (Server) with "Multi-domain" feature**, please set the common name as **Server name as Subject Name in the Certificate** being filled inthe application form.*

6 Complete your organization's name and your organizational unit, select HK (Hong Kong S.A.R.) for the Country/Region. Type Hong Kong for both State/province and City/locality, and then enter a file name and path for the certificate request, and then click **Next**.

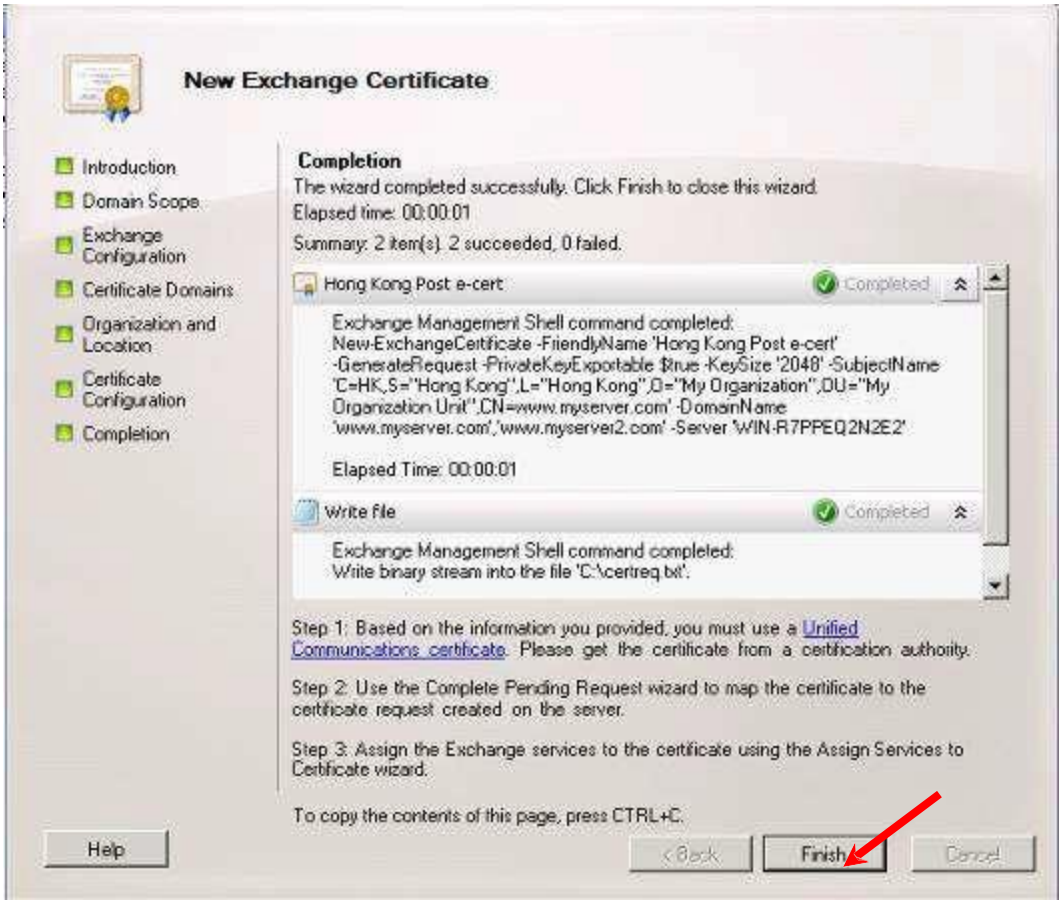
*Note: Please make sure that **Hong Kong S.A.R.** is in the **Country/Region** field.*



7 Check the detail information and click **New.**

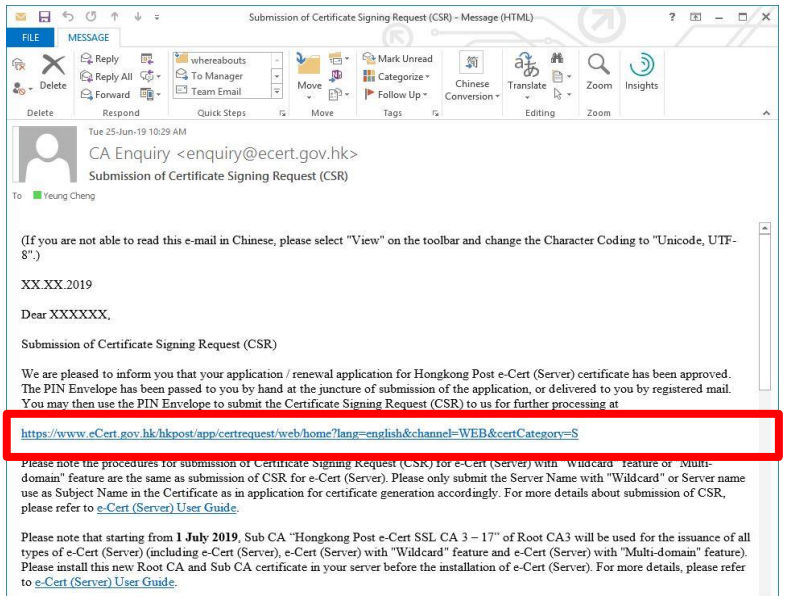


8 Click **Finish** to complete the procedure.

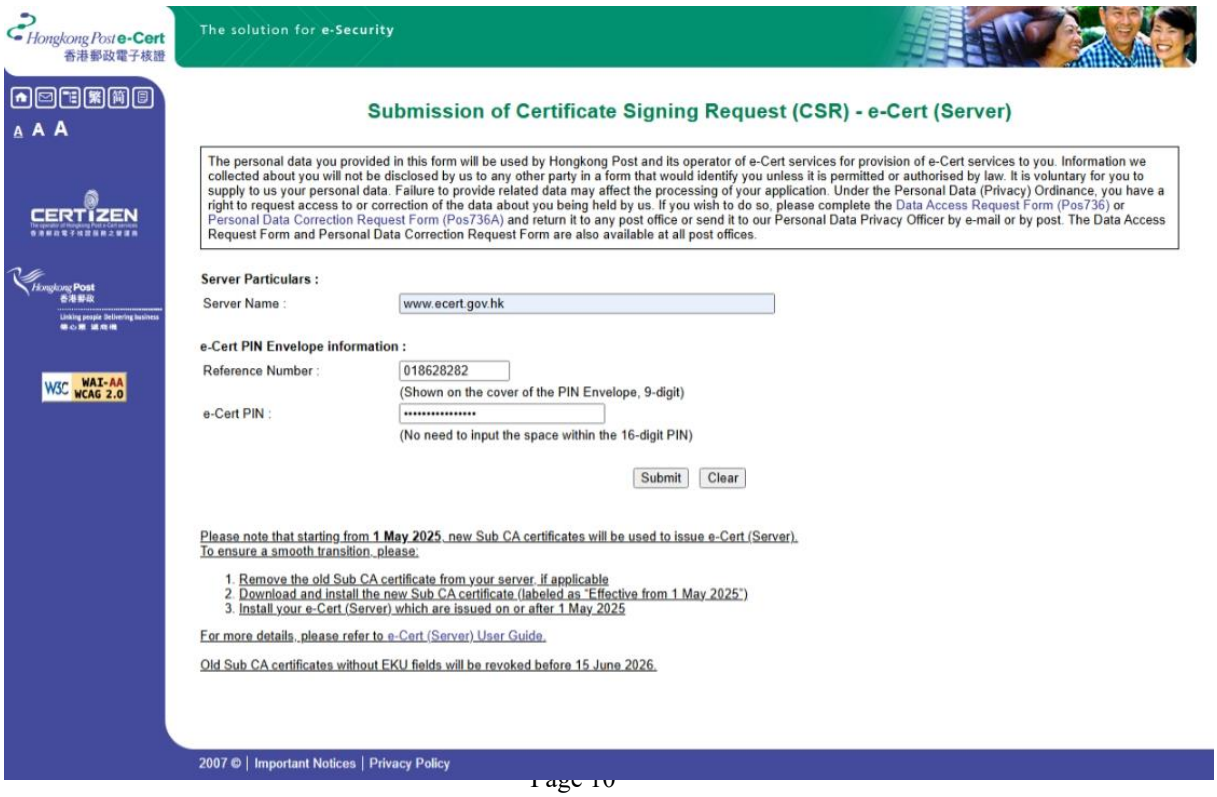


C. Submitting Certificate Signing Request (CSR)

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".



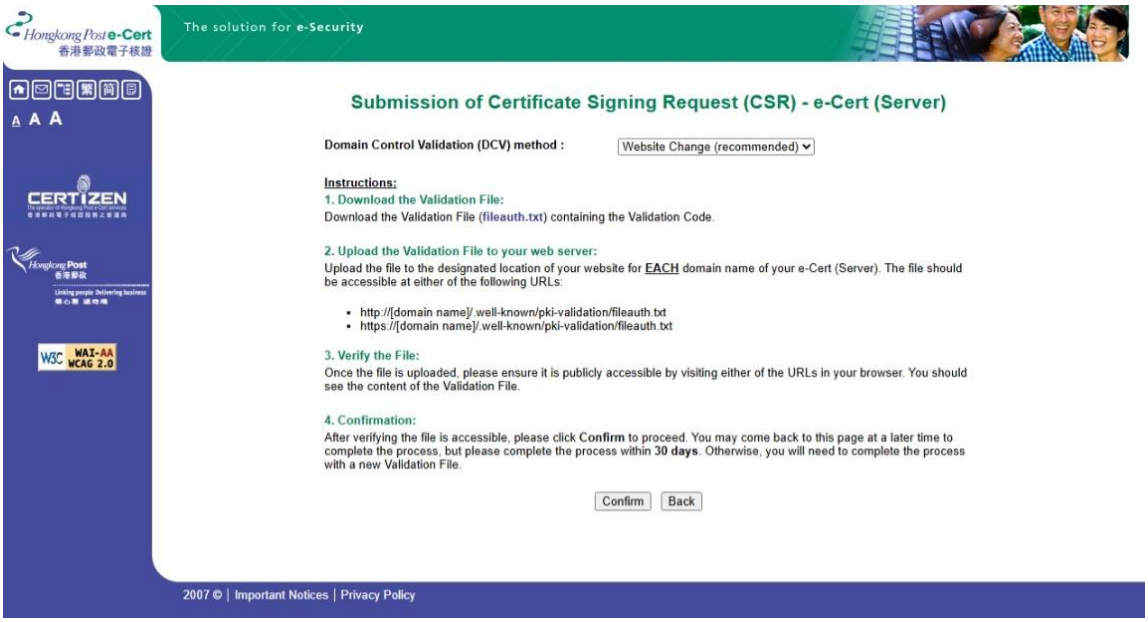
3. Click “Confirm” to confirm the application information. (If the information is incorrect, please contact Hongkong Post Certification Authority by email to enquiry@eCert.gov.hk.)

Note: If English and Chinese organisation name and/or branch name have been provided at the application form, in order to generate e-Cert (Server) with Chinese organisation name at Subject O field, click the button "Confirm Opt with Chinese" to proceed.

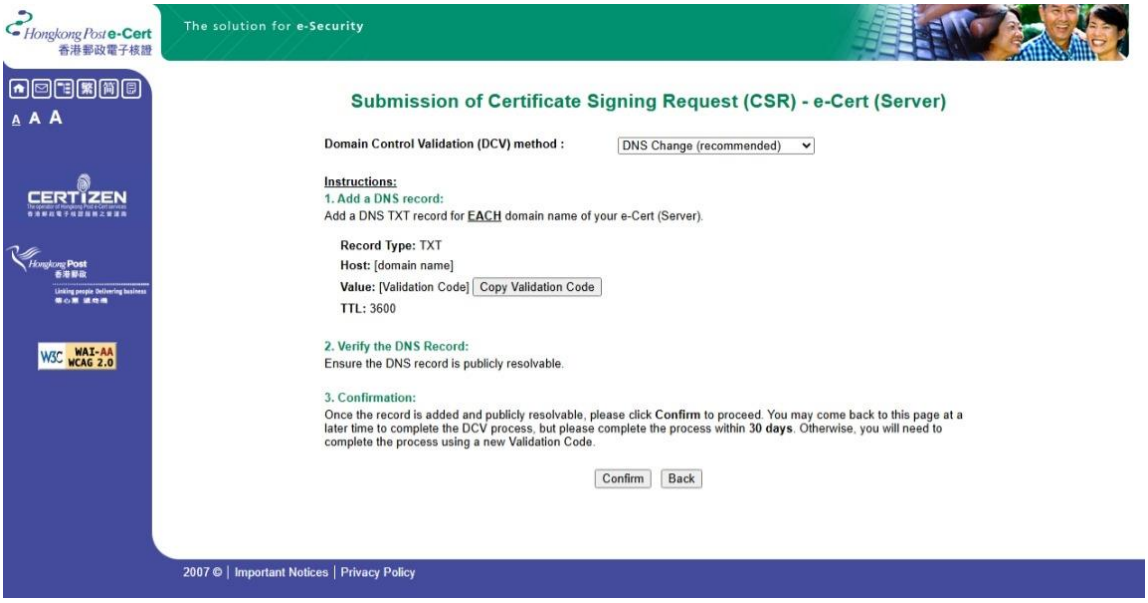
4. (**With effect <u>from 15 March 2026</u> and for <u>non-Government B/D subscribers</u> only**) Choose your desired Domain Control Validation (DCV) method from the list of applicable methods to your e-Cert (Server) and follow on-screen instructions to proceed. Once you confirm, the system will automatically verify and confirm your control over the domain name(s) of your e-Cert (Server). You will be allowed to submit your CSR if the DCV process is successful.

   (Please note that only applicable methods to your e-Cert (Server) type will be shown for selection.)

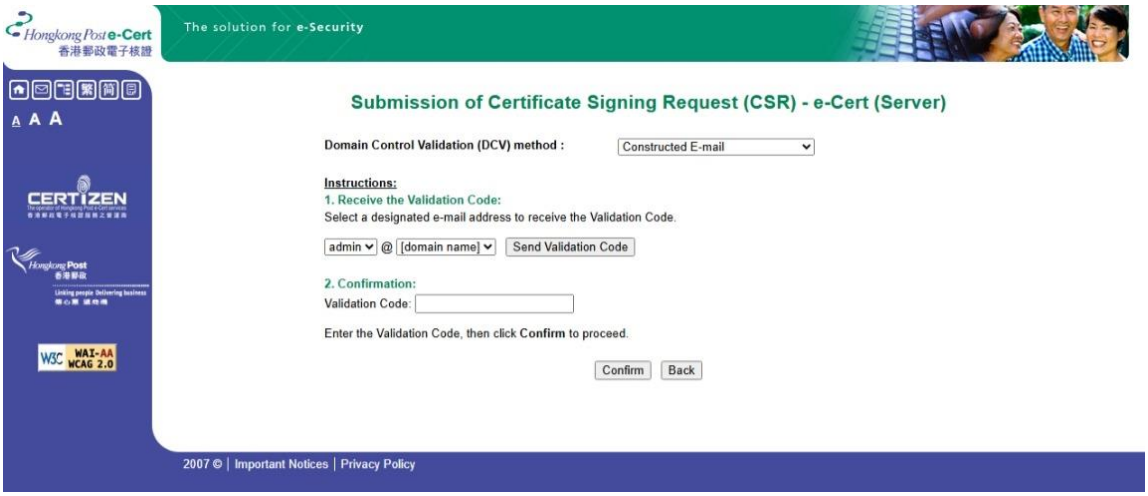
   A. For "Website Change" DCV method, download the Validation File "fileauth.txt" and upload the file to the designated location on your website for **<u>EACH</u>** domain name of your e-Cert (Server). Once the file is uploaded and publicly accessible, click "Confirm" to proceed. Please note that this method is NOT applicable to e-Cert (Server) with "Wildcard" feature.



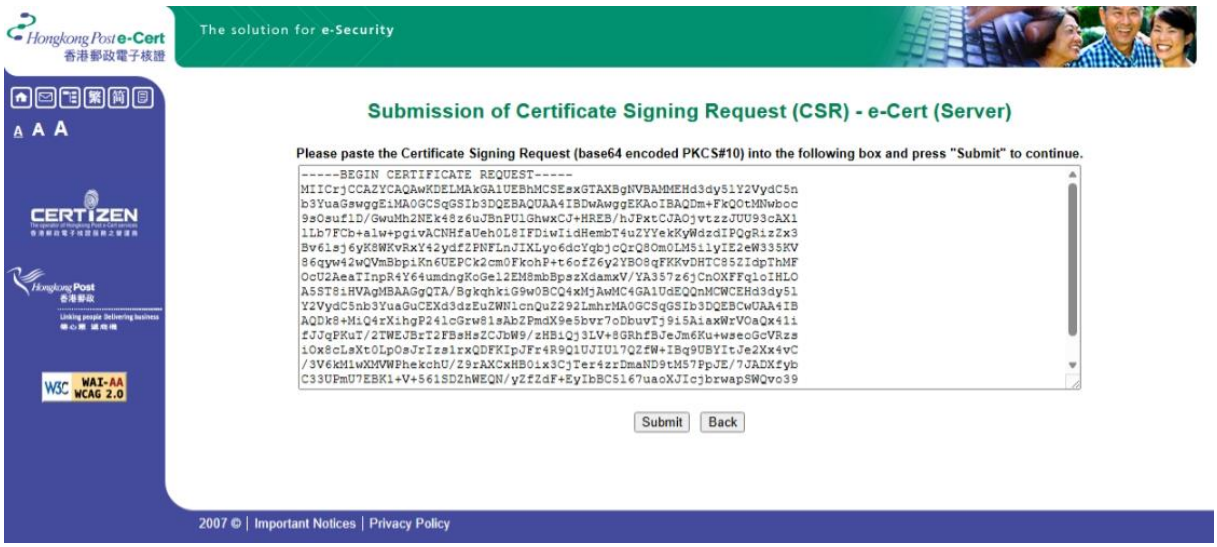
B. For "DNS Change" DCV method, add a DNS TXT record that includes the Validation Code for **EACH** domain name of your e-Cert (Server). Once the record(s) is/are added and publicly resolvable, click "Confirm" to proceed.



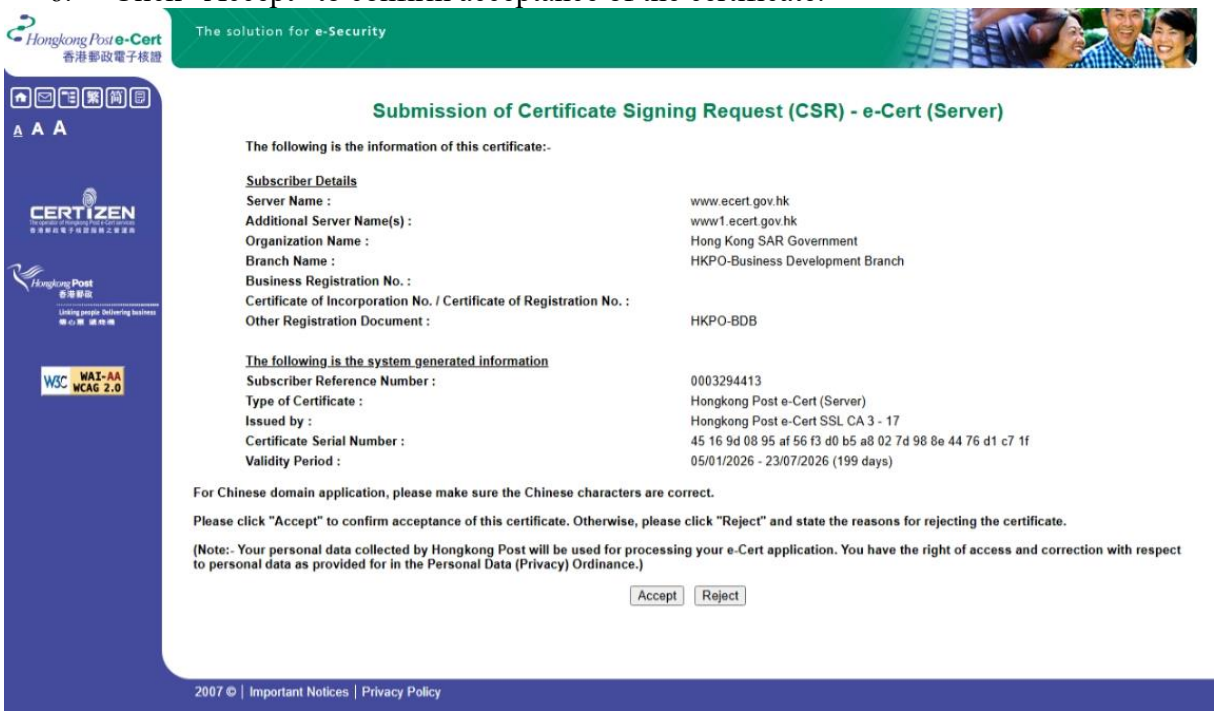
C. For "Constructed E-mail" DCV method, choose one of the designated e-mail addresses and click "Send Validation Code". Once you have received the e-mail, enter the Validation Code in the web page and click "Confirm" to proceed. Please note that this method is NOT applicable to e-Cert (Server) with "Multi-domain" feature.



5. Open the Certificate Signing Request (CSR) that you previously generated in Part B Step 2 with a text editor (e.g. Notepad) and copy the entire content including the lines "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----". Paste the content to the text box, and then click "Submit".



6. Click "Accept" to confirm acceptance of the certificate.



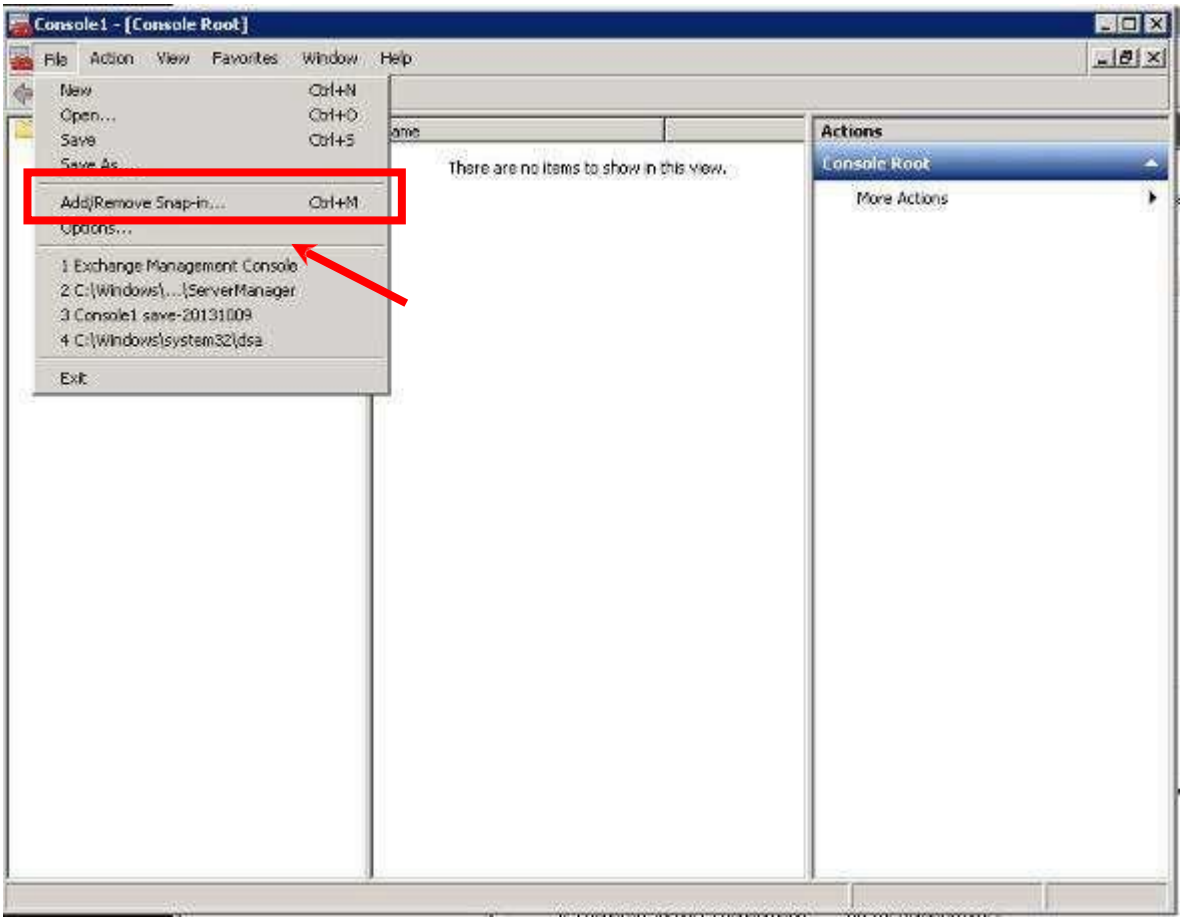
7. Click to download the Hongkong Post e-Cert (Server)

Note:

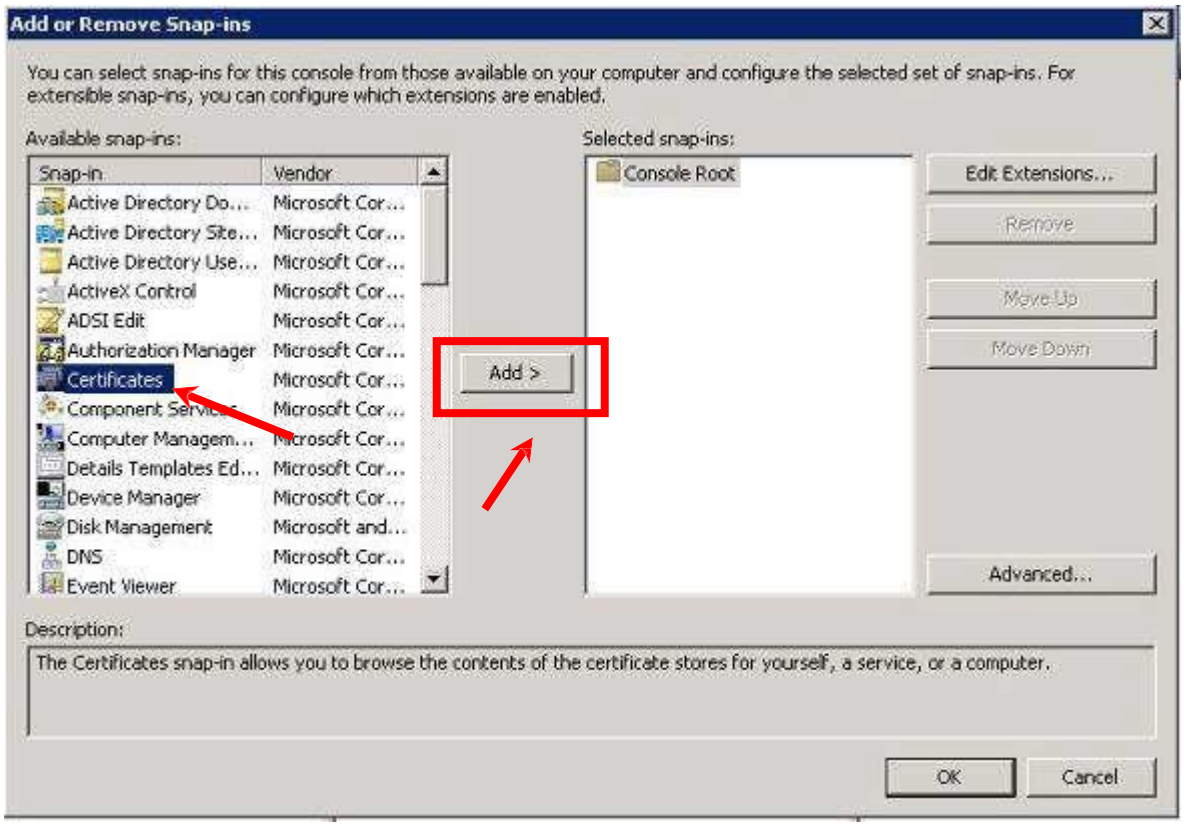
1. *You can also download your e-Cert (Server) from the Search and Download Certificate web page.*
   https://www.ecert.gov.hk/en/sc/index.html
2. *Install the Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" issued by Root CA3. Click the following link to download:*
   http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt
   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. *Install the Sub CA "Hongkong Post e-Cert EV SSL CA 3 - 17" issued by Root CA3. Click the following link to download:*
   http://www1.ecert.gov.hk/root/ecert_ev_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

D. Installing Sub CA / Cross Certificate

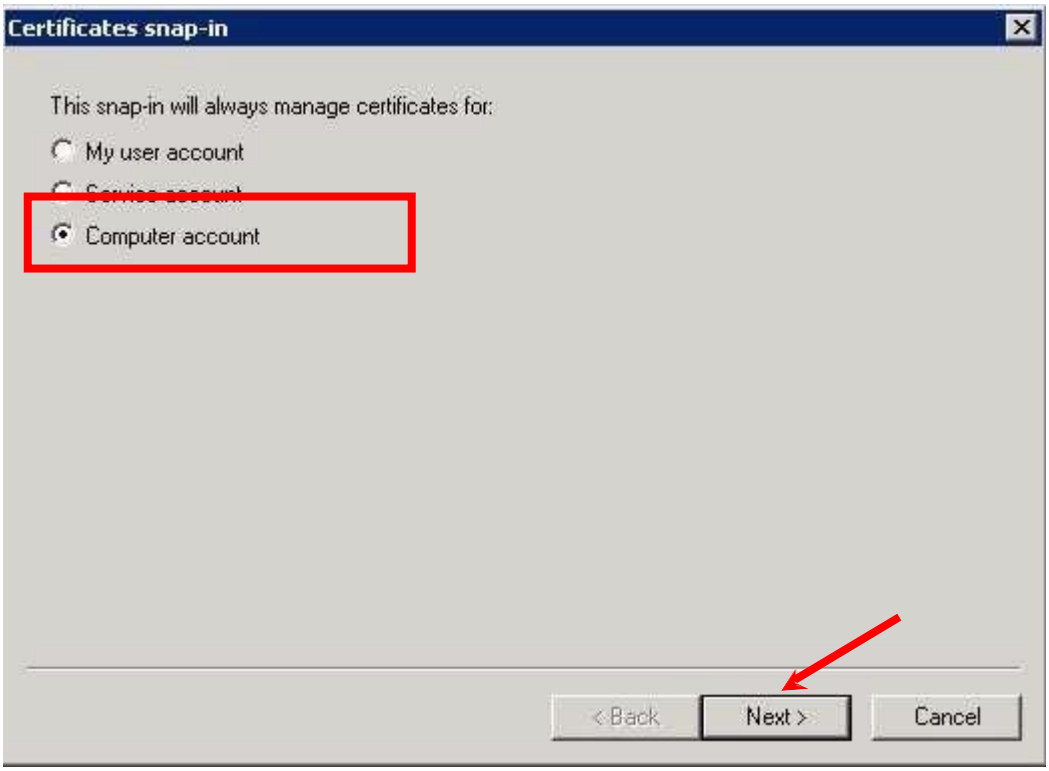
1. Start **Microsoft Management Console (MMC)** by clicking **Start > Run**, type **mmc** and click **OK**, and then select **Add/Remove Snap-in** from the **File** menu.



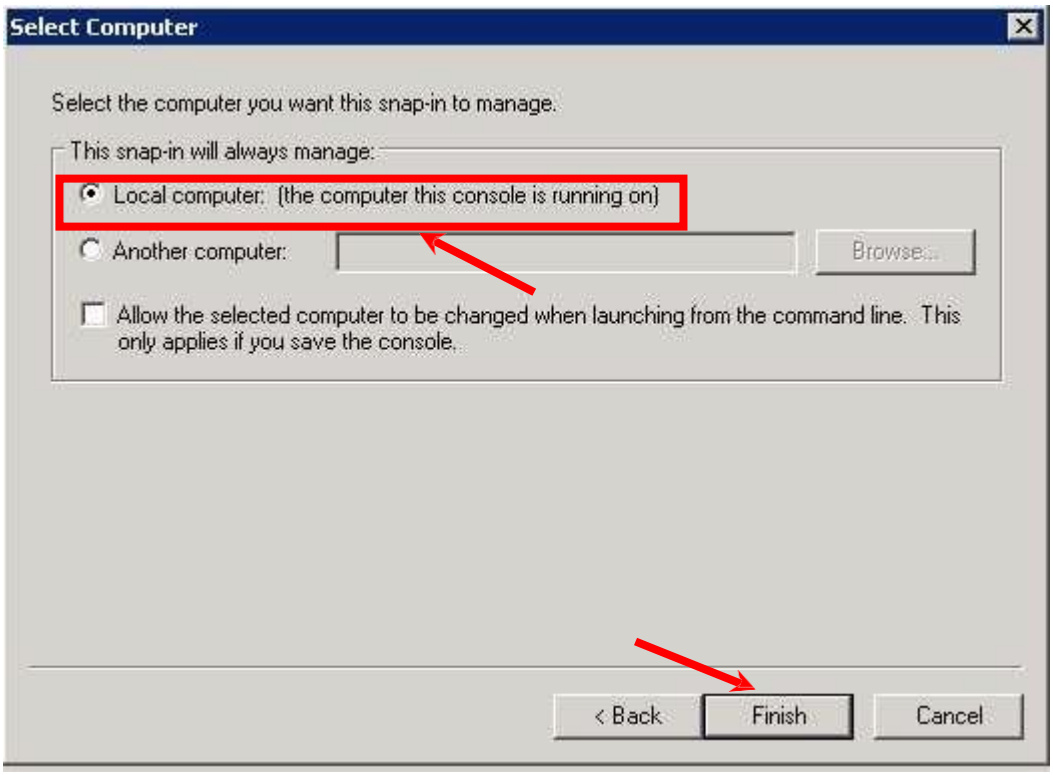
2. Select **Certificate** in **Available snap-in** then Click **Add**.



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



4. Select **Local computer**, and then click **Finish**, and then click **OK**.

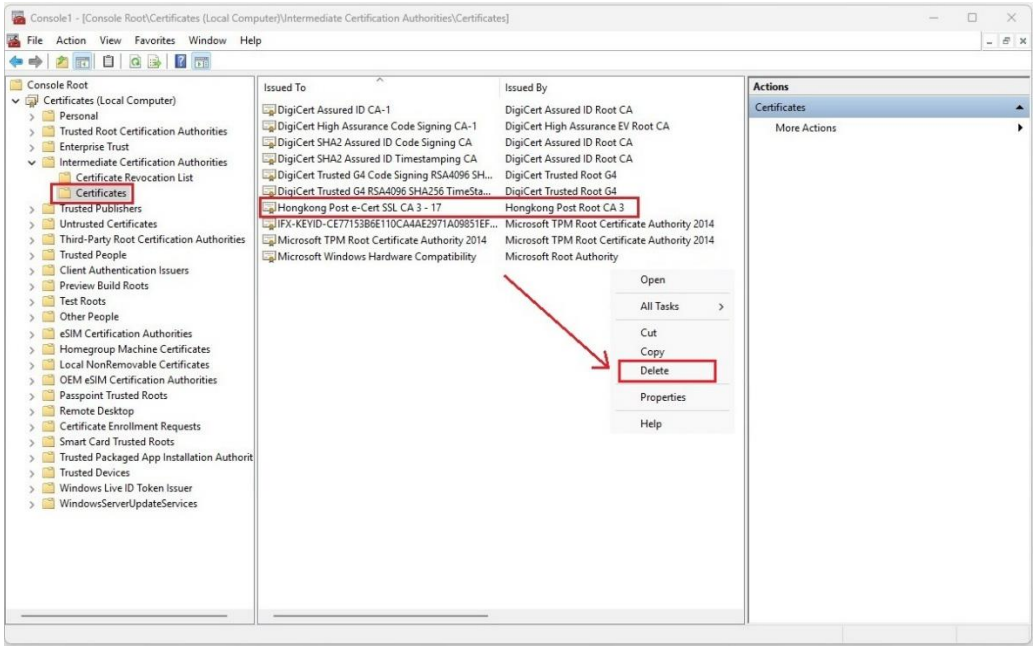


The following uses the "**Hongkong Post e-Cert SSL CA 3 - 17**" Sub CA certificate as example.

> ***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****.*

Removing the old Sub CA Certificate (if applicable)

Expand the "Intermediate Certification Authorities" and select "Certificates", right click the old "Hongkong Post e-Cert SSL CA3 - 17" and select "Delete".

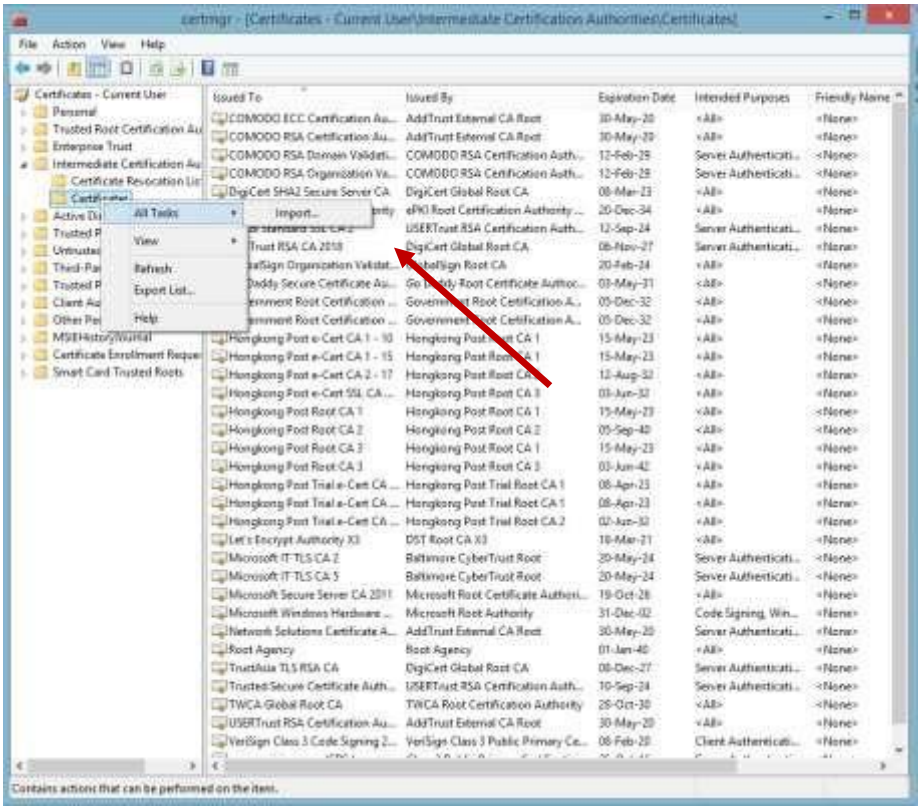


Click "Yes" to delete.

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

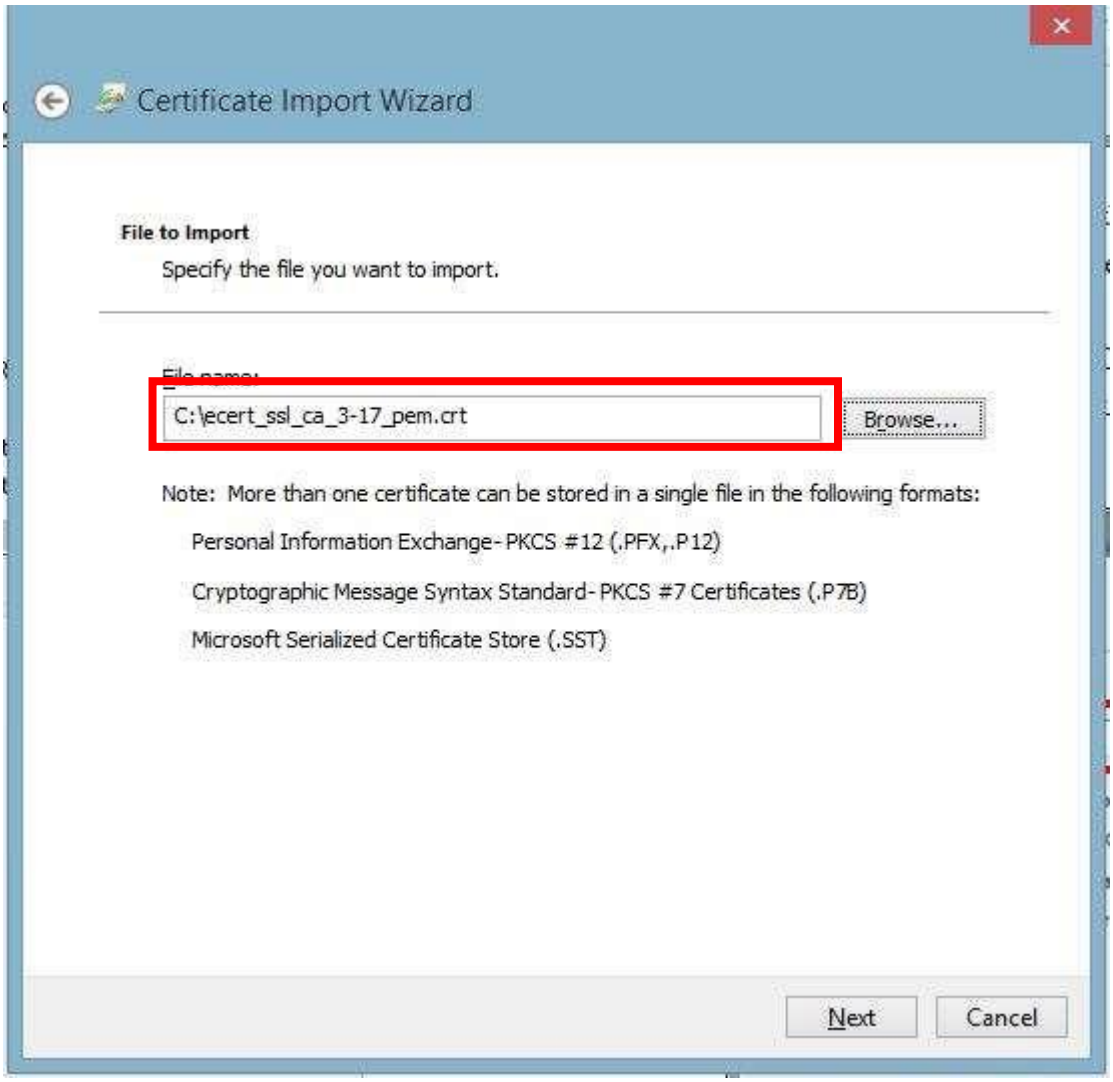
Installing Sub CA / Cross Certificate

5. Expand the **Certificates (Local Computer)** node, then right-click the **Intermediate Certification Authorities** and then select **All Tasks > Import**.

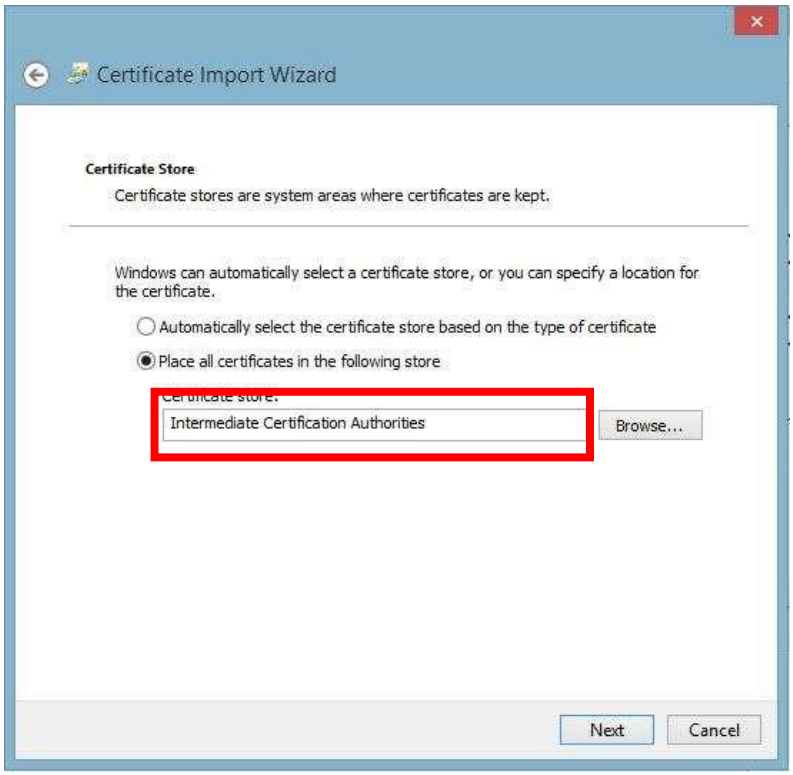


6. In the **Certificate Import Wizard**, click **Next** to continue.

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**, and choose **Intermediate Certification Authorities**, click **Next**.



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

10. Click **OK** to complete.

The **Hongkong Post e-Cert SSL CA 3 - 17** should now have been imported to the **Intermediate Certification Authorities > Certificates**.

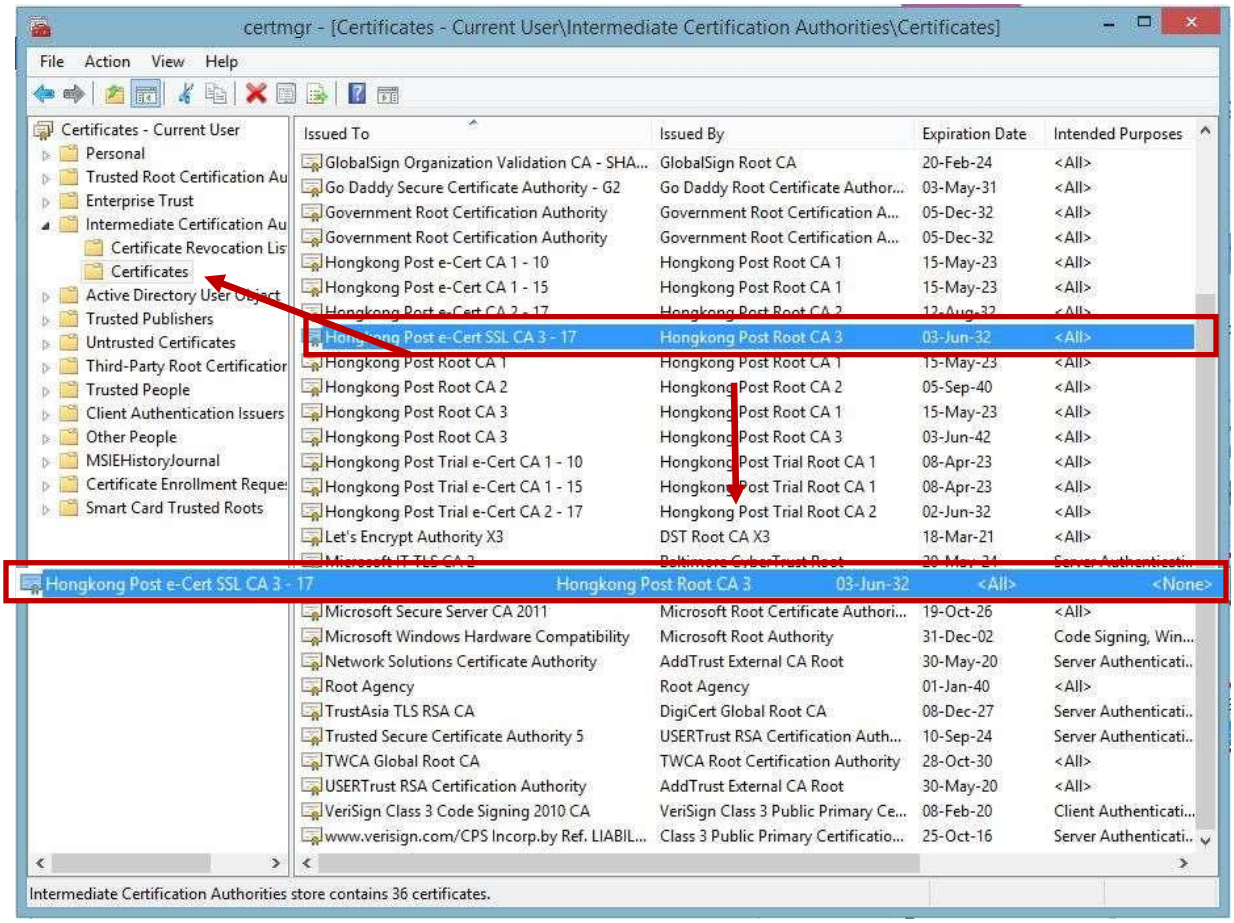


Figure 1: **Hongkong Post e-Cert SSL CA 3 - 17** certificate has been successfully installed

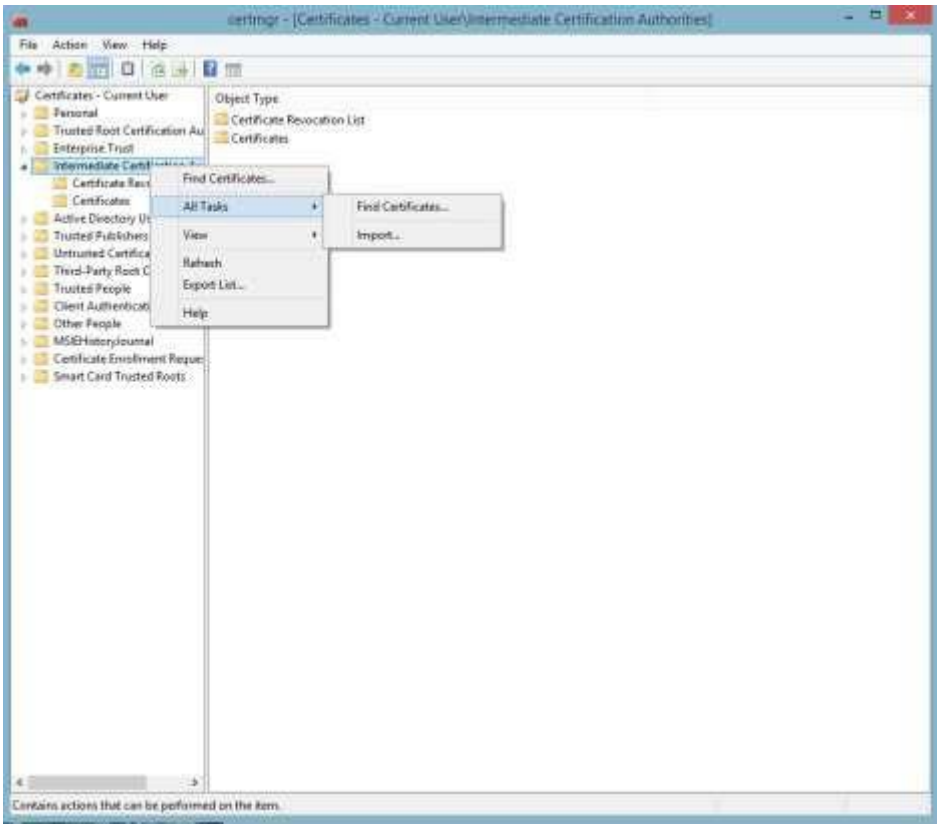
Repeat step 5 to step 10 for installation of cross-cert (root_ca_3_x_gsca_r3_pem.crt) which was downloaded in Section C step 7.

Installing Authority Revocation List (ARL)

11. Download the **Hongkong Post Authority Revocation List (ARL)** at:

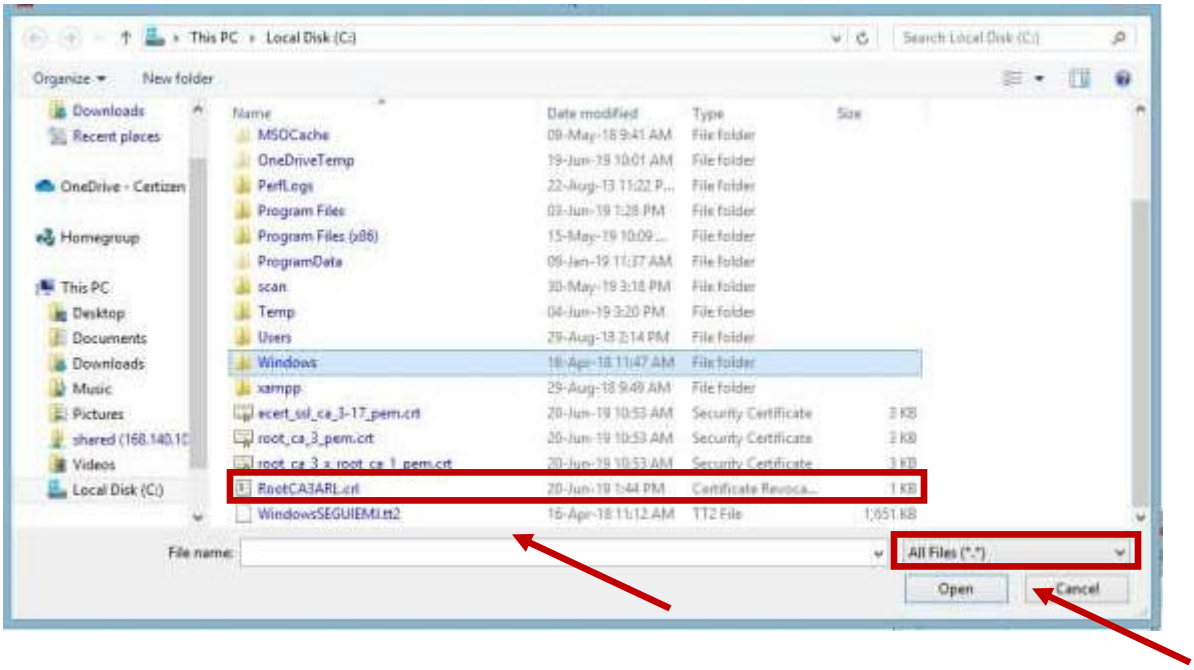
    http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl

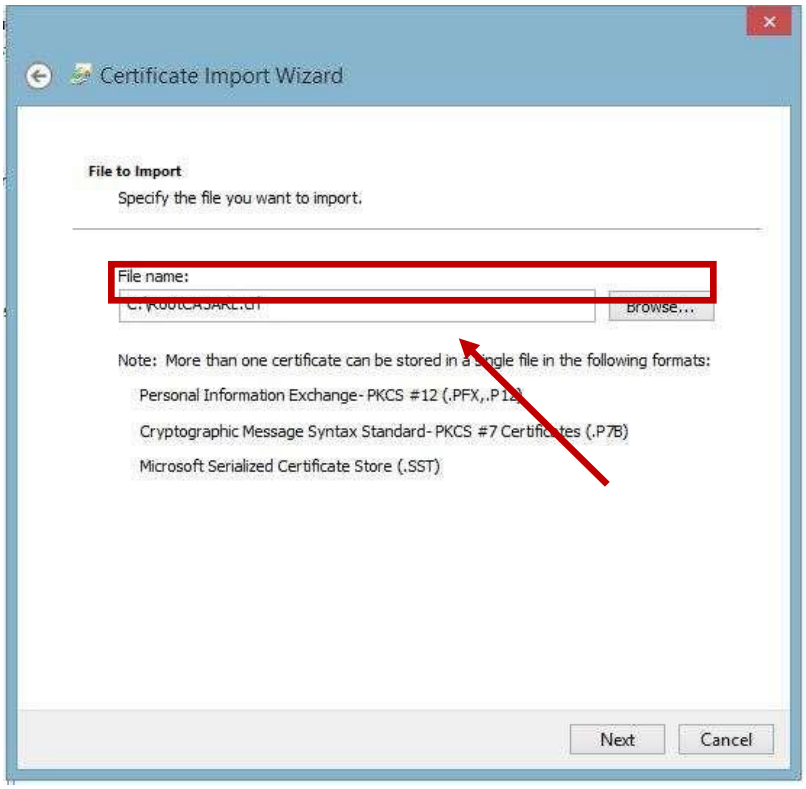
12. Expand the **Certificates (Local Computer)** node, then right-click choose the **Intermediate Certification Authorities**, and then select **All Tasks > Import**.



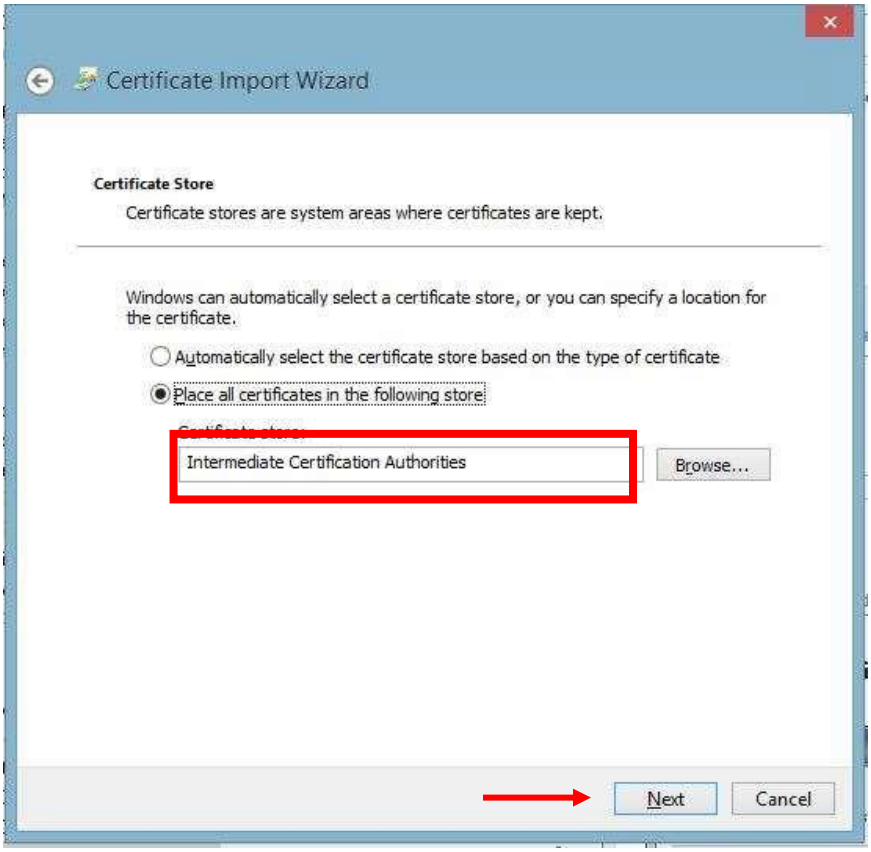
13. In the **Certificate Import Wizard**, click **Next** to continue.

14. Click **Browse** to locate the **Hongkong Post Authority Revocation List (ARL)** that you downloaded before in Step 11 (RootCA3ARL.crl), and then click **Next**. (Tip: choose **All Files**)

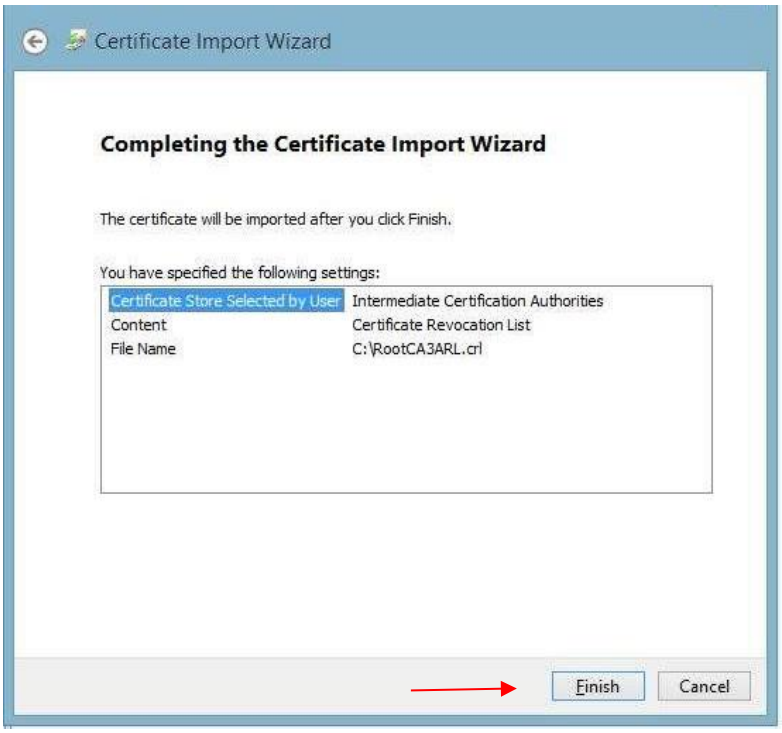




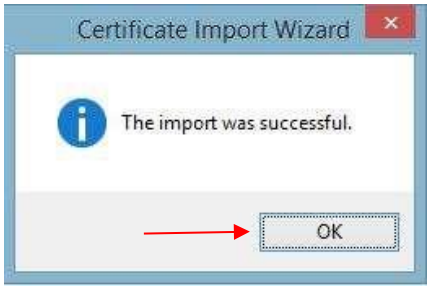
15. Select **Place all certificates in the following store** and choose **Intermediate Certification Authorities**, click **Next**.



16. Click **Finish** to close the wizard.



17. Click **OK** to complete.



The **ARL** should now have been imported to the **Intermediate Certification Authorities > Certificate Revocation List**.

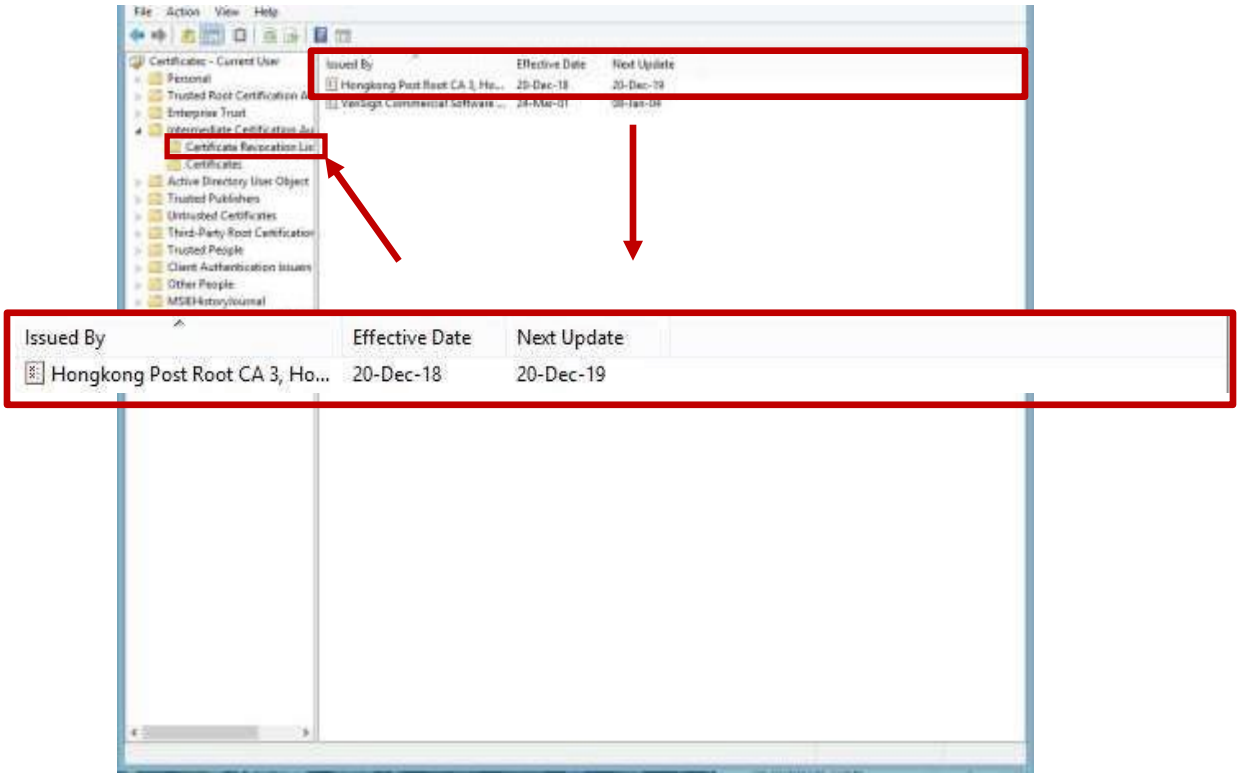
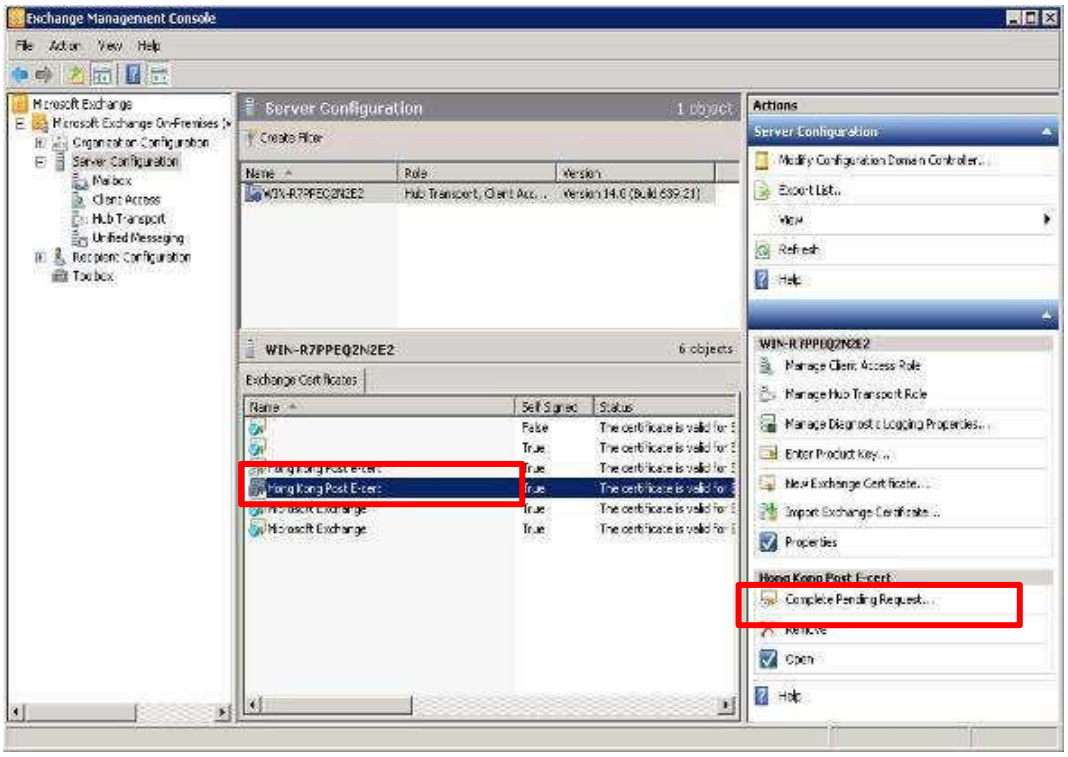


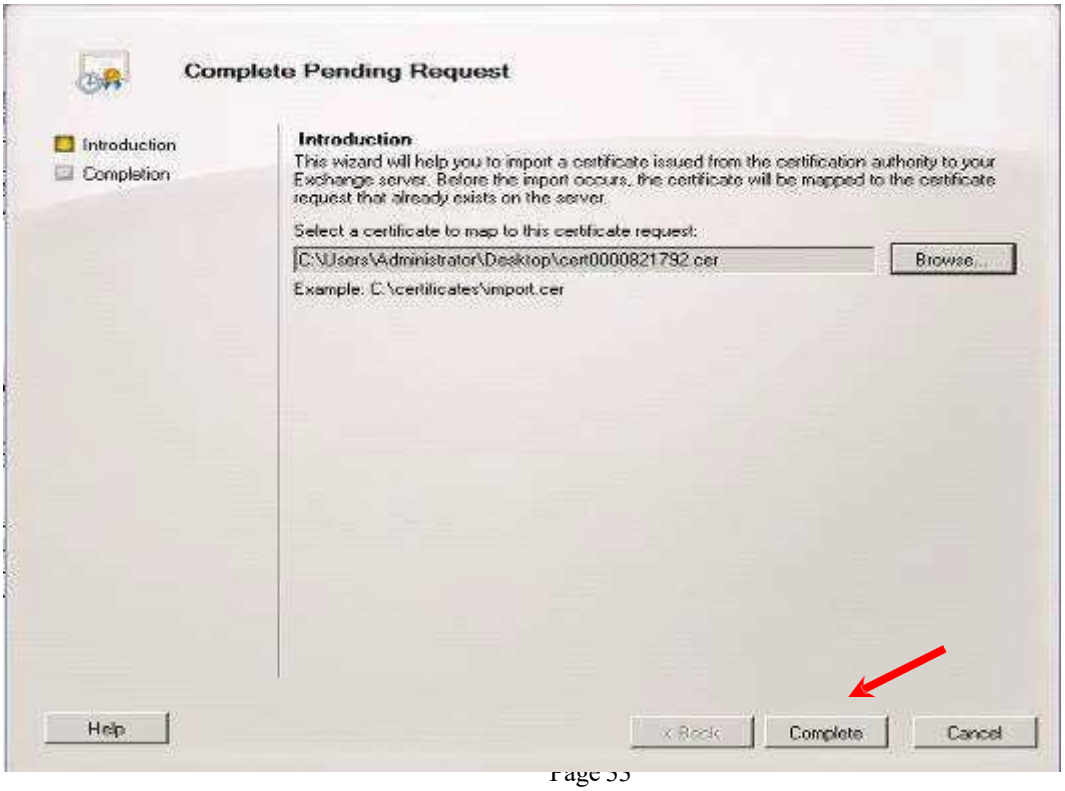
Figure 3: **Hongkong Post Authority Revocation List (ARL)** certificate has been successfully installed

E. Installing Server Certificate

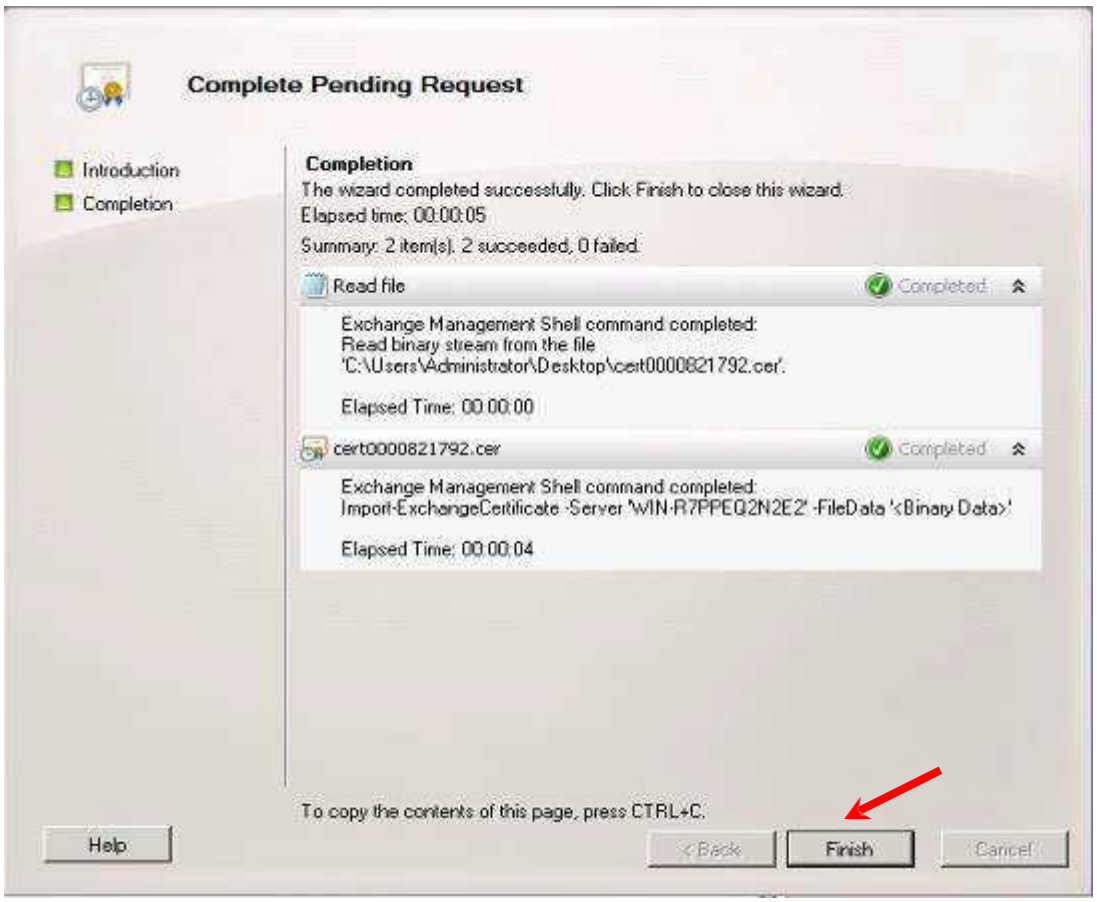
1. In **Exchange Management Console**, select **Server Configuration** by expanding the **Microsoft Exchange On-Premises**. Click the certificate you added before and choose **Complete Pending Request** from the right side of the window.



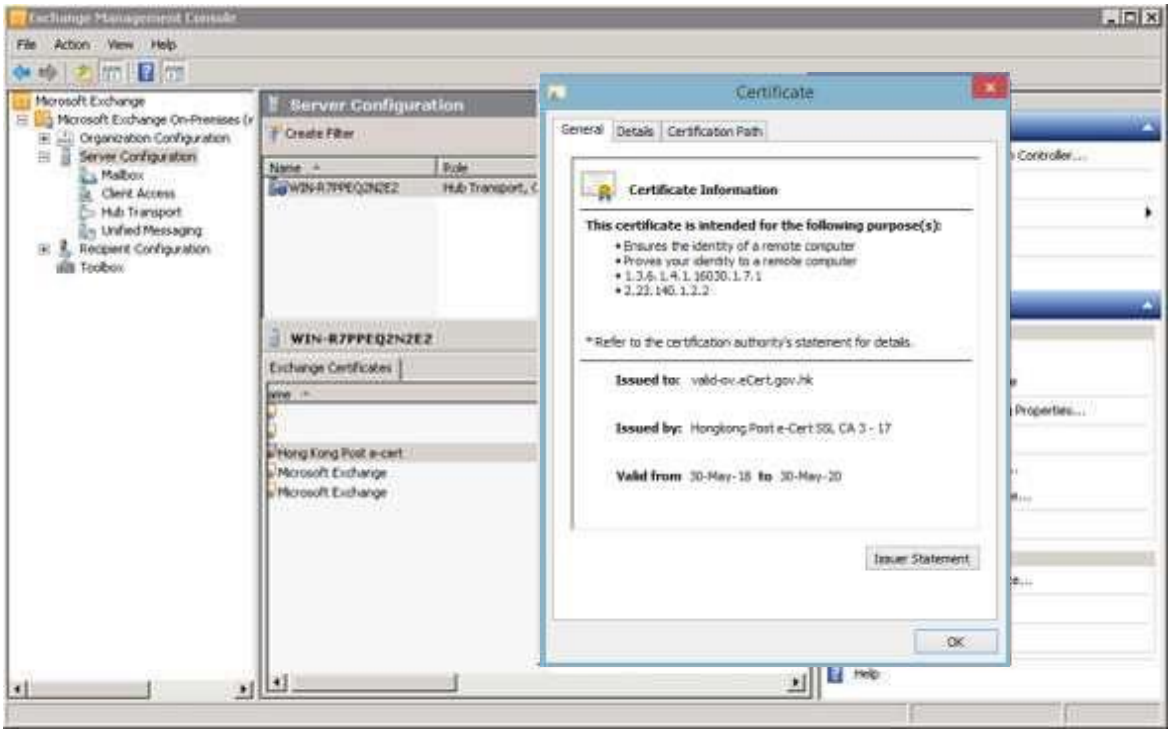
2. Click **Browse** to locate the **Hongkong Post e-Cert (Server)** certificate that you downloaded in Part C Step 7, click **Complete**.



3. Click **Finish** to complete the installation.

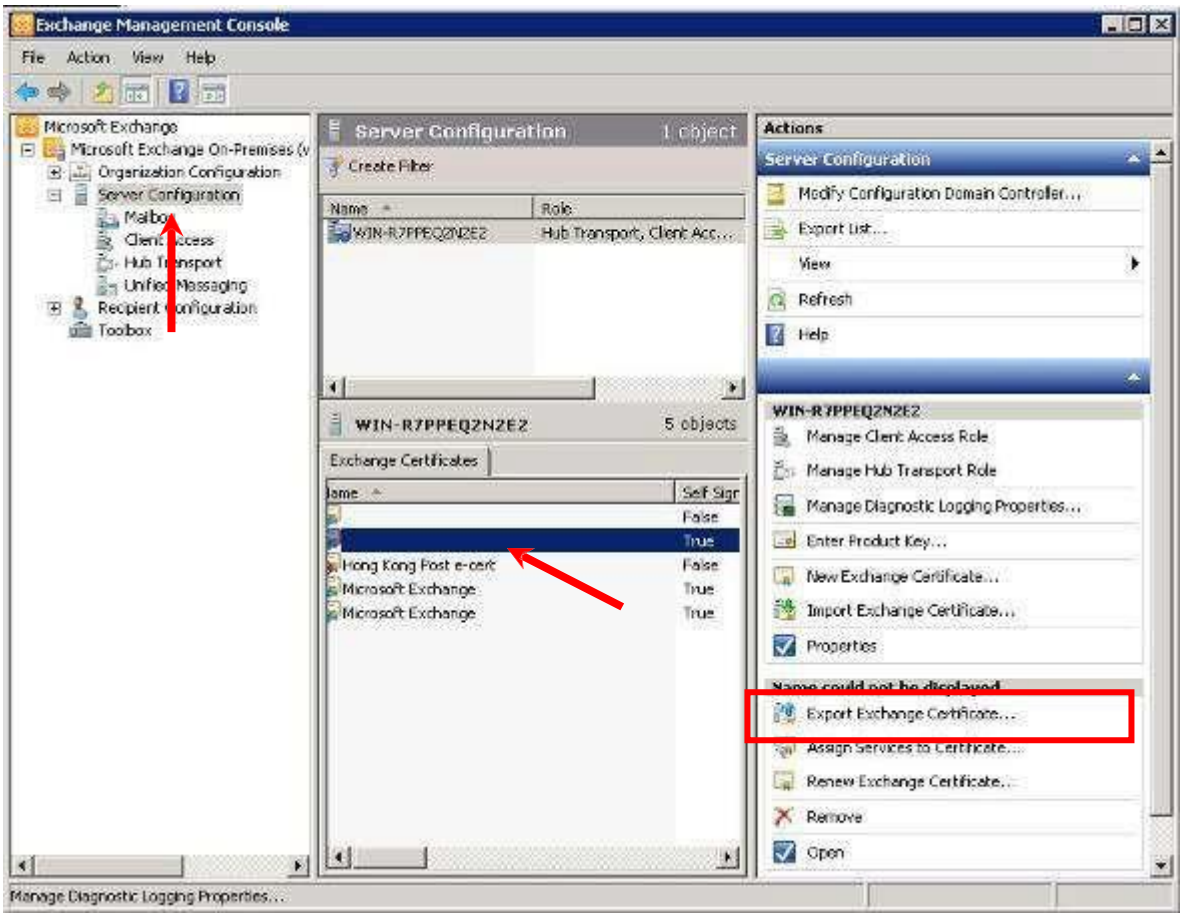


4. **Hongkong Post e-Cert (Server)** certificate has been successfully installed. You can check the detail information by double-clicking the certificate.

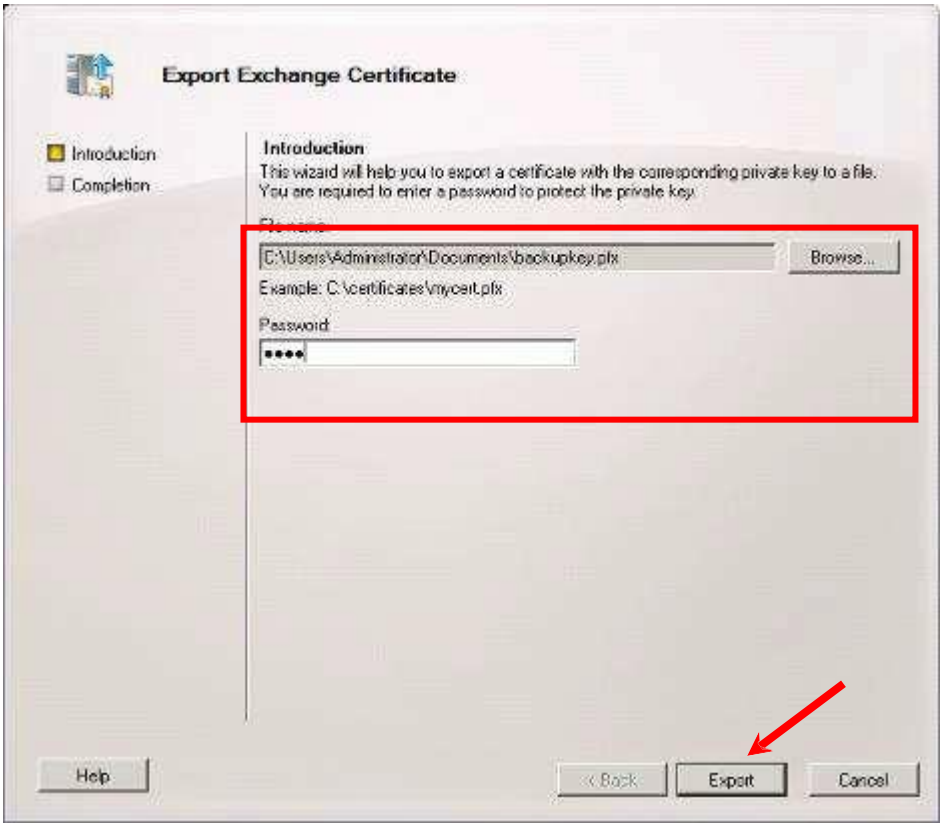


F. Backing up the Private Key

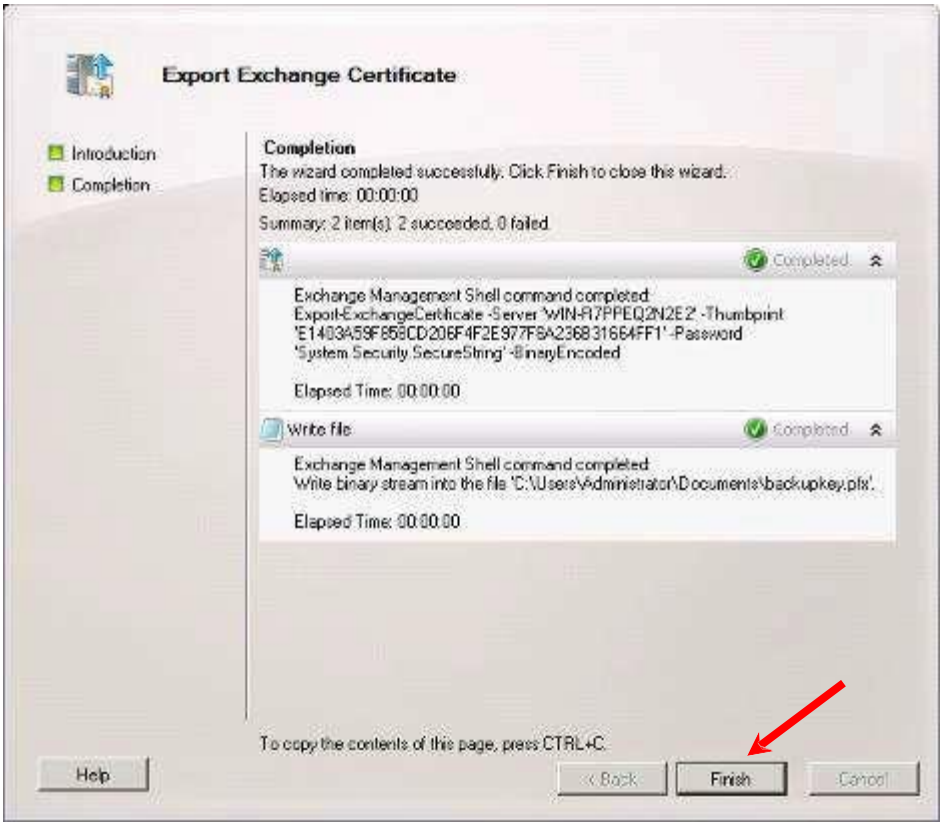
1. In **Exchange Management Console**, choose the certificate that you intend to export, and then click **Export Exchange Certificate**.



2. Specify the name of the file you intend to export, and type in the password. Then click **Export**. (By default, the file will be saved with a .PFX extension.)

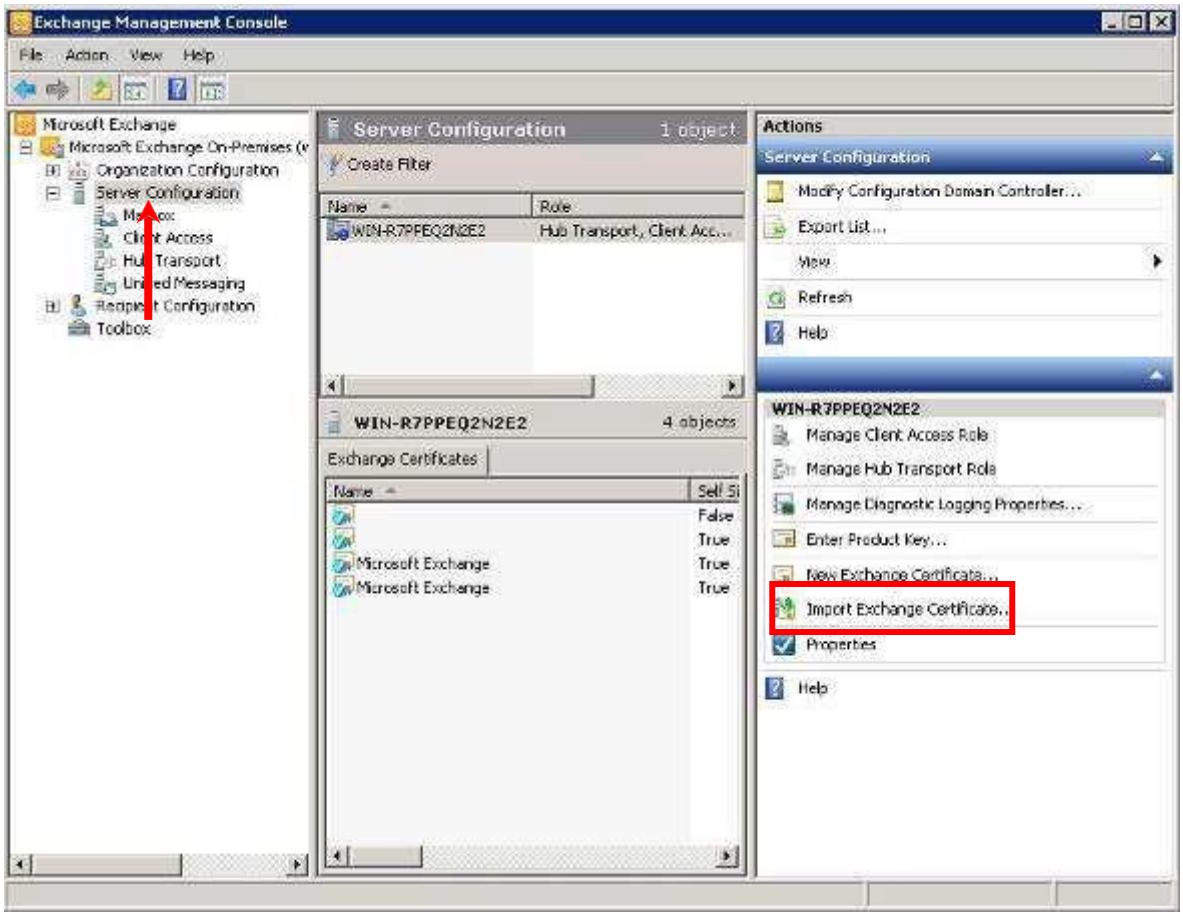


3. Click **Finish.** **Hongkong Post e-Cert (Server)** has been successful exported.

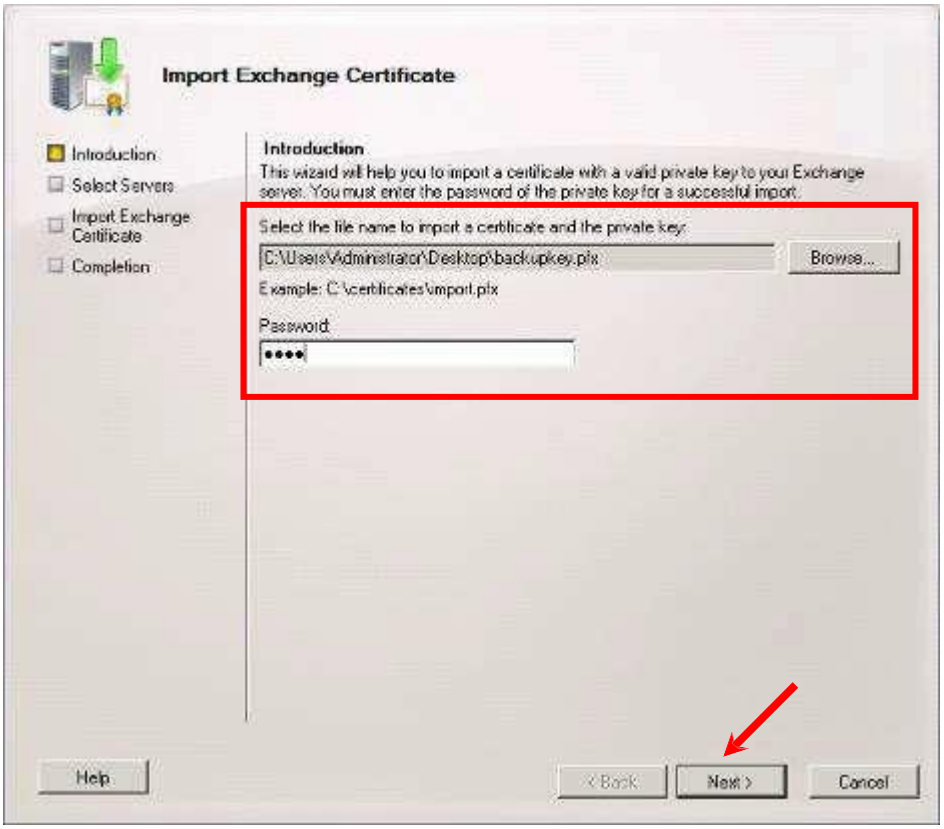


G. Restoring the Private Key

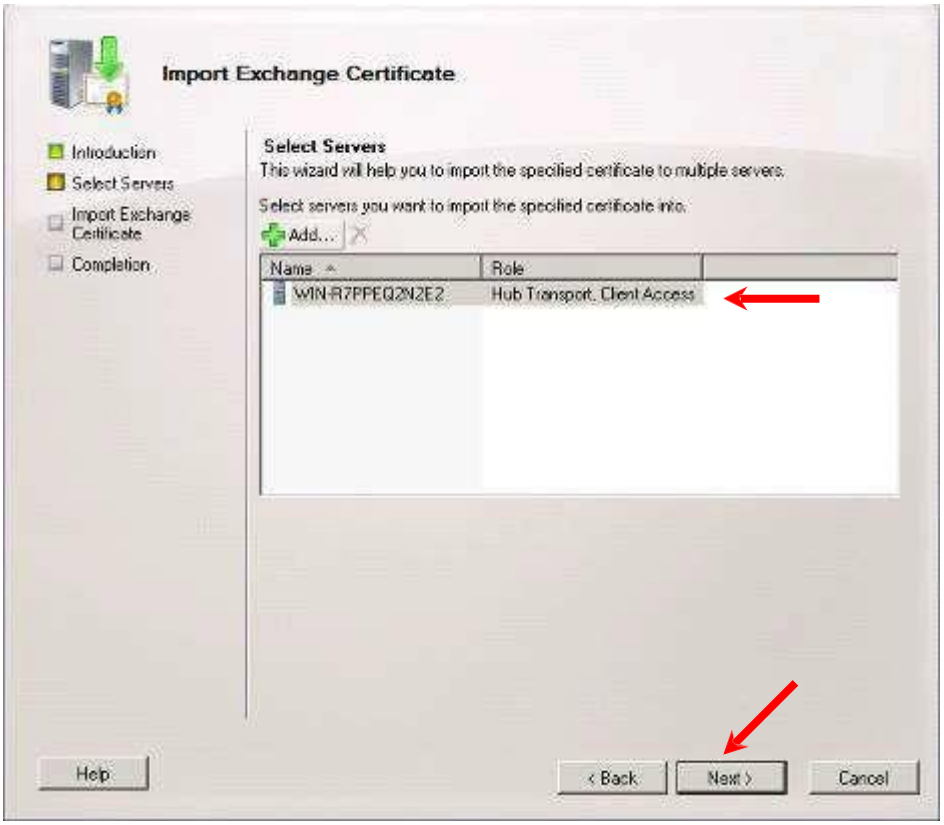
1 In **Exchange Management Console**, choose **Import Exchange Certificate** under Server Configuration.



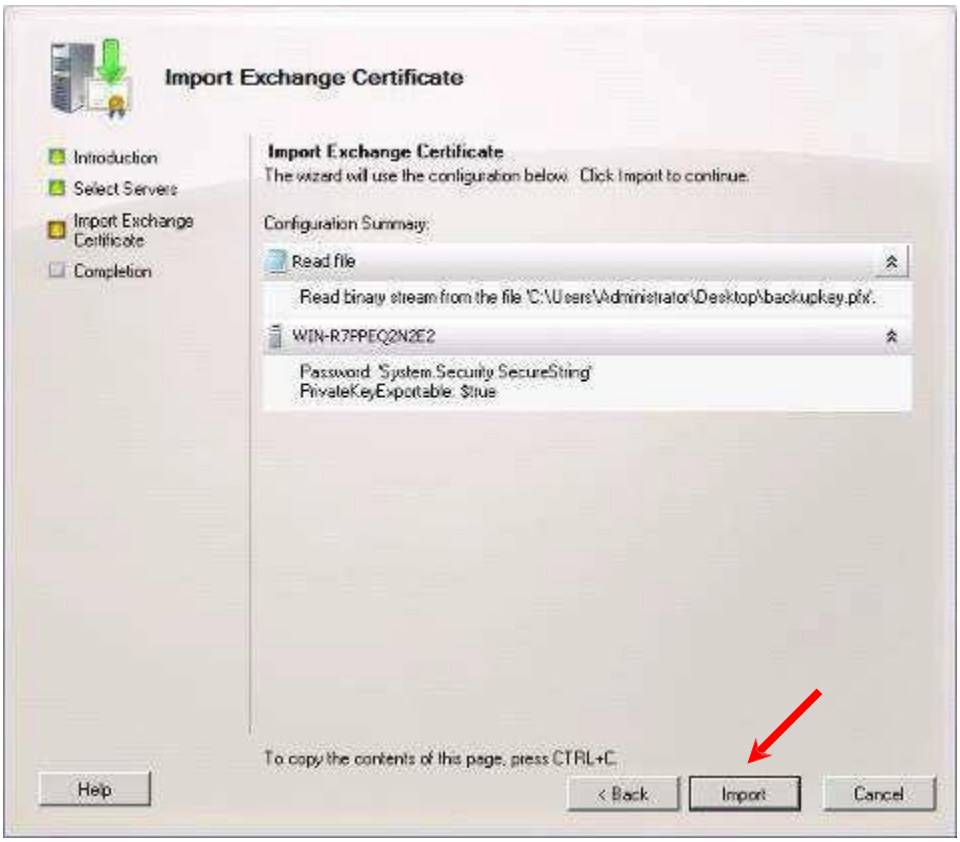
2 Select the private key you intend to import, and type in the password. Then, click **Next**.



3 Select **Servers** and click **Next**.



4 Check the detail and click **Import**.



5 Click **Finish** and **Hongkong Post e-Cert (Server)** certificate has been successfully restored.