



e-Cert (Server) User Guide
For Microsoft Exchange Server 2010

Revision Date: January 2026

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).....	10
D.	Installing Sub CA / Cross Certificate	16
	Removing the old Sub CA Certificate (if applicable)	19
	Installing Sub CA / Cross Certificate	20
	Installing Authority Revocation List (ARL)	25
E.	Installing Server Certificate	30
F.	Backing up the Private Key	36
G.	Restoring the Private Key	38

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:

F.	Backing up the Private Key	36
G.	Restoring the Private Key	38

New and Renew Application

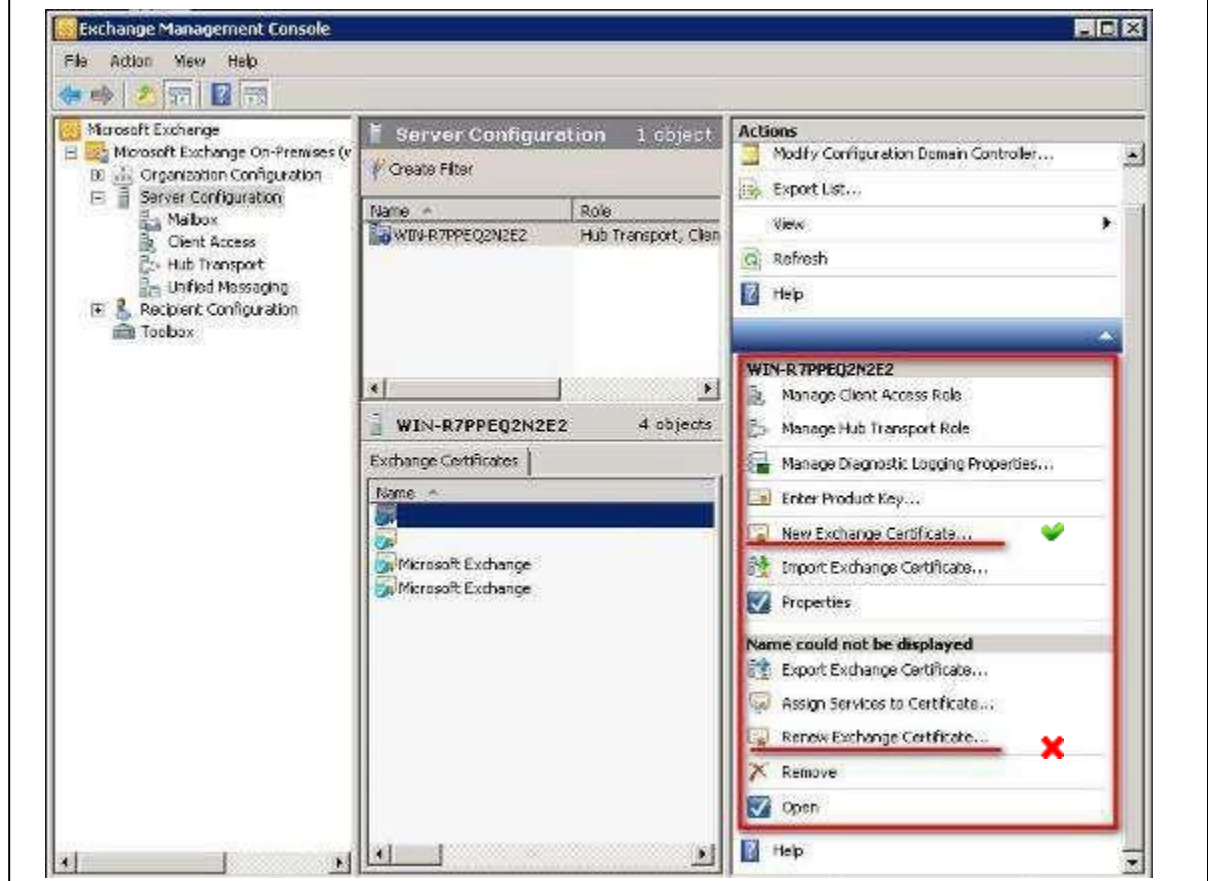
If this is the first time you apply for e-Cert (Server), please follow the instructions as described in the following sections for a new or renew application for e-Cert (Server):

B.	Generating Certificate Signing Request (CSR).....	4
C.	Submitting Certificate Signing Request (CSR).....	10
D.	Installing Sub CA / Cross Certificate	16
	Removing the old Sub CA Certificate (if applicable)	19
	Installing Sub CA / Cross Certificate	20
	Installing Authority Revocation List (ARL)	25
E.	Installing Server Certificate	30

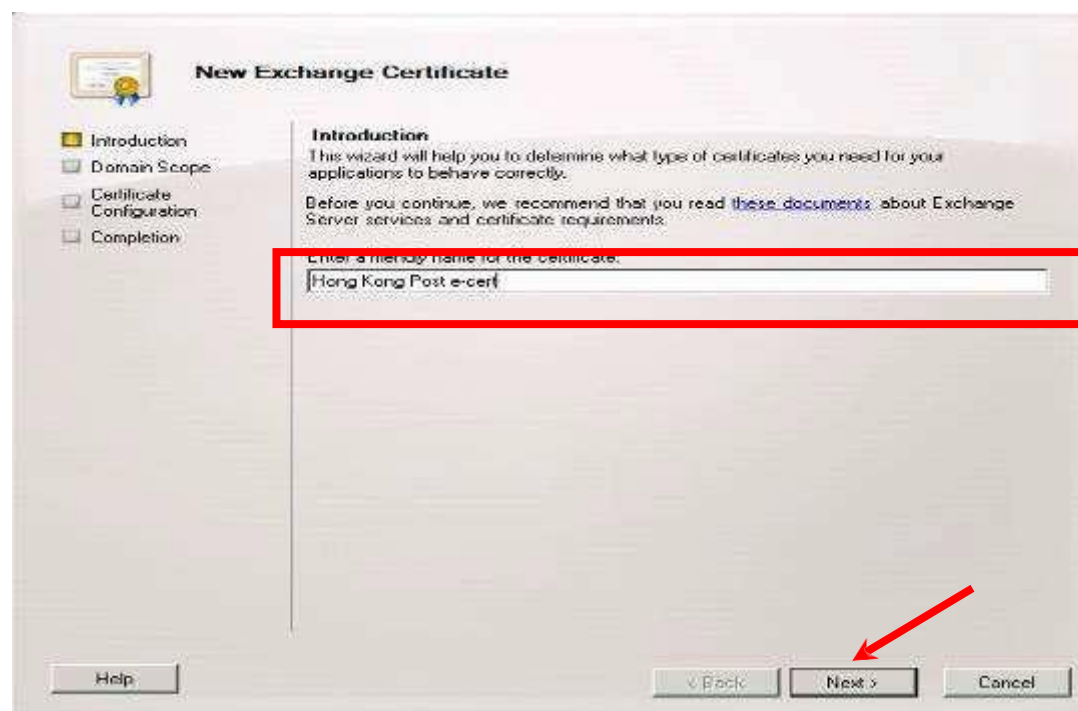
B. Generating Certificate Signing Request (CSR)

- 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**.



The screenshot shows the 'New Exchange Certificate' wizard in the 'Introduction' step. On the left, a navigation pane lists 'Introduction', 'Domain Scope', 'Certificate Configuration', and 'Completion'. The main area contains an 'Introduction' section with text explaining the wizard's purpose and a link to 'these documents'. Below this, a text box labeled 'Enter a friendly name for the certificate.' contains the text 'Hong Kong Post e-cert'. A red rectangle highlights this text box. At the bottom right, a red arrow points to the 'Next >' button. Other buttons include 'Help', '< Back', and 'Cancel'.

- 5 In the Domain Scope section,



The screenshot shows the 'New Exchange Certificate' wizard in the 'Domain Scope' step. The navigation pane on the left now has 'Domain Scope' selected. The main area contains a 'Domain Scope' section with instructions on using wildcards. Below this, there is a checkbox labeled 'Enable wildcard certificate' which is checked. Underneath, a text box labeled 'Root domain for wildcard (for example, contoso.com or *.contoso.com):' contains the text 'myserver.com'. A red rectangle highlights the checkbox and the text box. A red arrow points to the 'Next >' button at the bottom right. Other buttons include 'Help', '< Back', and 'Cancel'.

- 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.

The screenshot shows the 'New Exchange Certificate' wizard in Microsoft Exchange Server 2010. The 'Exchange Configuration' section is active, showing a list of services to be configured. A red box highlights the 'Outlook Web App' configuration options, which include checkboxes for 'Outlook Web App is on the Intranet' and 'Outlook Web App is on the Internet', and text boxes for the domain names used to access the Outlook Web App internally and externally. A red arrow points to the 'Next >' button at the bottom right of the wizard.

New Exchange Certificate

Exchange Configuration
Use this page to describe your Microsoft Exchange configuration and domain information. If the wizard does not automatically provide this information, you can enter it yourself.

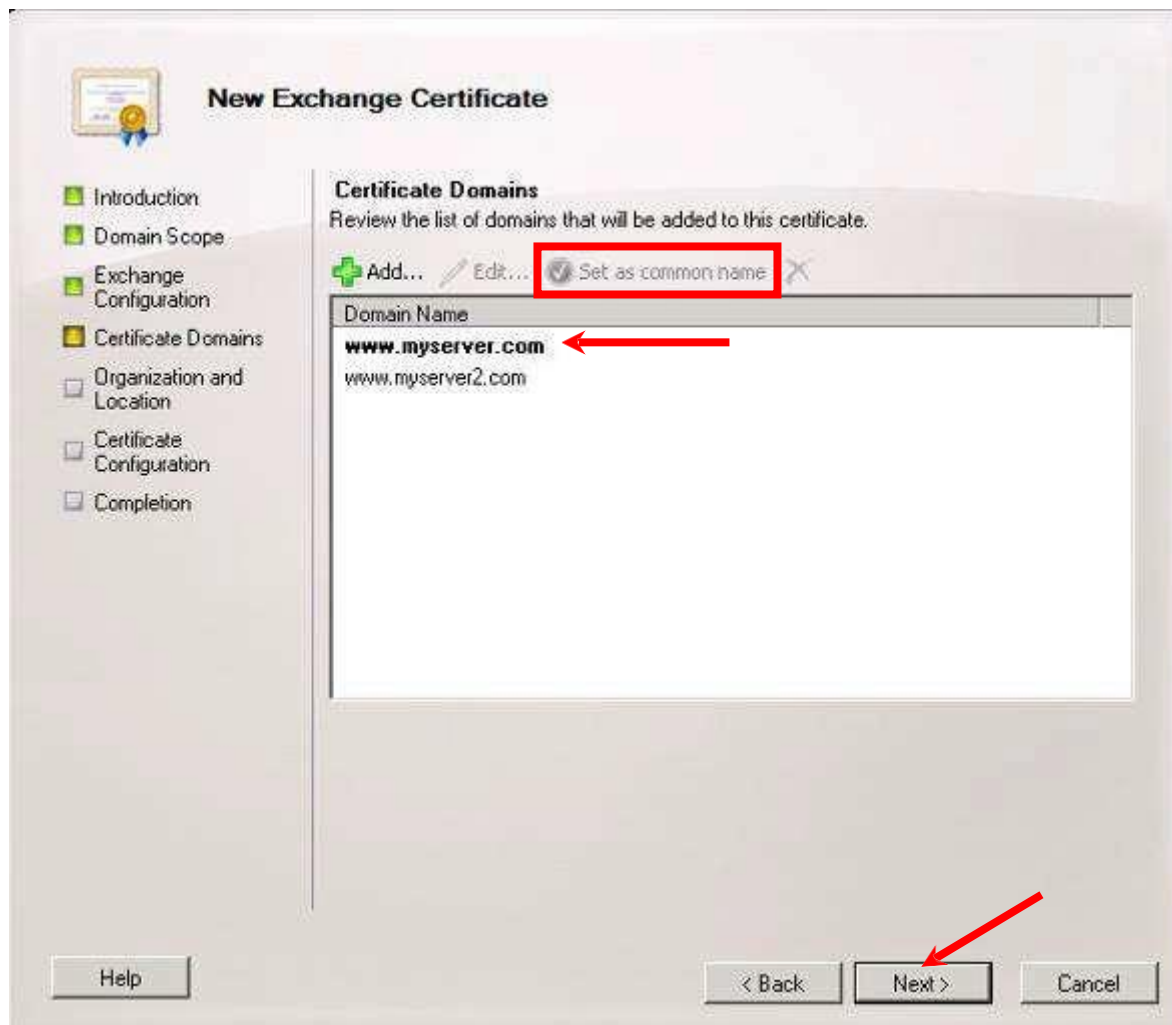
☒ Outlook Web App is on the Intranet
Domain name you use to access Outlook Web App internally:
www.myserver.com

☒ Outlook Web App is on the Internet
Domain name you use to access Outlook Web App (example: mail.contoso.com):
www.myserver2.com

☐ Client Access server (Exchange ActiveSync)
☐ Client Access server (Web Services, Outlook Anywhere, and Autodiscover)
☐ Client Access server (POP/IMAP)
☐ Unified Messaging server
☐ Hub Transport server
☐ Legacy Exchange Server

Help Reset < Back Next > Cancel

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 in the 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.*

New Exchange Certificate

Introduction
Domain Scope
Exchange Configuration
Certificate Domains
Organization and Location
Certificate Configuration
Completion

Organization and Location
Use this page to enter the name of your organization, organizational unit, location, and certificate request file path.

Organization:
My Organization

Organization unit:
My Organization Unit

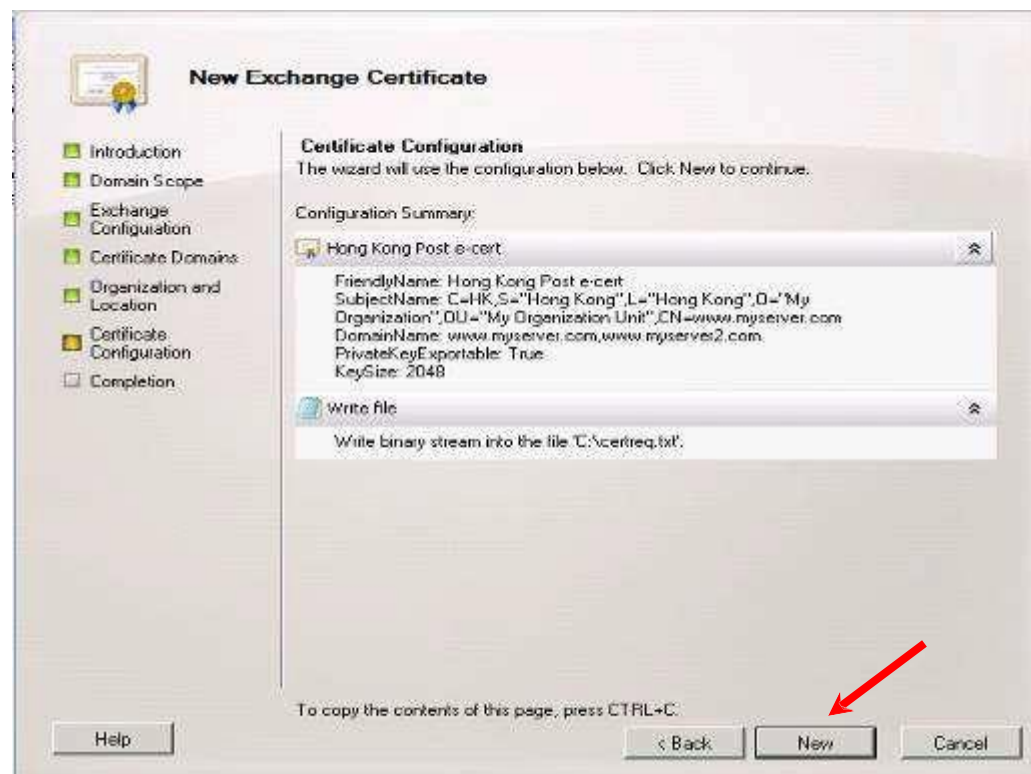
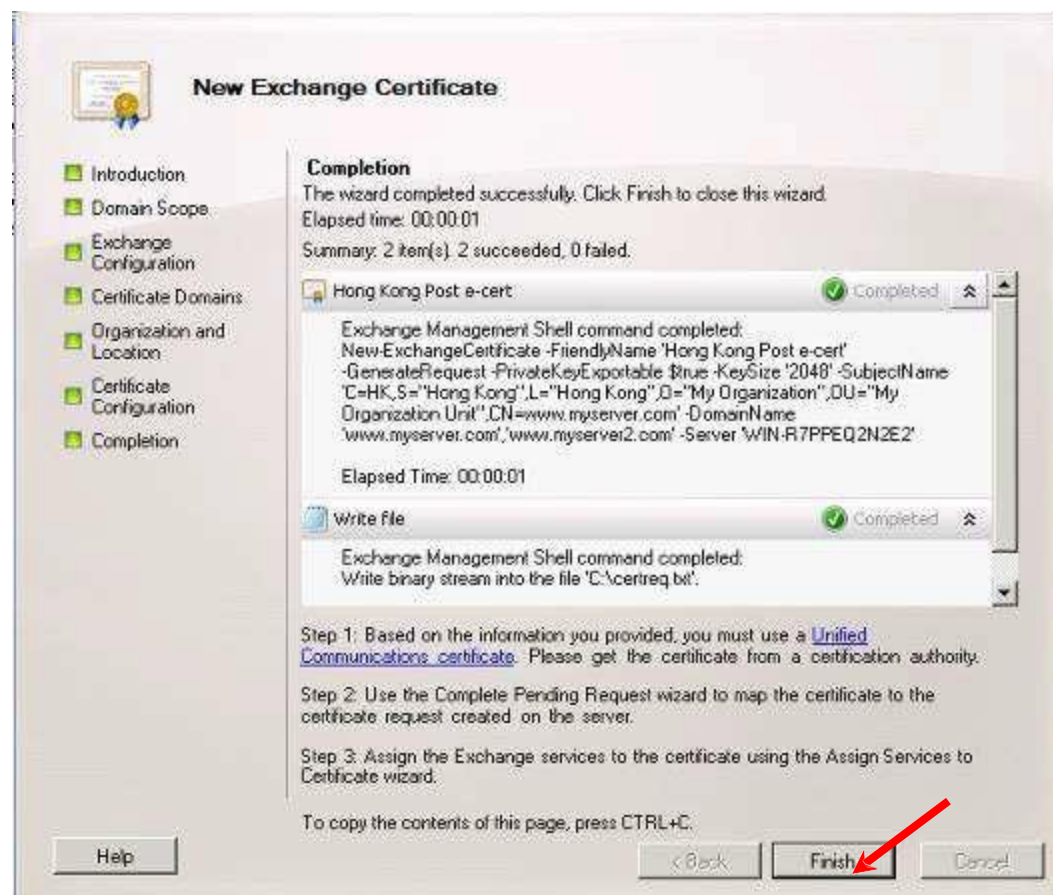
Location:
Country/region:
Hong Kong S.A.R.

City/locality:
Hong Kong

State/province:
Hong Kong

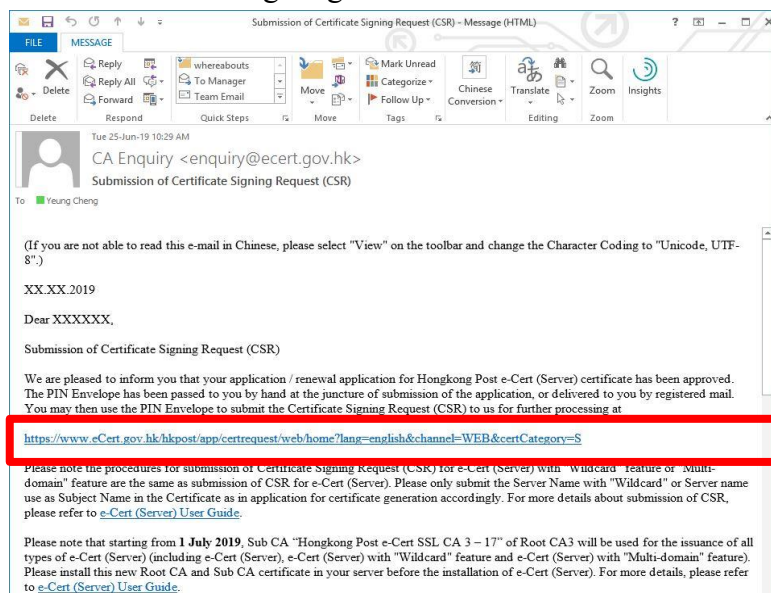
Certificate Request File Path:
Specify the name of the request file in the text box below. Use the Browse button to select the folder where you want the request file to be created. The name must end with the extension ".req".
C:\certreq.txt

Help < Back Next > Cancel

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”.

Hongkong Post e-Cert
香港郵政電子核證

The solution for e-Security

Submission of Certificate Signing Request (CSR) - e-Cert (Server)

The personal data you provided in this form will be used by Hongkong Post and its operator of e-Cert services for provision of e-Cert services to you. Information we collected about you will not be disclosed by us to any other party in a form that would identify you unless it is permitted or authorised by law. It is voluntary for you to supply to us your personal data. Failure to provide related data may affect the processing of your application. Under the Personal Data (Privacy) Ordinance, you have a right to request access to or correction of the data about you being held by us. If you wish to do so, please complete the Data Access Request Form (Pos736) or Personal Data Correction Request Form (Pos736A) and return it to any post office or send it to our Personal Data Privacy Officer by e-mail or by post. The Data Access Request Form and Personal Data Correction Request Form are also available at all post offices.

Server Particulars :

Server Name :

e-Cert PIN Envelope information :

Reference Number :
(Shown on the cover of the PIN Envelope, 9-digit)

e-Cert PIN :
(No need to input the space within the 16-digit PIN)

Please note that starting from **1 May 2025**, new Sub CA certificates will be used to issue e-Cert (Server). To ensure a smooth transition, please:

1. Remove the old Sub CA certificate from your server, if applicable
2. Download and install the new Sub CA certificate (labeled as "Effective from 1 May 2025")
3. Install your e-Cert (Server) which are issued on or after 1 May 2025

For more details, please refer to [e-Cert \(Server\) User Guide](#).

Old Sub CA certificates without EKU fields will be revoked before 15 June 2026.

2007 © | Important Notices | Privacy Policy

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.)



The screenshot shows the 'Submission of Certificate Signing Request (CSR) - e-Cert (Server)' page. The page has a green header with the Hongkong Post e-Cert logo and the tagline 'The solution for e-Security'. The left sidebar contains navigation icons and logos for CERTIZEN, Hongkong Post, and W3C. The main content area is divided into two sections: 'Subscriber Details' and 'Information of the certificate to be generated'. The 'Subscriber Details' section contains fields for Server Name, Additional Server Name(s), Number of Additional Server(s), Organisation Name, Branch Name, Business Registration No., Certificate of Incorporation No. / Certificate of Registration No., and Other Registration Document. The 'Information of the certificate to be generated' section contains fields for Type of Certificate and Subscription Period. Below these sections, there is a confirmation message and four buttons: Confirm, Reject, Back, and Confirm Opt with Chinese. A footnote at the bottom states: '*For Chinese domain application, please make sure the Chinese characters are correct.'

Submission of Certificate Signing Request (CSR) - e-Cert (Server)

Subscriber Details

Server Name :	www.ecert.gov.hk
Additional Server Name(s) :	www1.ecert.gov.hk
Number of Additional Server(s) :	1
Organisation Name :	Hong Kong SAR Government 香港特別行政區政府
Branch Name :	HKPO-Business Development Branch 香港郵政
Business Registration No. :	
Certificate of Incorporation No. / Certificate of Registration No. :	
Other Registration Document :	HKPO-BDB

Information of the certificate to be generated

Type of Certificate :	e-Cert (Server) with "Multi-domain" Feature
Subscription Period :	1-year

This page is to confirm the application data. If the above information is correct, please click "Confirm" to proceed
You may opt to get the e-Cert (Server) containing the organisation name and branch name in "Chinese" by clicking "Confirm Opt with Chinese" button to proceed

*For Chinese domain application, please make sure the Chinese characters are correct.

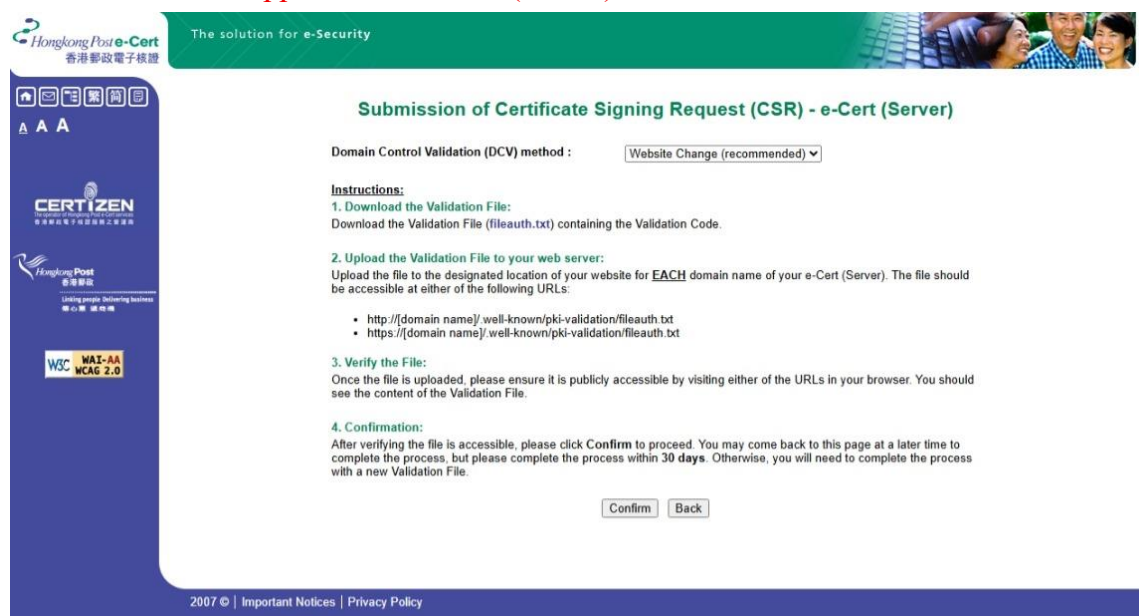
2007 © | Important Notices | Privacy Policy

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 **from 15 March 2026** and for **non-Government B/D subscribers 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 **EACH** 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.**



Hongkong Post e-Cert
香港郵政電子核證

The solution for e-Security

Submission of Certificate Signing Request (CSR) - e-Cert (Server)

Domain Control Validation (DCV) method :

Instructions:

- 1. Download the Validation File:**
Download the Validation File (fileauth.txt) containing the Validation Code.
- 2. Upload the Validation File to your web server:**
Upload the file to the designated location of your website for **EACH** domain name of your e-Cert (Server). The file should be accessible at either of the following URLs:
 - [http://\[domain name\]/well-known/pki-validation/fileauth.txt](http://[domain name]/well-known/pki-validation/fileauth.txt)
 - [https://\[domain name\]/well-known/pki-validation/fileauth.txt](https://[domain name]/well-known/pki-validation/fileauth.txt)
- 3. Verify the File:**
Once the file is uploaded, please ensure it is publicly accessible by visiting either of the URLs in your browser. You should see the content of the Validation File.
- 4. Confirmation:**
After verifying the file is accessible, please click Confirm to proceed. You may come back to this page at a later time to complete the process, but please complete the process within **30 days**. Otherwise, you will need to complete the process with a new Validation File.

2007 © | Important Notices | Privacy Policy

- 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.



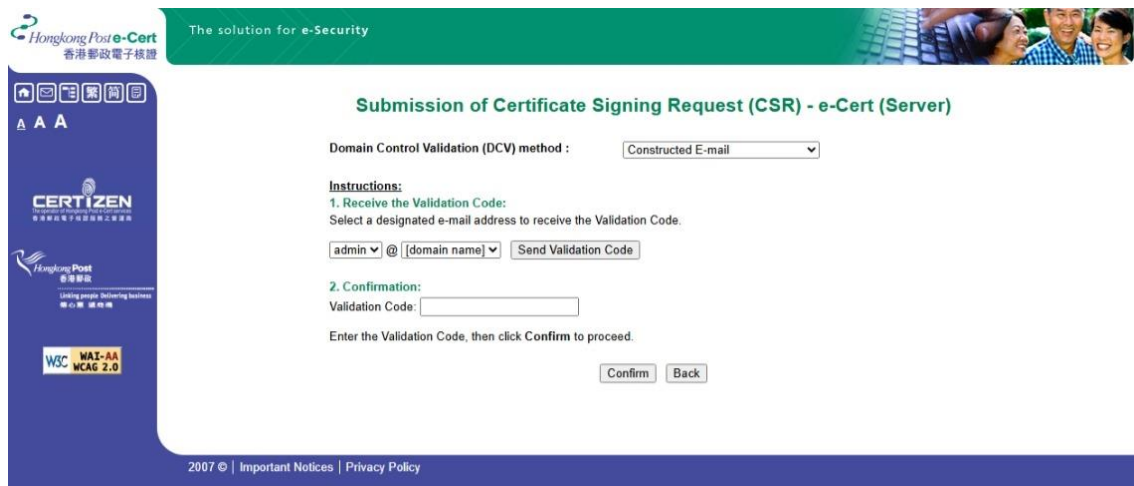
The screenshot shows the 'Submission of Certificate Signing Request (CSR) - e-Cert (Server)' page. The 'Domain Control Validation (DCV) method' is set to 'DNS Change (recommended)'. The instructions are as follows:

- 1. Add a DNS record:** Add a DNS TXT record for **EACH** domain name of your e-Cert (Server).
 - Record Type:** TXT
 - Host:** [domain name]
 - Value:** [Validation Code] [Copy Validation Code](#)
 - TTL:** 3600
- 2. Verify the DNS Record:** Ensure the DNS record is publicly resolvable.
- 3. Confirmation:** Once the record is added and publicly resolvable, please click **Confirm** to proceed. You may come back to this page at a later time to complete the DCV process, but please complete the process within **30 days**. Otherwise, you will need to complete the process using a new Validation Code.

Buttons: [Confirm](#) [Back](#)

2007 © | [Important Notices](#) | [Privacy Policy](#)

- 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.**




The screenshot shows the 'Submission of Certificate Signing Request (CSR) - e-Cert (Server)' page. The 'Domain Control Validation (DCV) method' is set to 'Constructed E-mail'. The instructions are as follows:

- 1. Receive the Validation Code:** Select a designated e-mail address to receive the Validation Code.
 - admin** [dropdown] @ [domain name] [dropdown] [Send Validation Code](#)
- 2. Confirmation:**
 - Validation Code:** [input field]
 - Enter the Validation Code, then click **Confirm** to proceed.


Buttons: [Confirm](#) [Back](#)


2007 © | [Important Notices](#) | [Privacy Policy](#)

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".





The solution for e-Security

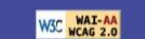




A A A







Submission of Certificate Signing Request (CSR) - e-Cert (Server)

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


```

-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZCgAwQWDEEMAKA1UEBhMCSEExGTAxBGhVBAAMHED3dy51Y2VydC5n
b3YuaG9wsggE1MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQMDFkQ0tMhWboc
9vOuf1D/Gwuh2NEk48z6uBnPB1GhwCJ+HRES/hJFxtCJA0vtzzJU93cA21
1lb7FCb+alw+pgiVACNHRfaUe0L8IFD1wIldHembT4uZYyKkYwDzdIPQgRizZx3
Bv61aj6yK8WKvRxy42ydfzPNFLnJIXLwYocdcYqbjcQrQ80mLMS1lyIE2eW3S3KV
86qyw42wQVmBbp1Kn6UEPCk2cm0FkohP+t6cfZ6y2YB08qFKKvDHTC852IDpThMF
OcU2AeaTInpr4Y64umdngrK0Gel2EM8mbBpsZXdamxV/YA357z6jCnOXXFqlHLO
A5ST8iHVAqMBAAQgQTA/BgkqhkiG9w0BCQ4xMjAwMCA4GA1UdEQQnMCWCEH3dy51Y
2VydC5nb3YuaG9wCgCEX3dzdUZW1lc0uZ292LmhrMA0GCSqGSIb3DQEBCwUAA4IB
AQDk8+M14QrXihgP241cGrw81sAbZPmdX9e5bvr7oDbuvTj915AiaXwRVoQx41i
fUJqFkuT/2TWEJbTz2FBsHszCJbW9/zHB1Q33LV+8GRhfBjeOm6Ku+wse0GcVRzs
10X8cLxT0Lp0aJr1zslrQDFKipJFr4R9Q1UJ1U7QZfW+IBq9UBYitJe2Xx4vC
/3V6kH1wXWVPheKohU/Z9rAXCxBH01x3CjTer4zrDmaND9tM57PpJE/7JADKfyz
C33UFmU7EBK1+V+561SDzhWEQN/yZfZdF+EyIbBC5167uacXJicjbrwapSWQvo39

```

2007 © | [Important Notices](#) | [Privacy Policy](#)

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



The solution for e-Security

Submission of Certificate Signing Request (CSR) - e-Cert (Server)

The following is the information of this certificate:-

Subscriber Details	
Server Name :	www.ecert.gov.hk
Additional Server Name(s) :	www1.ecert.gov.hk
Organization Name :	Hong Kong SAR Government
Branch Name :	HKPO-Business Development Branch
Business Registration No. :	
Certificate of Incorporation No. / Certificate of Registration No. :	
Other Registration Document :	HKPO-BDB


The following is the system generated information

Subscriber Reference Number :	0003294413
Type of Certificate :	Hongkong Post e-Cert (Server)
Issued by :	Hongkong Post e-Cert SSL CA 3 - 17
Certificate Serial Number :	45 16 9d 08 95 af 56 f3 d0 b5 a8 02 7d 98 8e 44 76 d1 c7 1f
Validity Period :	05/01/2026 - 23/07/2026 (199 days)


For Chinese domain application, please make sure the Chinese characters are correct.

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

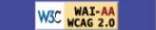
(Note: Your personal data collected by Hongkong Post will be used for processing your e-Cert application. You have the right of access and correction with respect to personal data as provided for in the Personal Data (Privacy) Ordinance.)



Leading people, Delivering business




Leading people, Delivering business



2007 © | Important Notices | Privacy Policy

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



Hongkong Post e-Cert
香港郵政電子核證

The solution for e-Security

Submission of Certificate Signing Request (CSR) - e-Cert (Server)

You may now:-

1. Download the "Hongkong Post e-Cert (Server)" certificate
2. Download the Hongkong Post CA Root Certificates
3. Download the e-Cert (Server) User Guide

Reminder
To ensure the accessibility of your websites/servers by the older versions of mobile/desktop devices not yet preloaded with Root CA3 after expiry of Root CA1, please install the "Hongkong Post Root CA 3 (cross-certificate 2022)" to your websites/servers. For details, please refer to the news announcement.

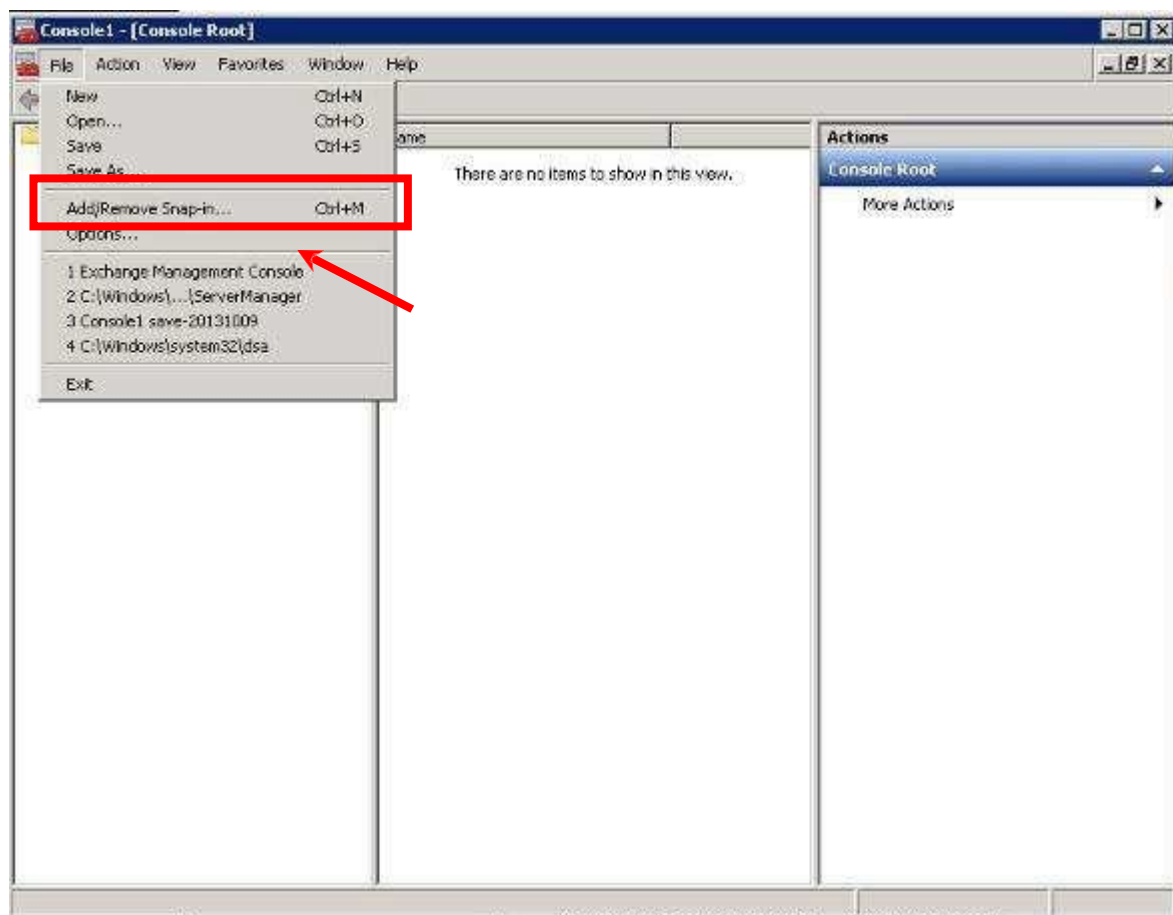
2007 © | Important Notices | Privacy Policy

Note:

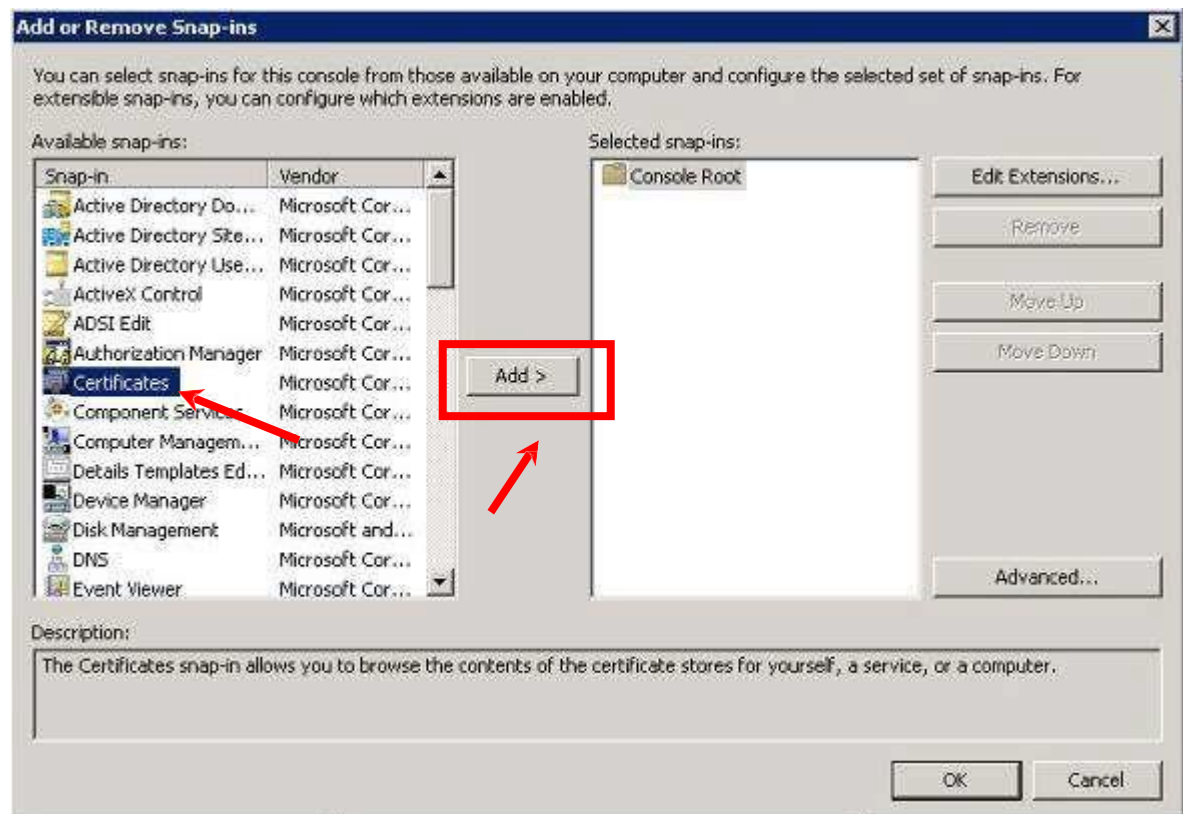
1. You can also download your e-Cert (Server) from the Search and Download Certificate web page.
<https://www.ecert.gov.hk/en/sc/index.html>
2. Install the Sub CA "Hongkong Post e-Cert SSL CA 3 - 17" issued by Root CA3. Click the following link to download:
http://www1.ecert.gov.hk/root/ecert_ssl_ca_3-17_pem.crt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

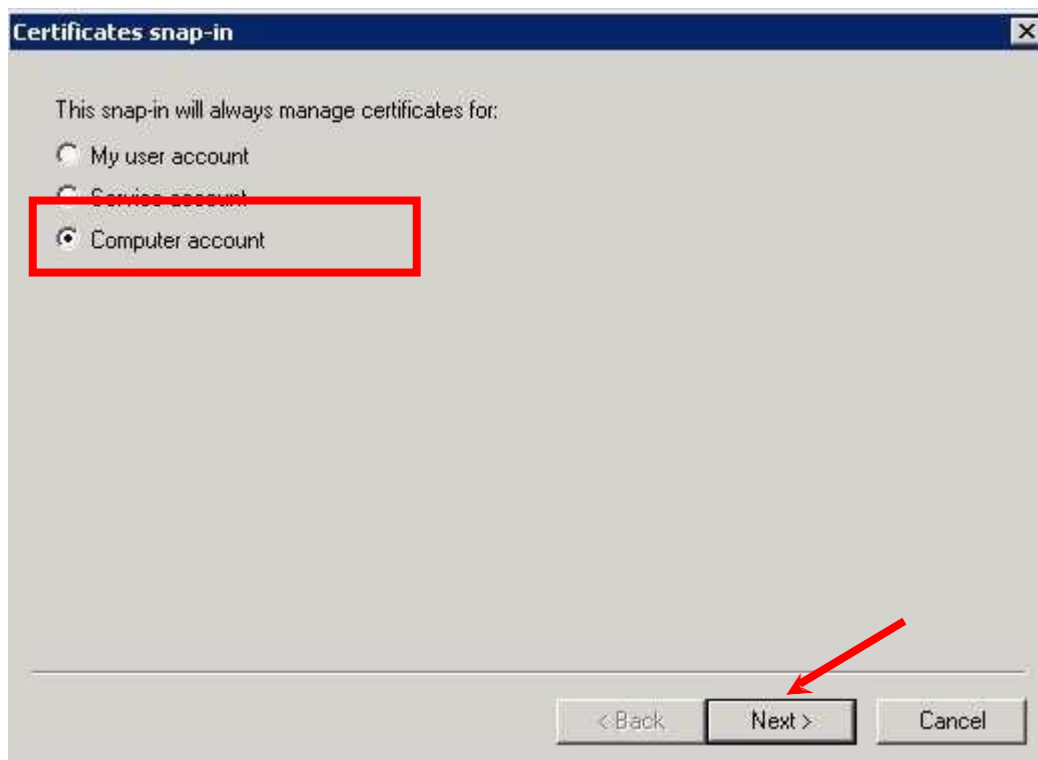
1. Start **Microsoft Management Console (MMC)** by clicking **Start > Run**, type **mmc** and click **OK**, and then select **Add/Remove Snap-in** from the **File** menu.



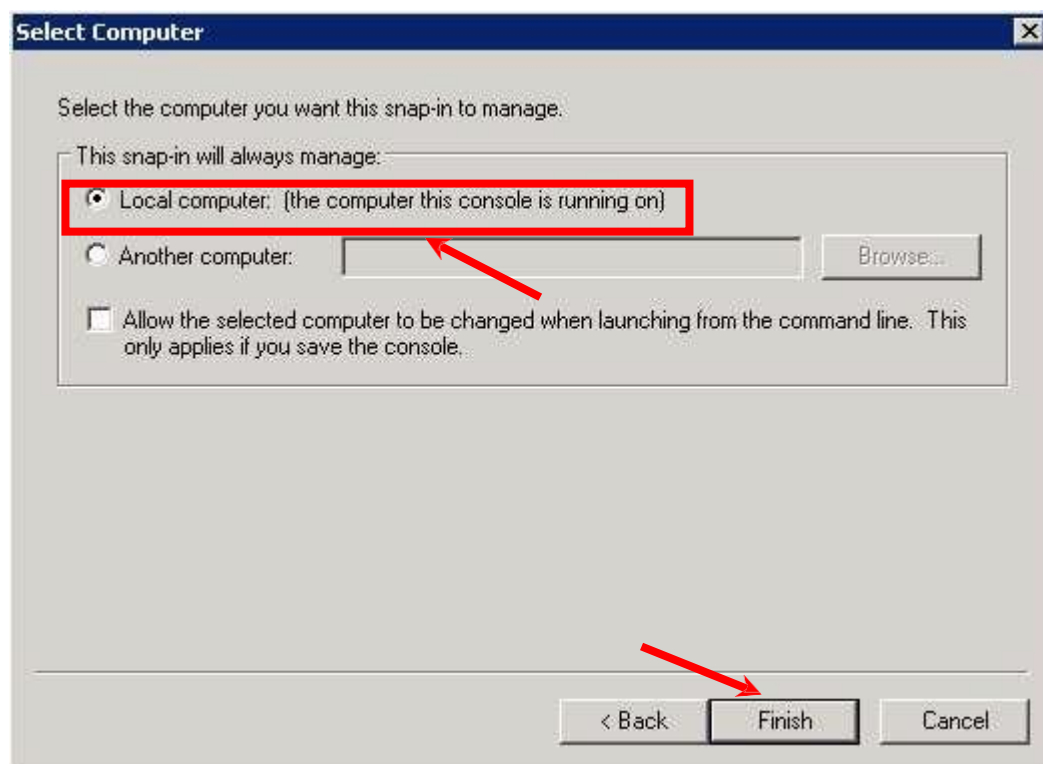
2. Select **Certificate** in **Available snap-in** then Click **Add**.



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



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

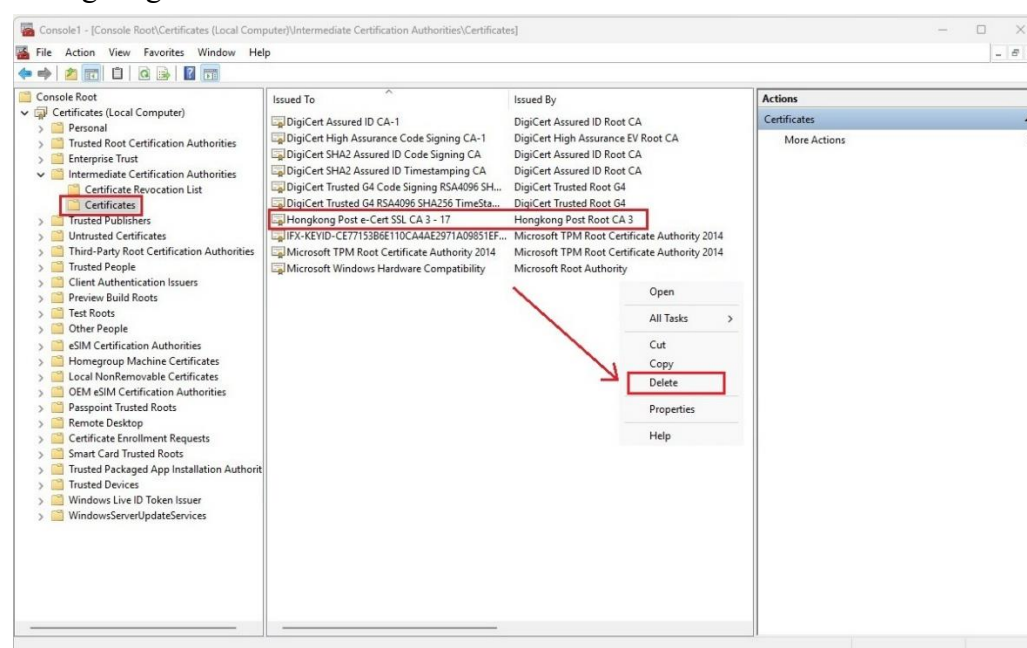


The following uses the “**Hongkong Post e-Cert SSL CA 3 - 17**” Sub CA certificate as example.

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”.



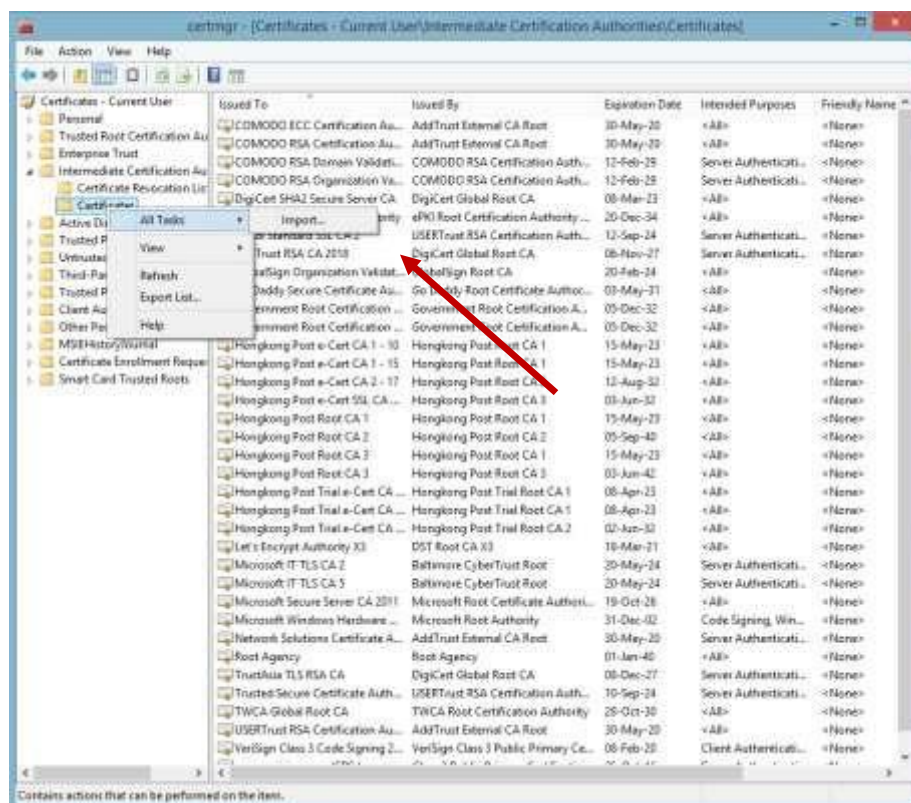
Click “Yes” to delete.



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

Installing Sub CA / Cross Certificate

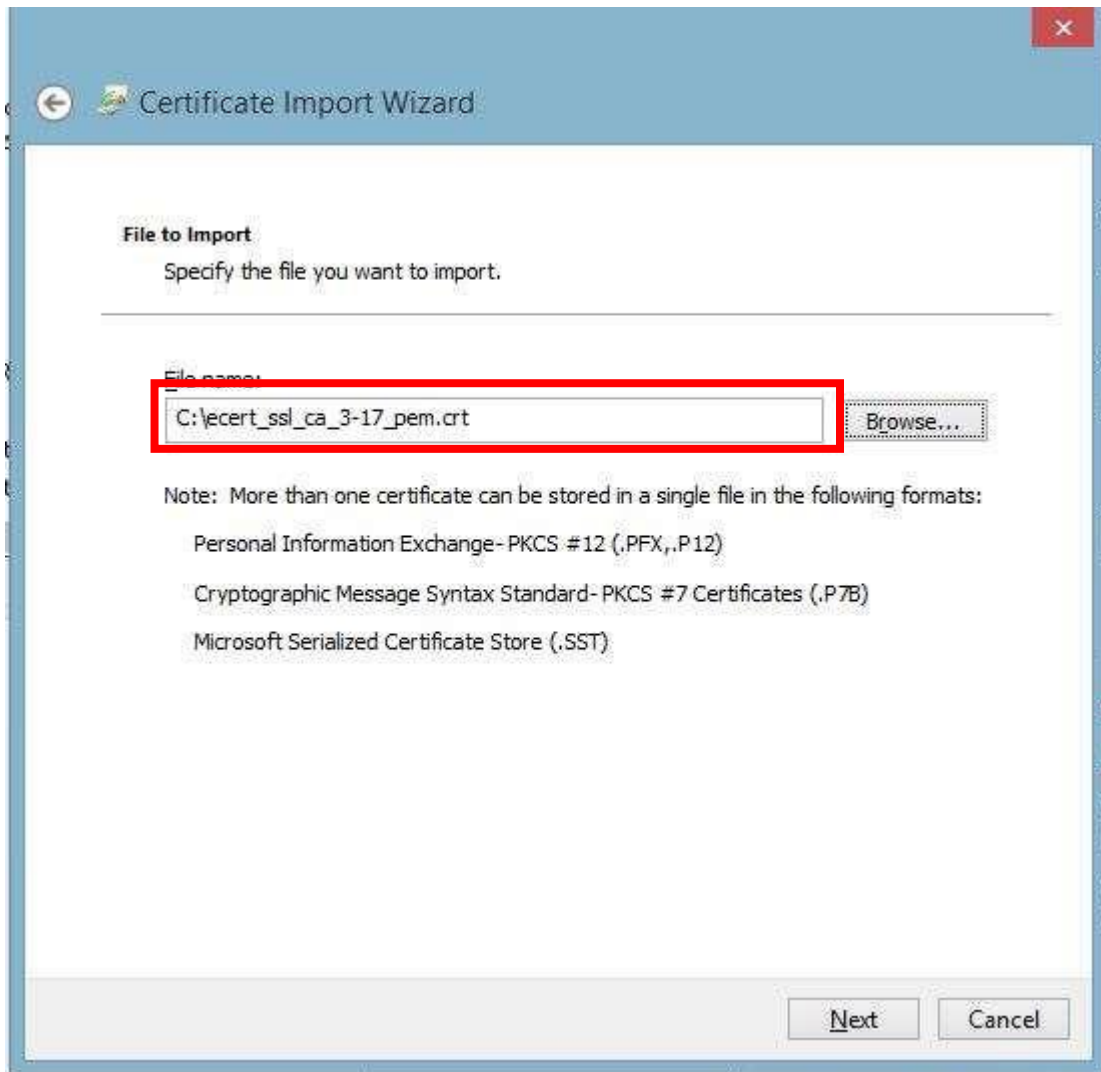
5. Expand the **Certificates (Local Computer)** node, then right-click the **Intermediate Certification Authorities** and then select **All Tasks > Import**.



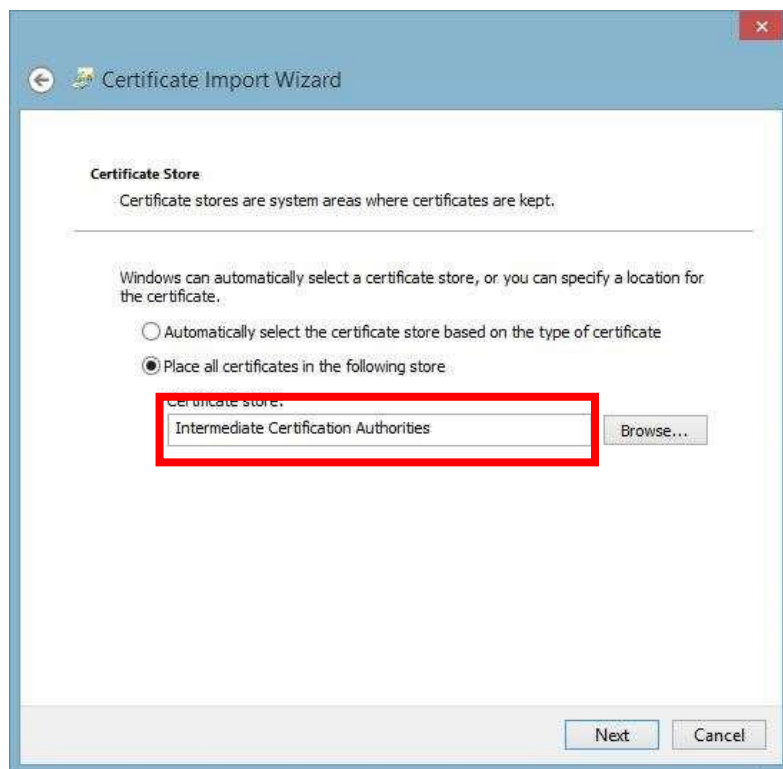
6. In the **Certificate Import Wizard**, click **Next** to continue.



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**.

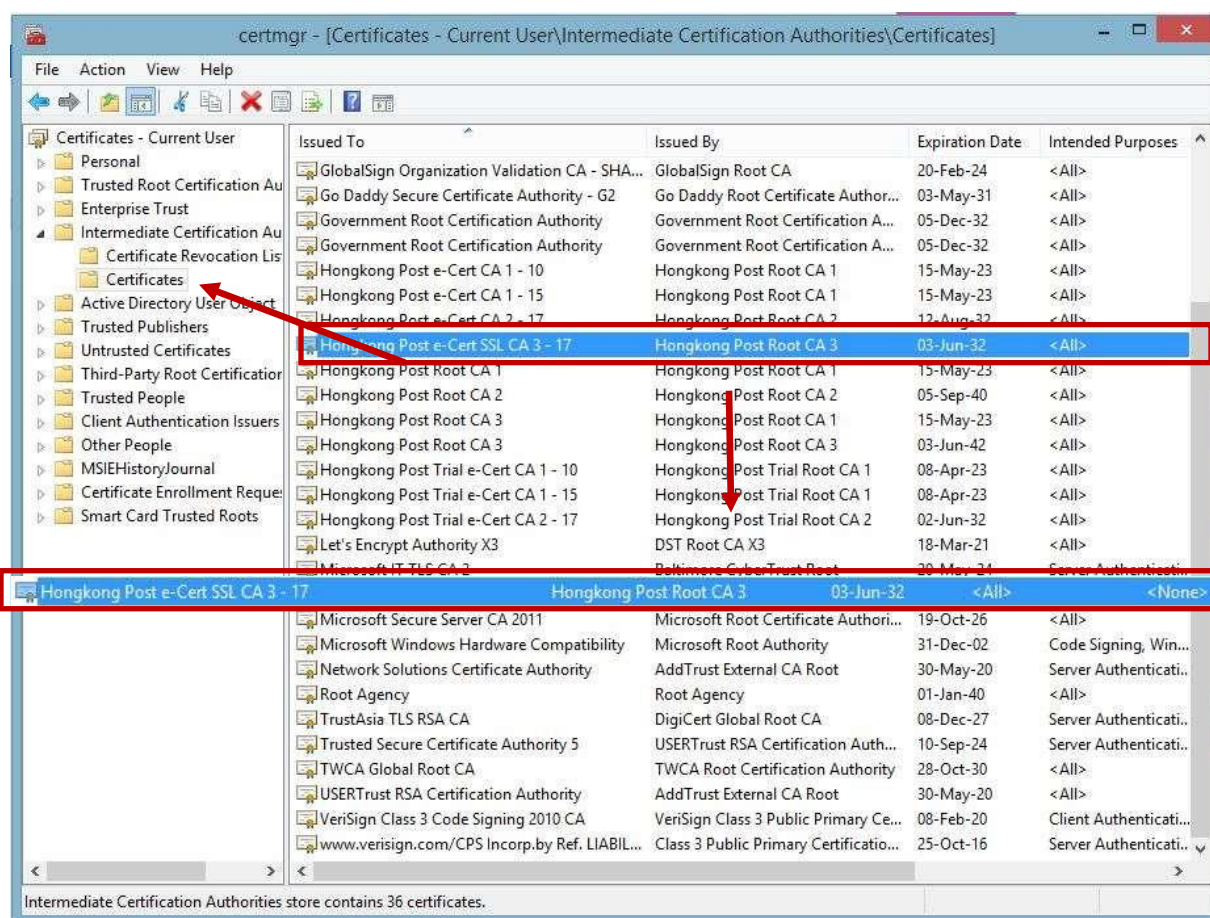
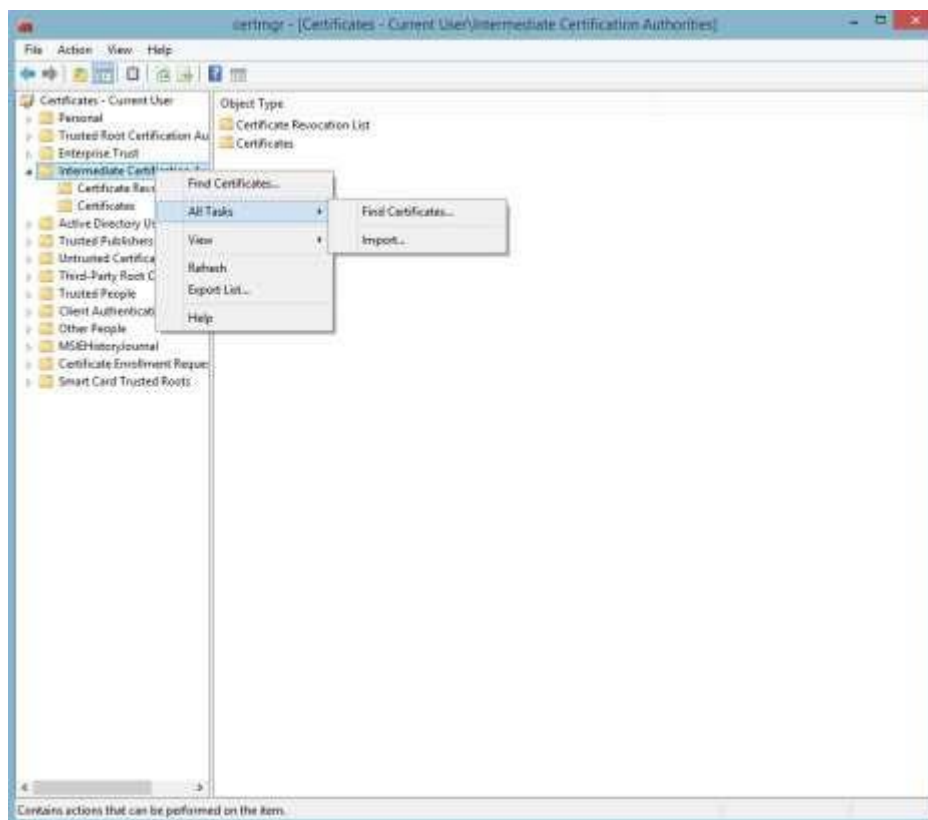


Figure 1: **Hongkong Post e-Cert SSL CA 3 - 17** certificate has been successfully installed

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)

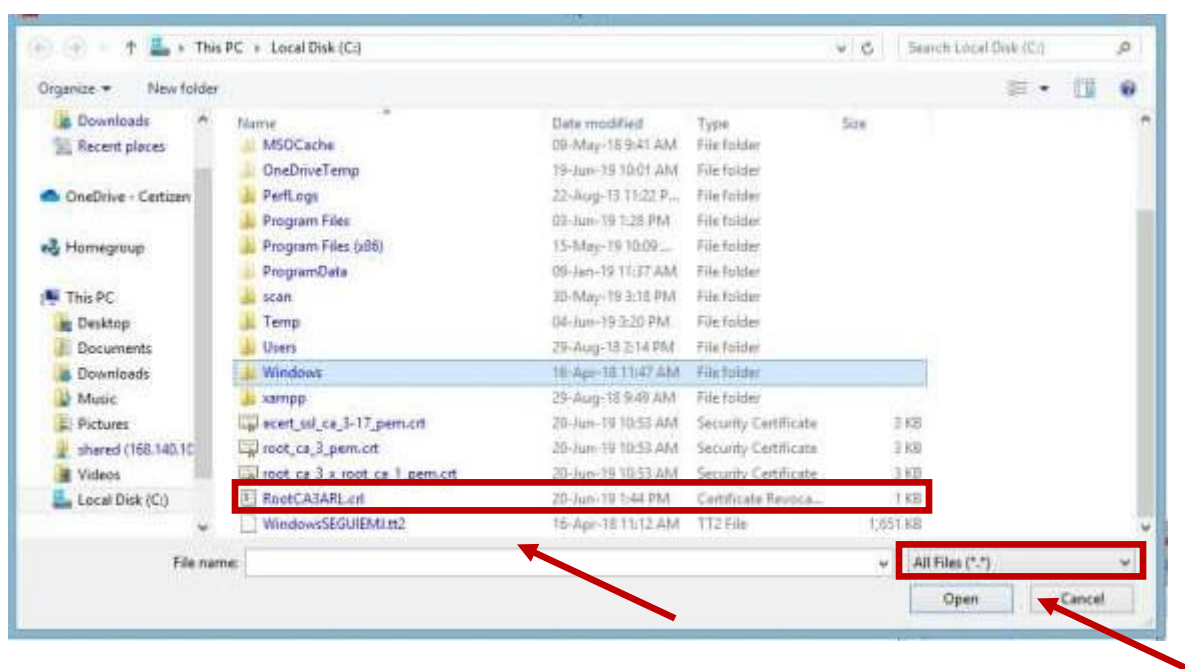
11. Download the **Hongkong Post Authority Revocation List (ARL)** at:
<http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl>
12. Expand the **Certificates (Local Computer)** node, then right-click choose the **Intermediate Certification Authorities**, and then select **All Tasks > Import**.

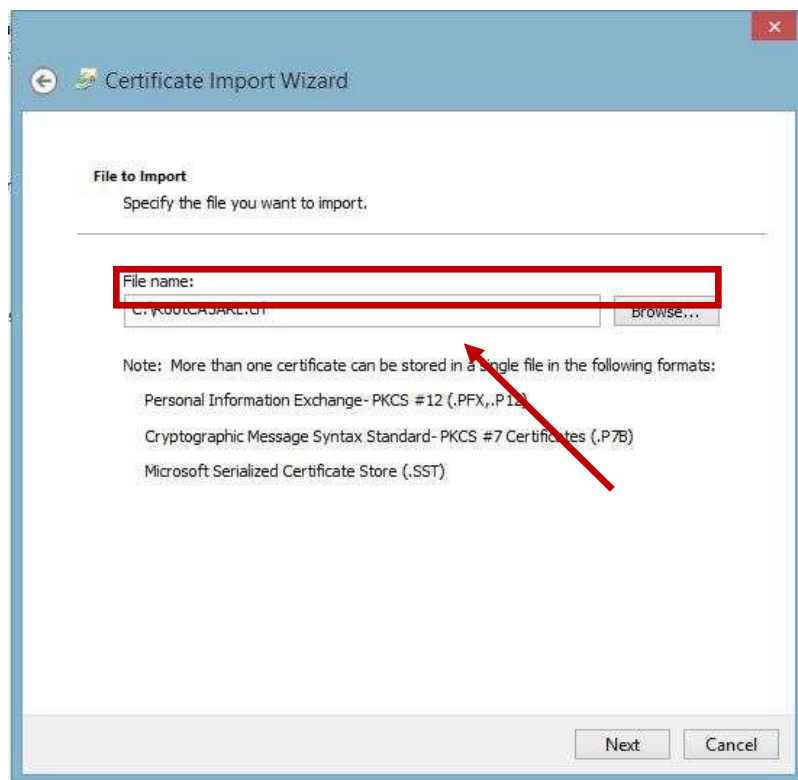


13. In the **Certificate Import Wizard**, click **Next** to continue.

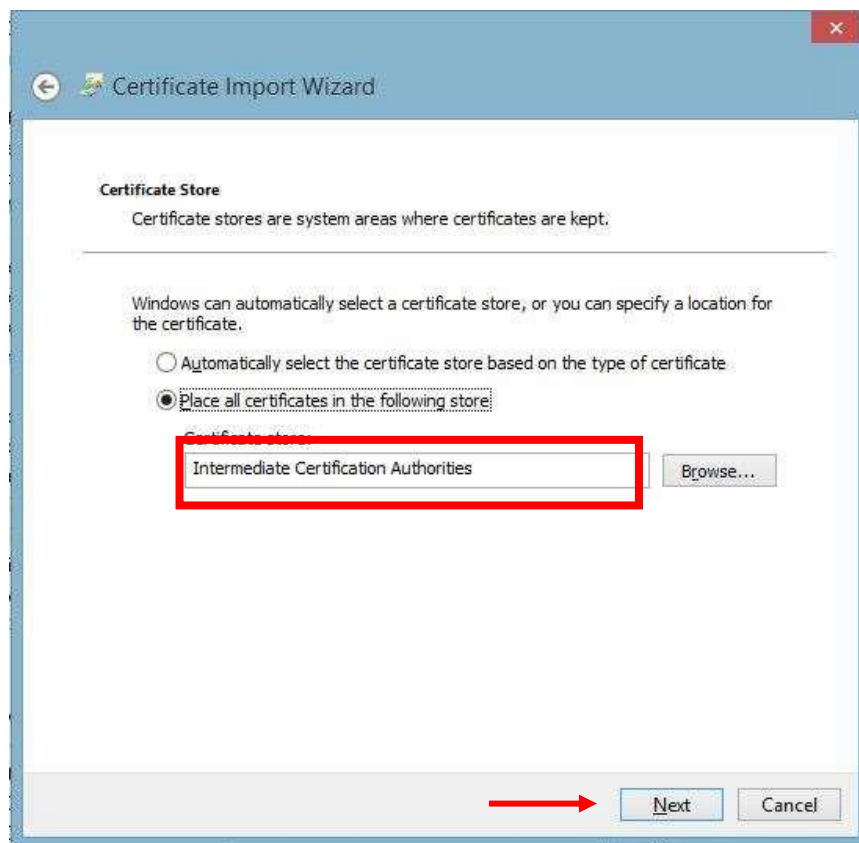


14. Click **Browse** to locate the **Hongkong Post Authority Revocation List (ARL)** that you downloaded before in Step 11 (RootCA3ARL.crl), and then click **Next**. (Tip: choose **All Files**)

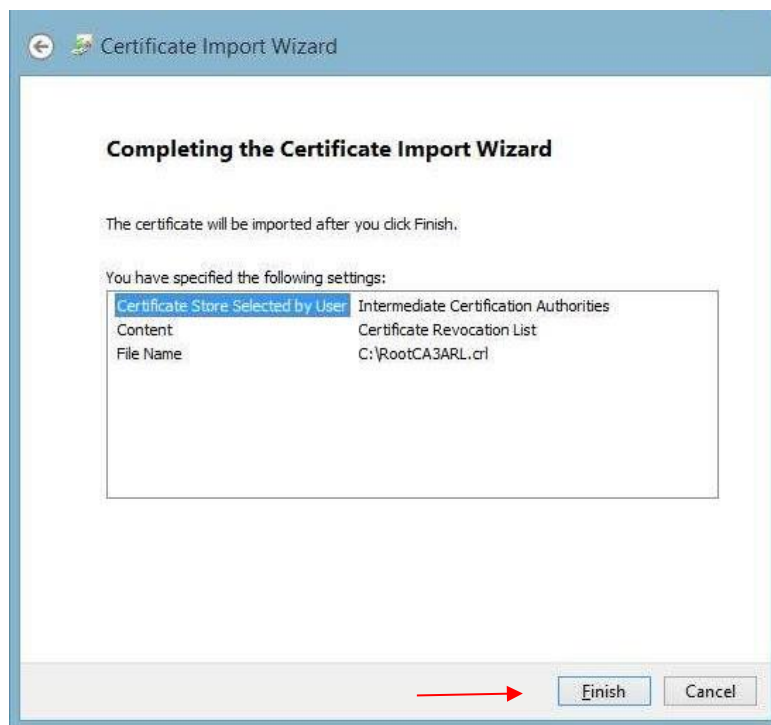




15. Select **Place all certificates in the following store** and choose **Intermediate Certification Authorities**, click **Next**.



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**.

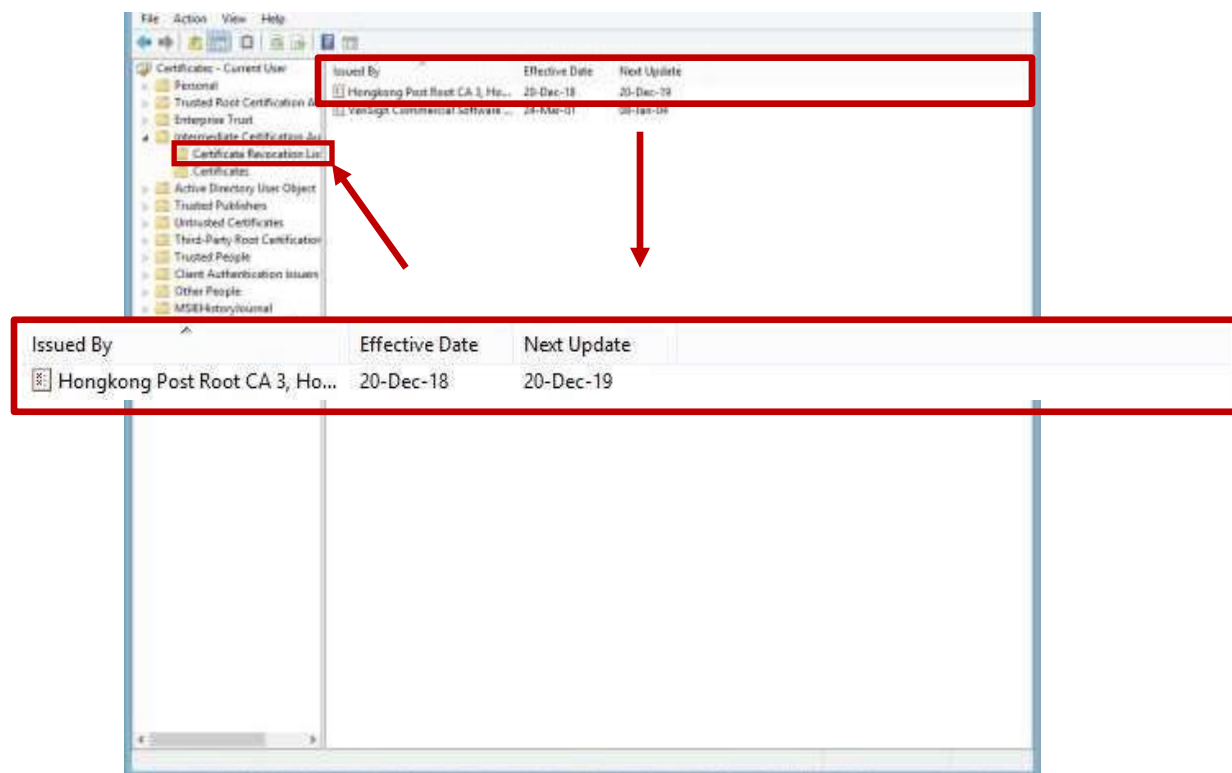
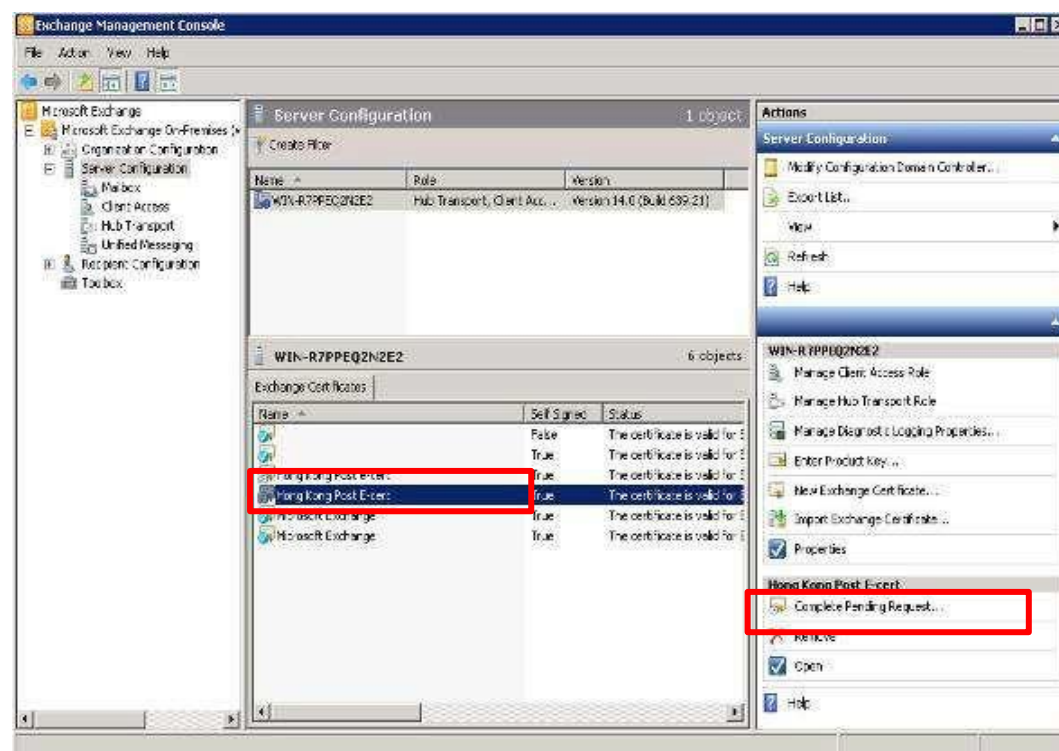


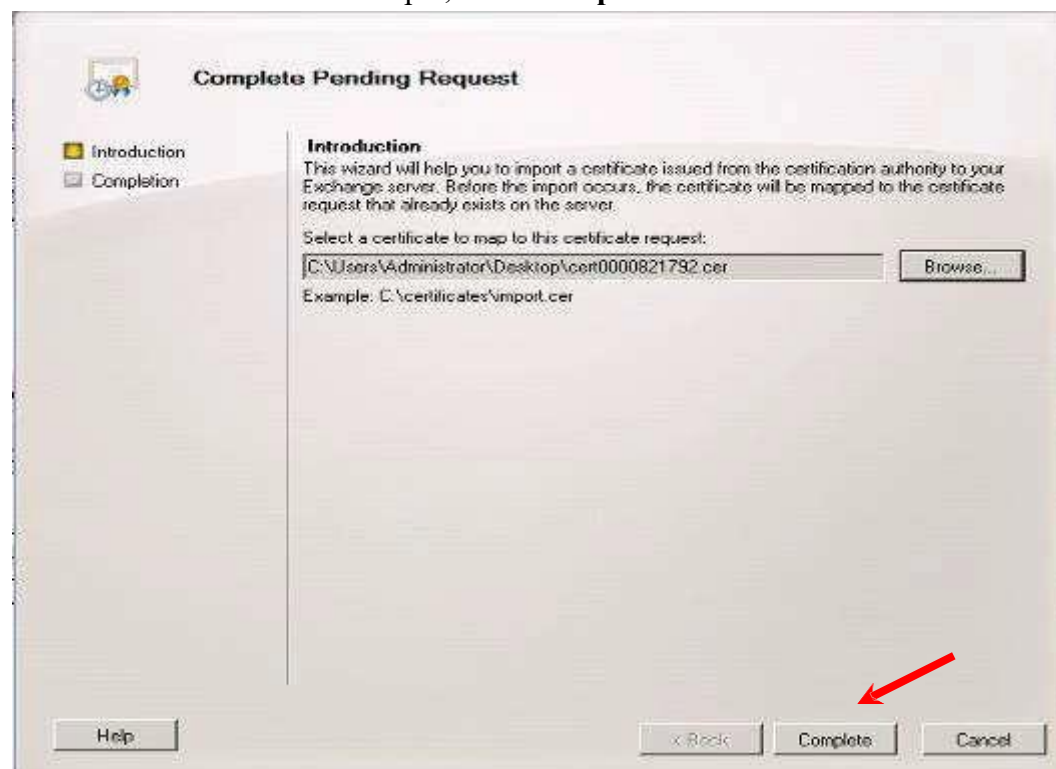
Figure 3: Hongkong Post Authority Revocation List (ARL) certificate has been successfully installed

E. Installing Server Certificate

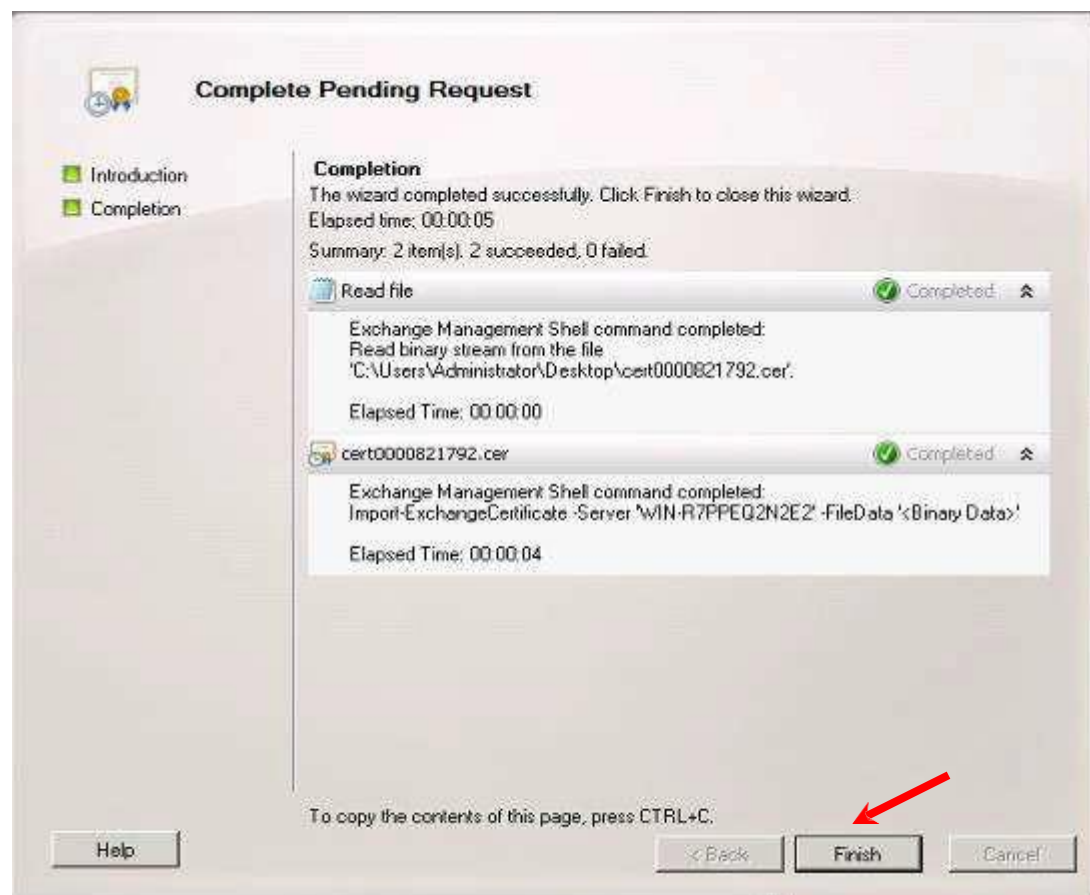
1. In **Exchange Management Console**, select **Server Configuration** by expanding the **Microsoft Exchange On-Premises**. Click the certificate you added before and choose **Complete Pending Request** from the right side of the window.



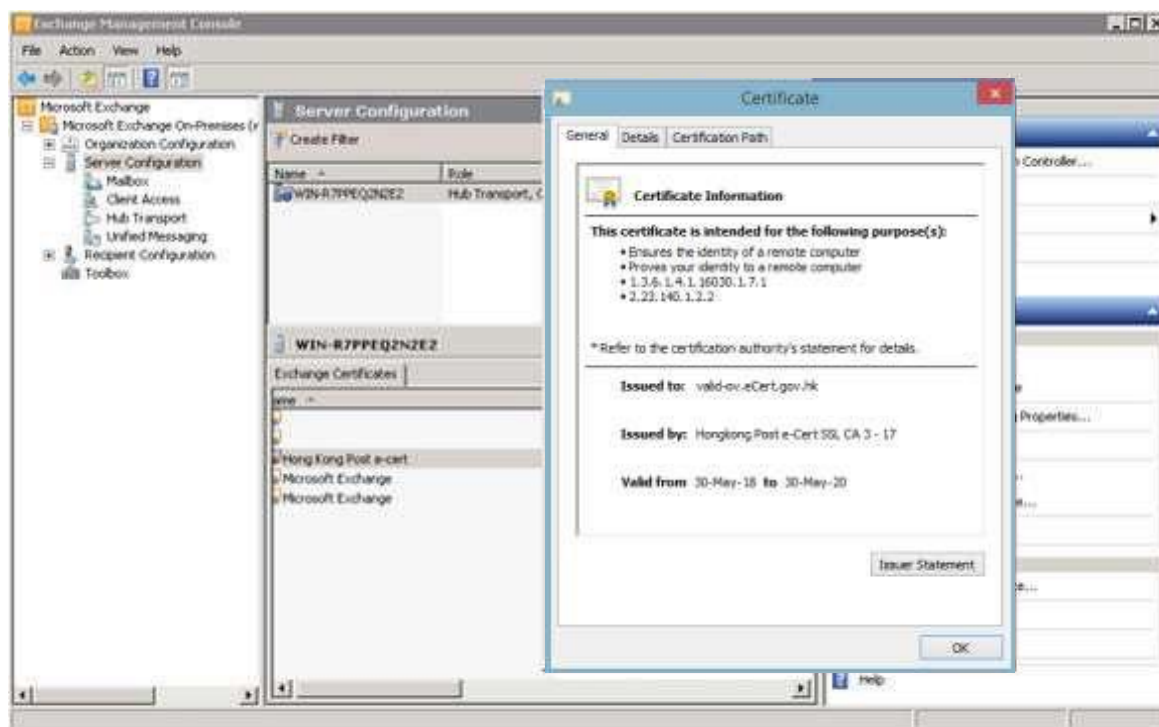
2. Click **Browse** to locate the **Hongkong Post e-Cert (Server)** certificate that you downloaded in Part C Step 7, click **Complete**.



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

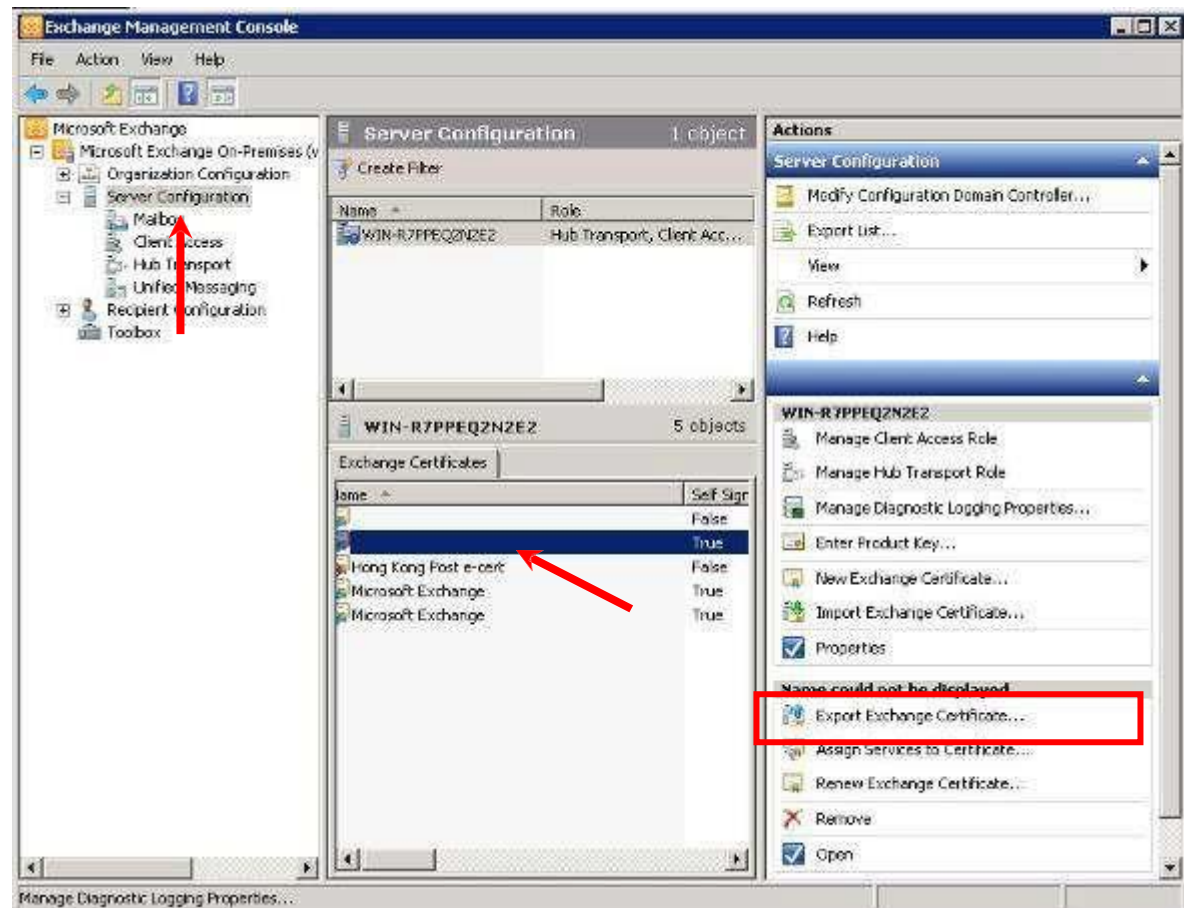


4. **Hongkong Post e-Cert (Server)** certificate has been successfully installed. You can check the detail information by double-clicking the certificate.

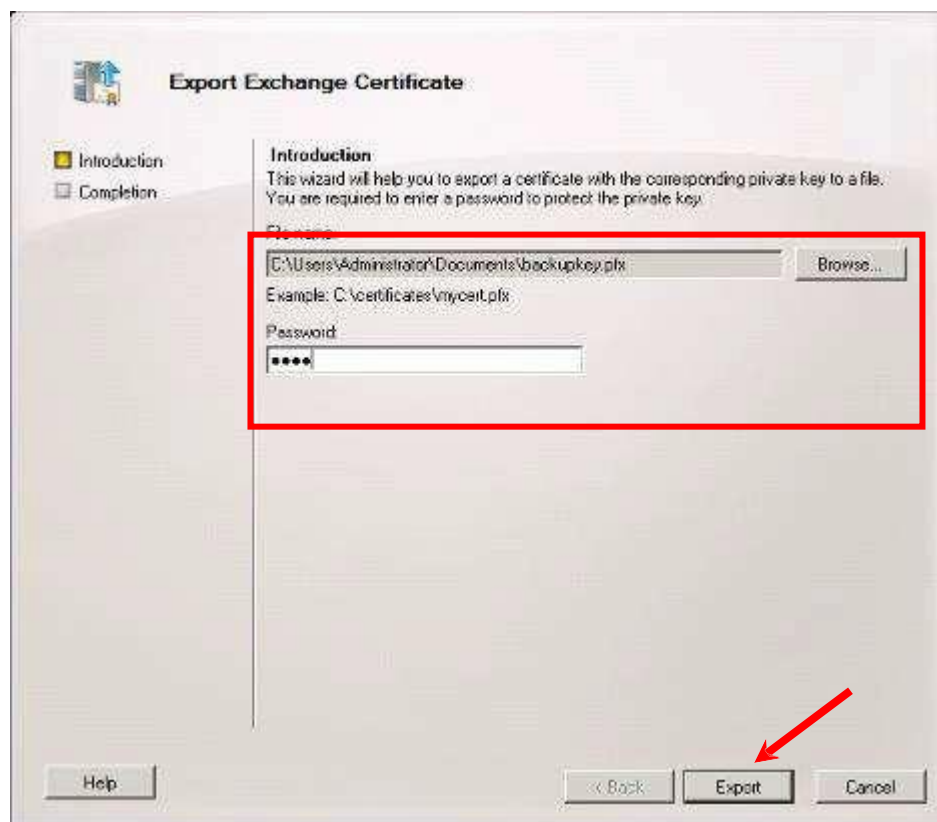


F. Backing up the Private Key

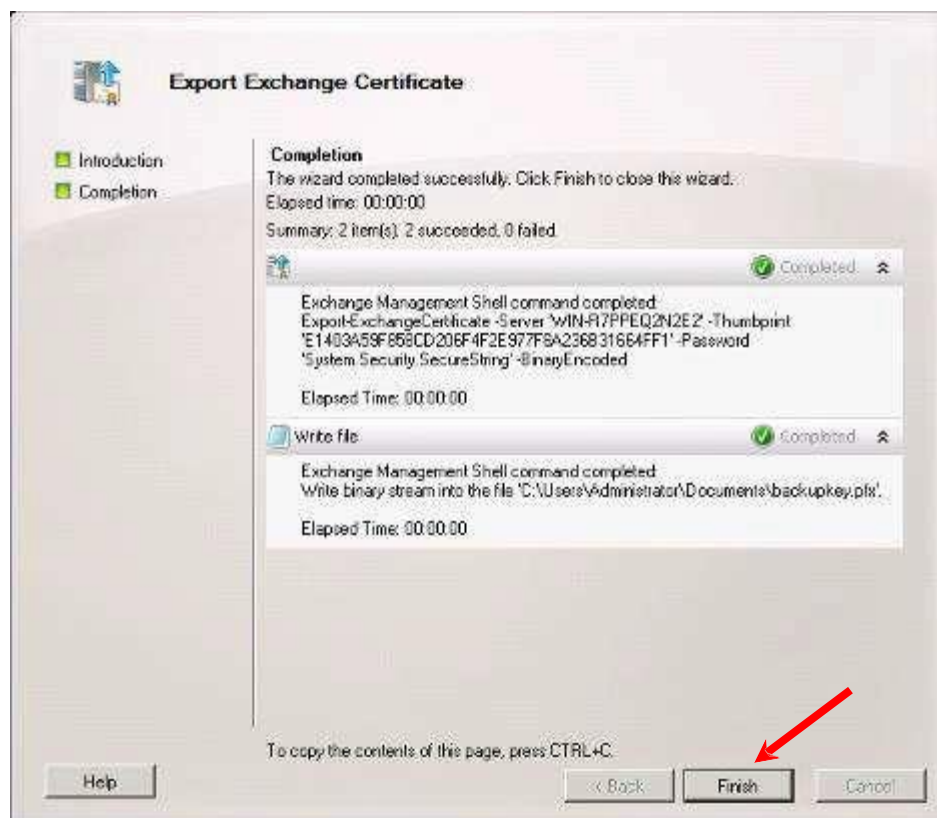
1. In **Exchange Management Console**, choose the certificate that you intend to export, and then click **Export Exchange Certificate**.



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.)

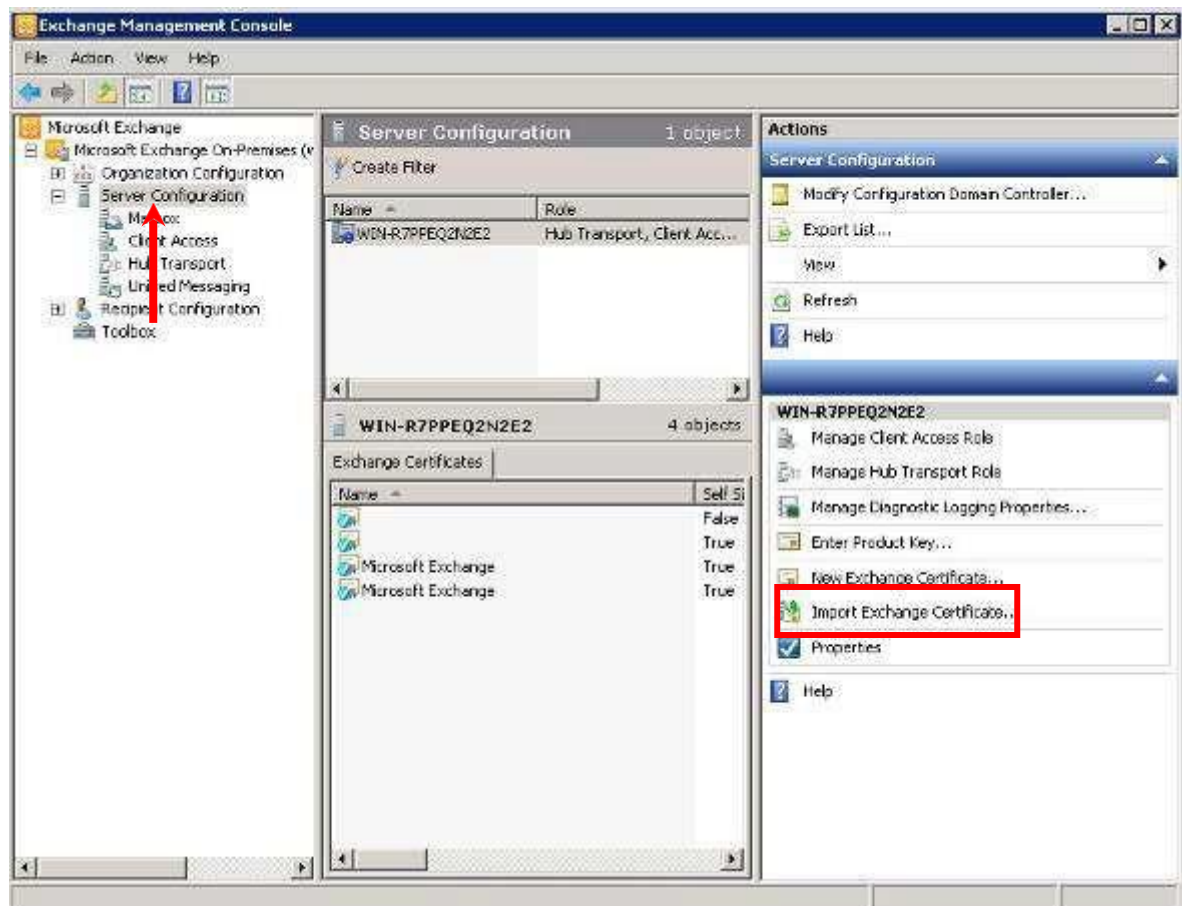


3. Click **Finish**. Hongkong Post e-Cert (Server) has been successful exported.

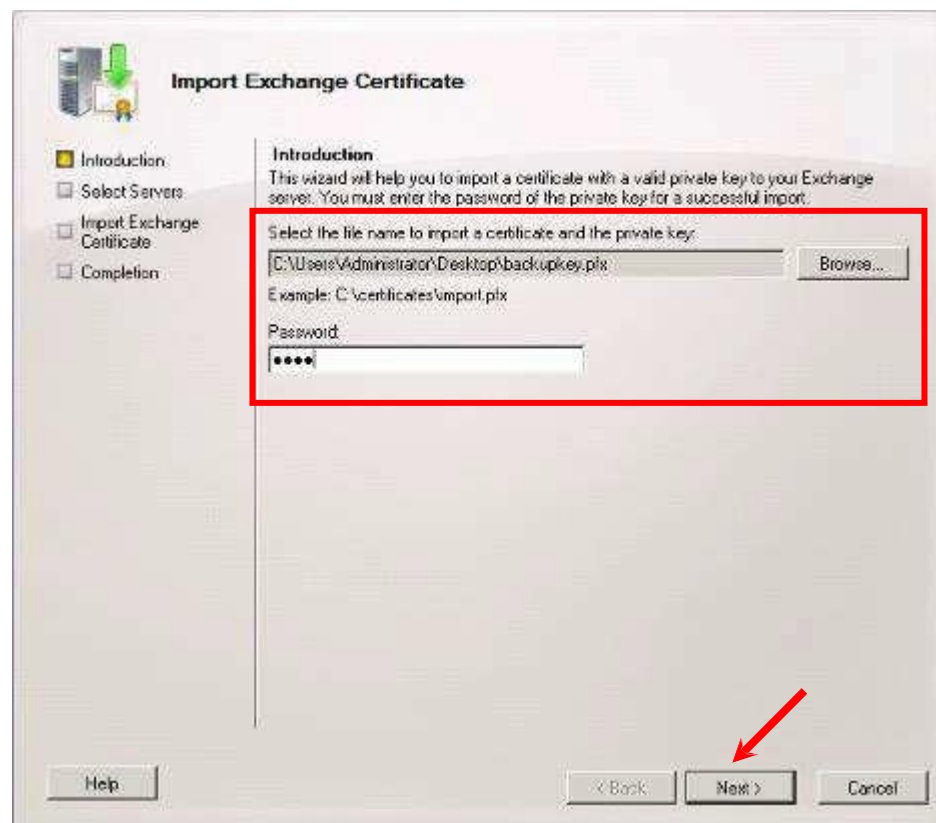


G. Restoring the Private Key

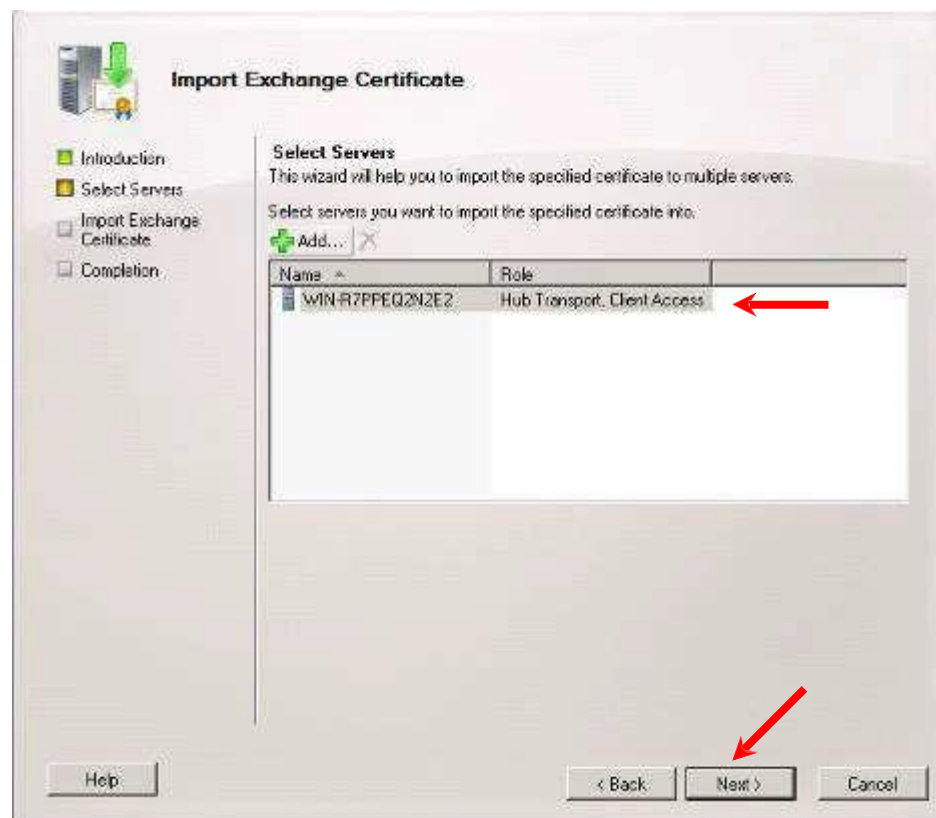
- 1 In **Exchange Management Console**, choose **Import Exchange Certificate** under **Server Configuration**.



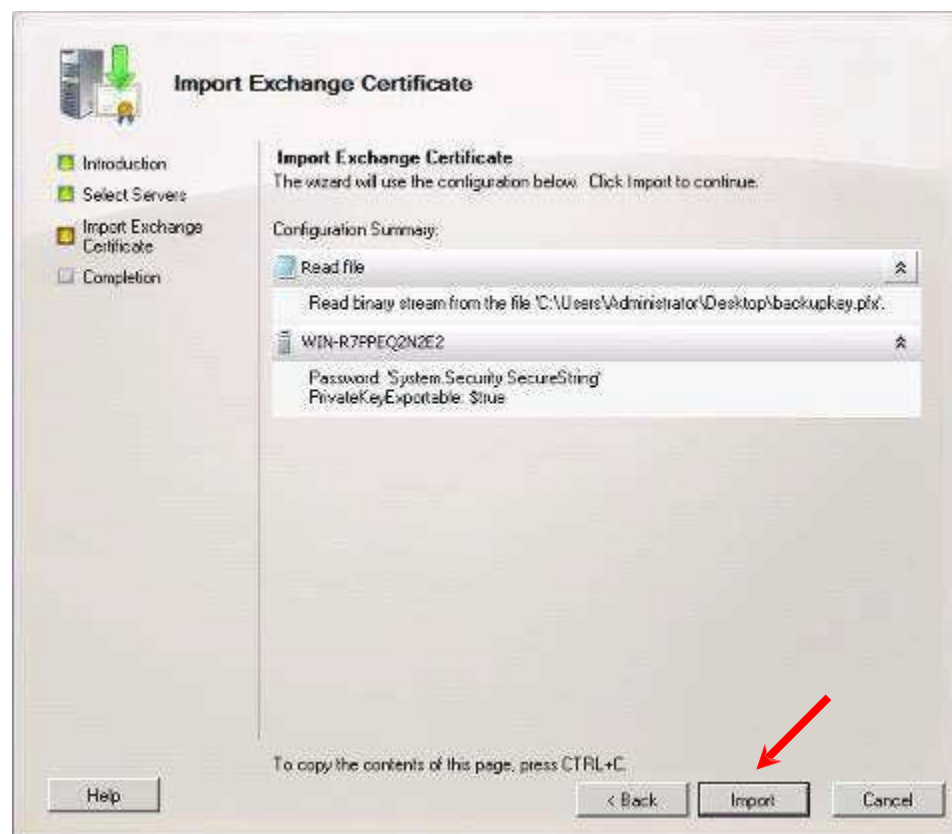
- 2 Select the private key you intend to import, and type in the password. Then, click **Next**.



- 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.

