Hongkong Post e-Cert
香港郵政電子核證

e-Cert (Server) User Guide

For Microsoft Exchange Server 2010

Revision Date: April 2025

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 15
Removing the old Sub CA Certificate (if applicable)....18
Installing Sub CA / Cross Certificate 19
Installing Authority Revocation List (ARL) 24
E. Installing Server Certificate 29
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 15
Removing the old Sub CA Certificate (if applicable)....18
Installing Sub CA / Cross Certificate 19
Installing Authority Revocation List (ARL) 24
E. Installing Server Certificate 29

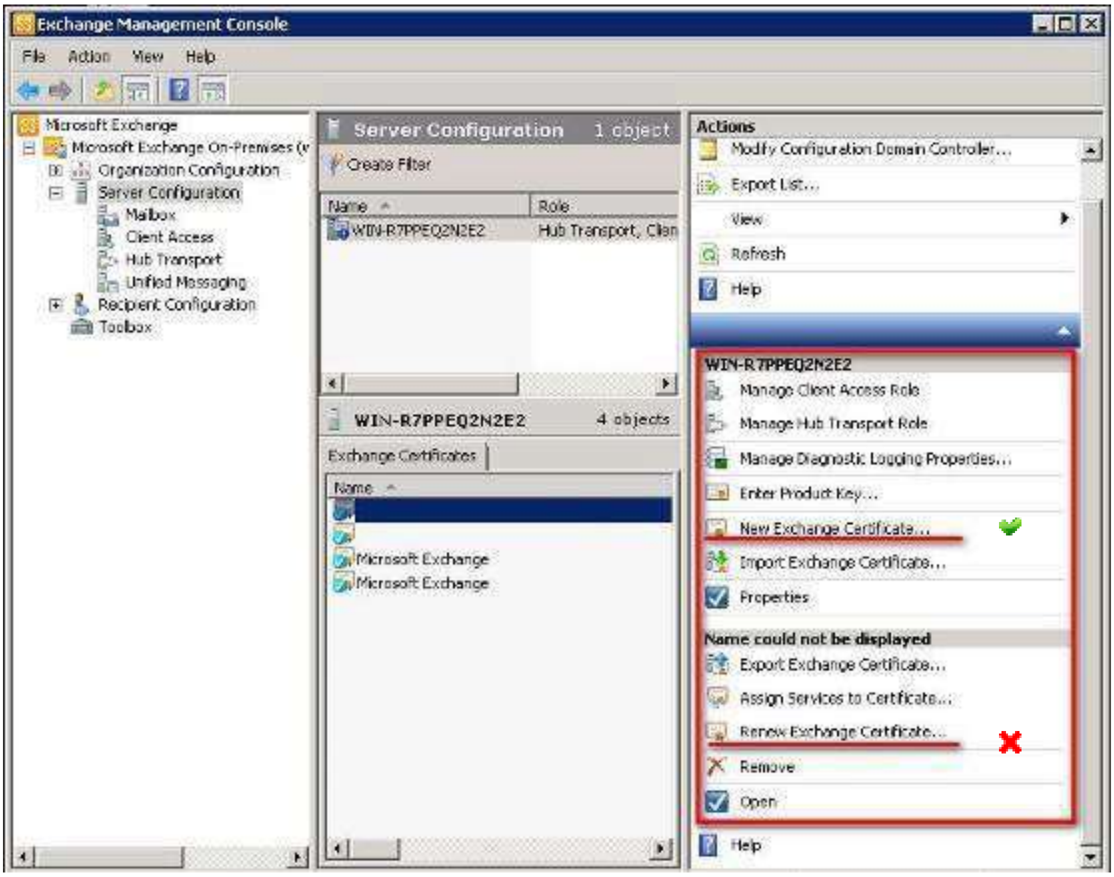
B. Generating Certificate Signing Request (CSR)

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

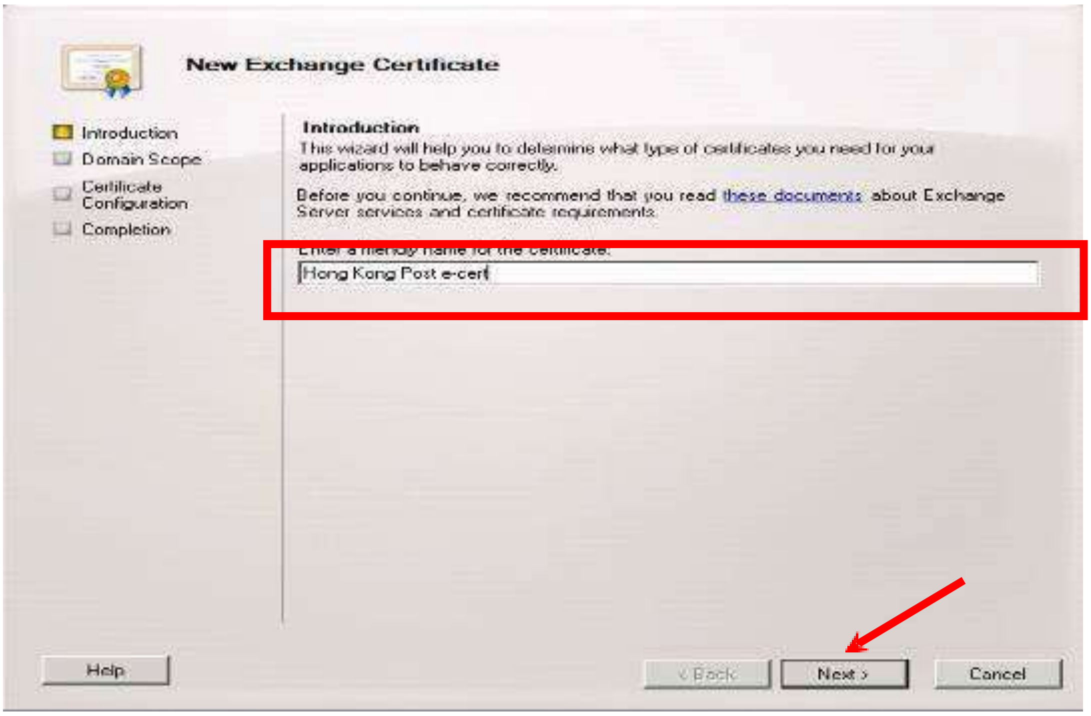
2 In Exchange Management Console, click **+** next to **Microsoft Exchange On-Premises** to expand the list of services.

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).*


Exchange Management Console
File Action View Help
Microsoft Exchange
Microsoft Exchange On-Premises
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Server Configuration 1 object
Create Filter
Name
Role
WIN-R7PPEQ2N2E2
Hub Transport, Clien
WIN-R7PPEQ2N2E2 4 objects
Exchange Certificates
Name
Microsoft Exchange
Microsoft Exchange
Actions
Modify Configuration Domain Controller...
Export List...
View
Refresh
Help
WIN-R7PPEQ2N2E2
Manage Client Access Role
Manage Hub Transport Role
Manage Diagnostic Logging Properties...
Enter Product Key...
New Exchange Certificate...
Import Exchange Certificate...
Properties
Name could not be displayed
Export Exchange Certificate...
Assign Services to Certificate...
Renew Exchange Certificate...
Remove
Open
Help

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



New Exchange Certificate

Introduction

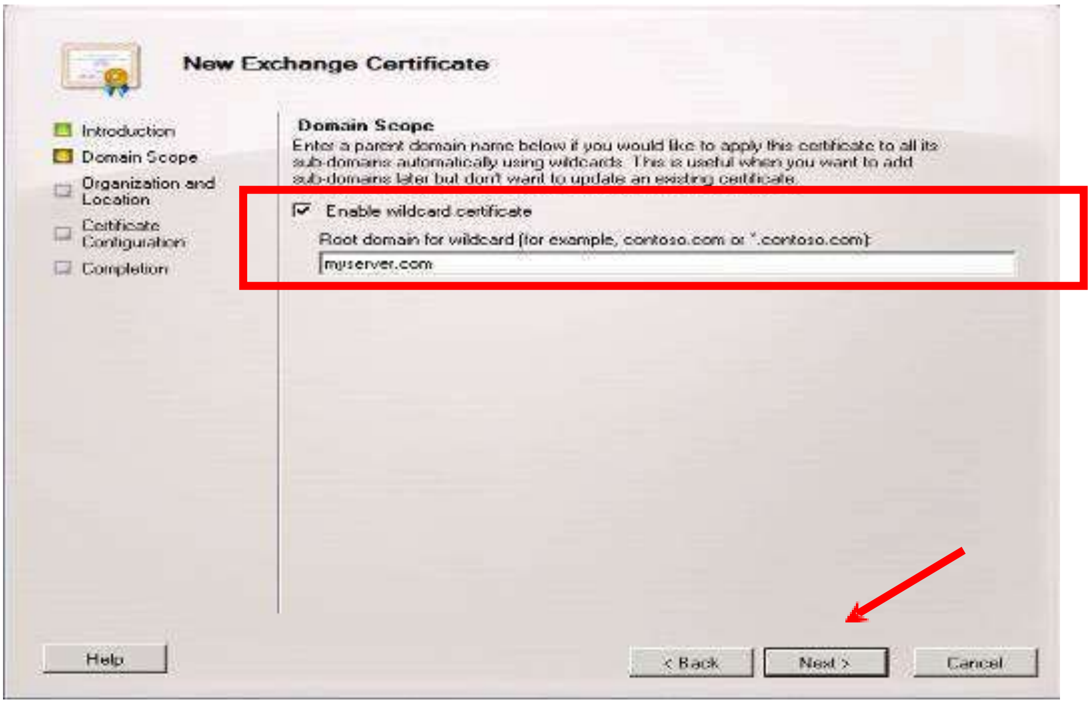
This wizard will help you to determine what type of certificates you need for your applications to behave correctly.

Before you continue, we recommend that you read these documents about Exchange Server services and certificate requirements.

Enter a friendly name for the certificate:

Hong Kong Post e-cert

5 In the Domain Scope section,



New Exchange Certificate

Domain Scope

Enter a parent domain name below if you would like to apply this certificate to all its sub-domains automatically using wildcards. This is useful when you want to add sub-domains later but don't want to update an existing certificate.

☑ Enable wildcard certificate

Root domain for wildcard (for example, contoso.com or *.contoso.com):

myserver.com

- 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.

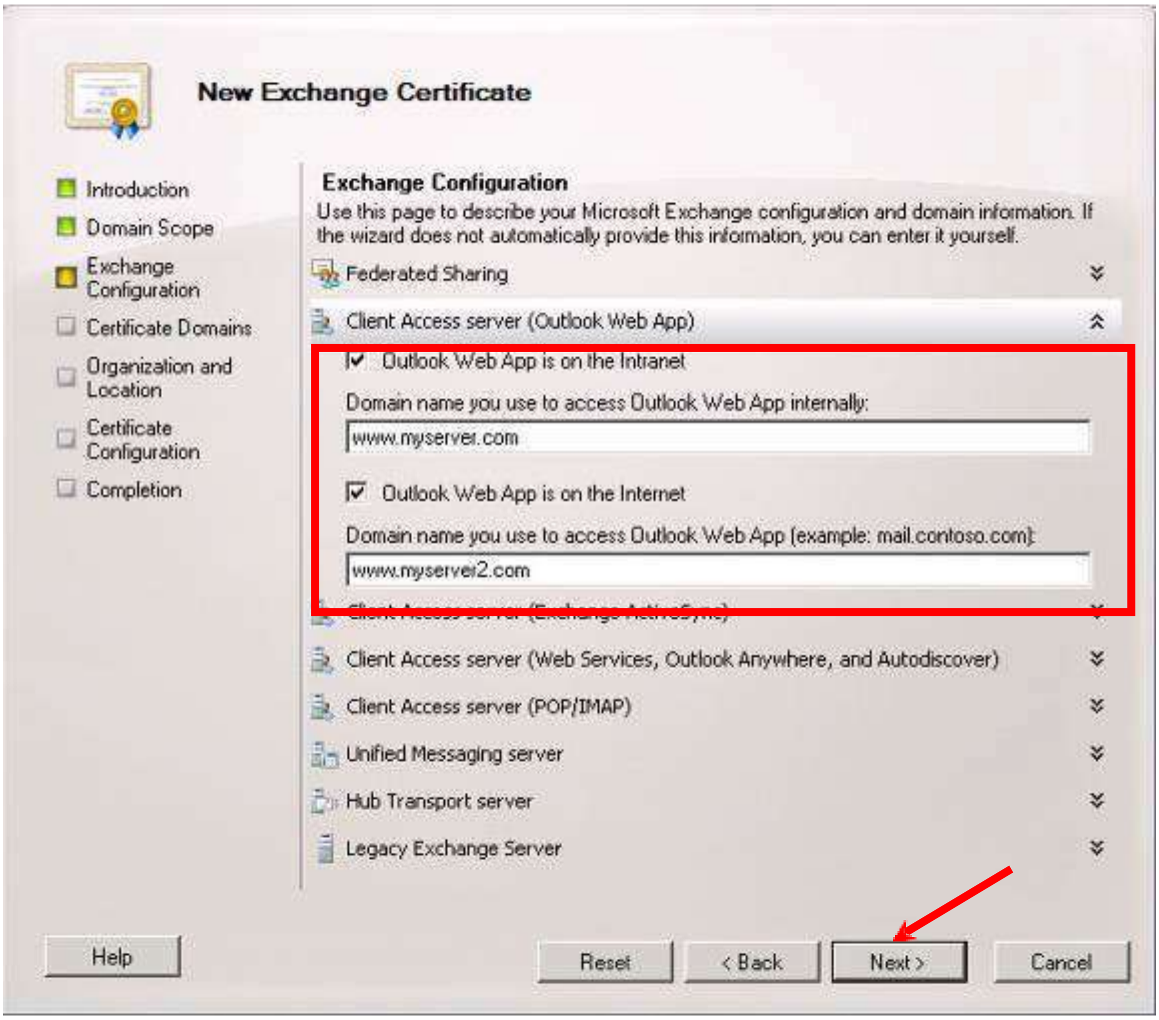
> ***Note:*** *Please make sure that* ***root domain for wildcard*** *is filled with* ***Server Name with Wildcard*** *(both the names with or without wildcard component, i.e. the asterisk '*'are acceptable).*

- 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.*



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

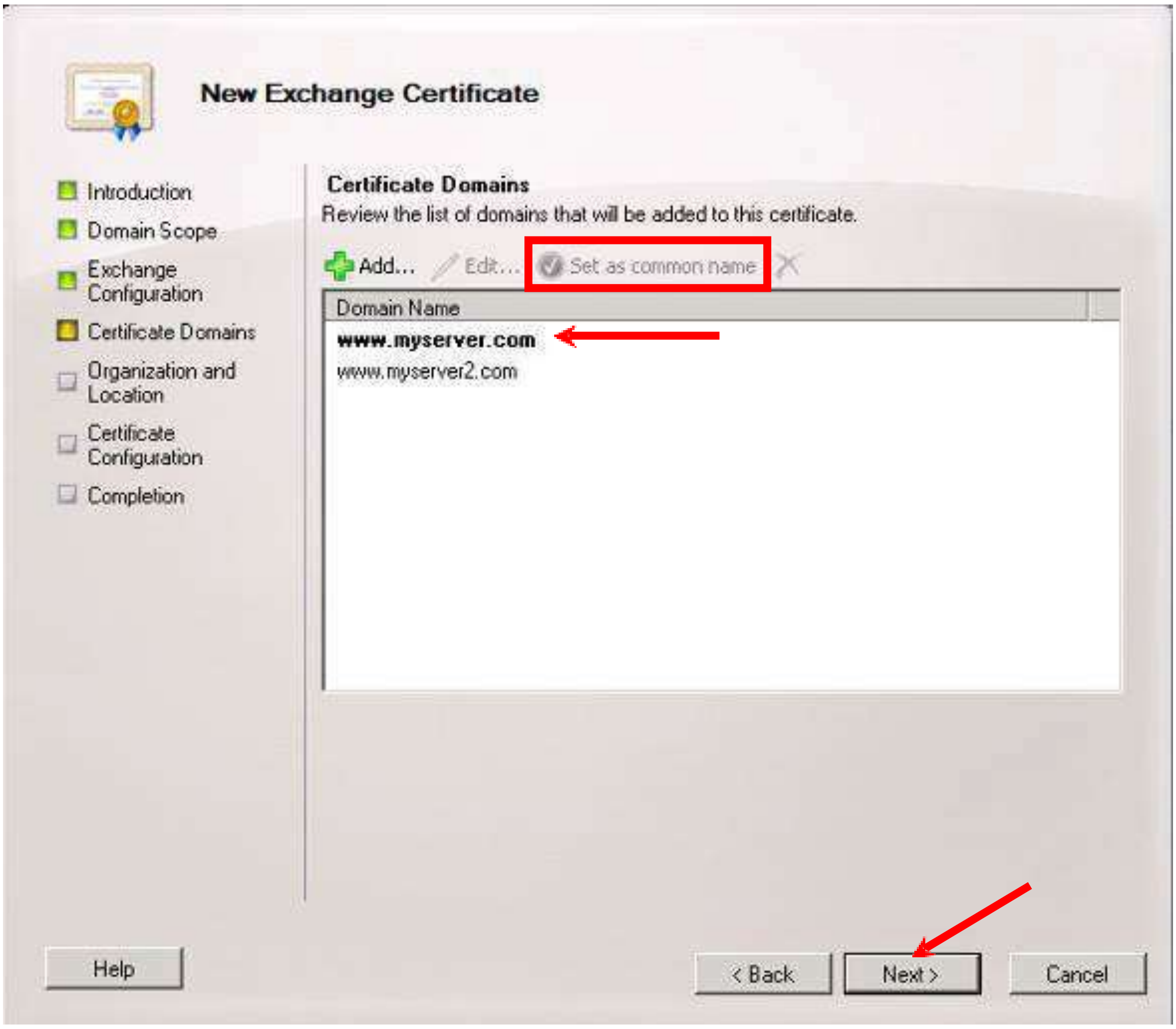
☑ Outlook Web App is on the Internet

Domain name you use to access Outlook Web App (example: mail.contoso.com):

www.myserver2.com

Introduction
Domain Scope
Exchange Configuration
Certificate Domains
Organization and Location
Certificate Configuration
Completion
Federated Sharing
Client Access server (Outlook Web App)
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)



New Exchange Certificate

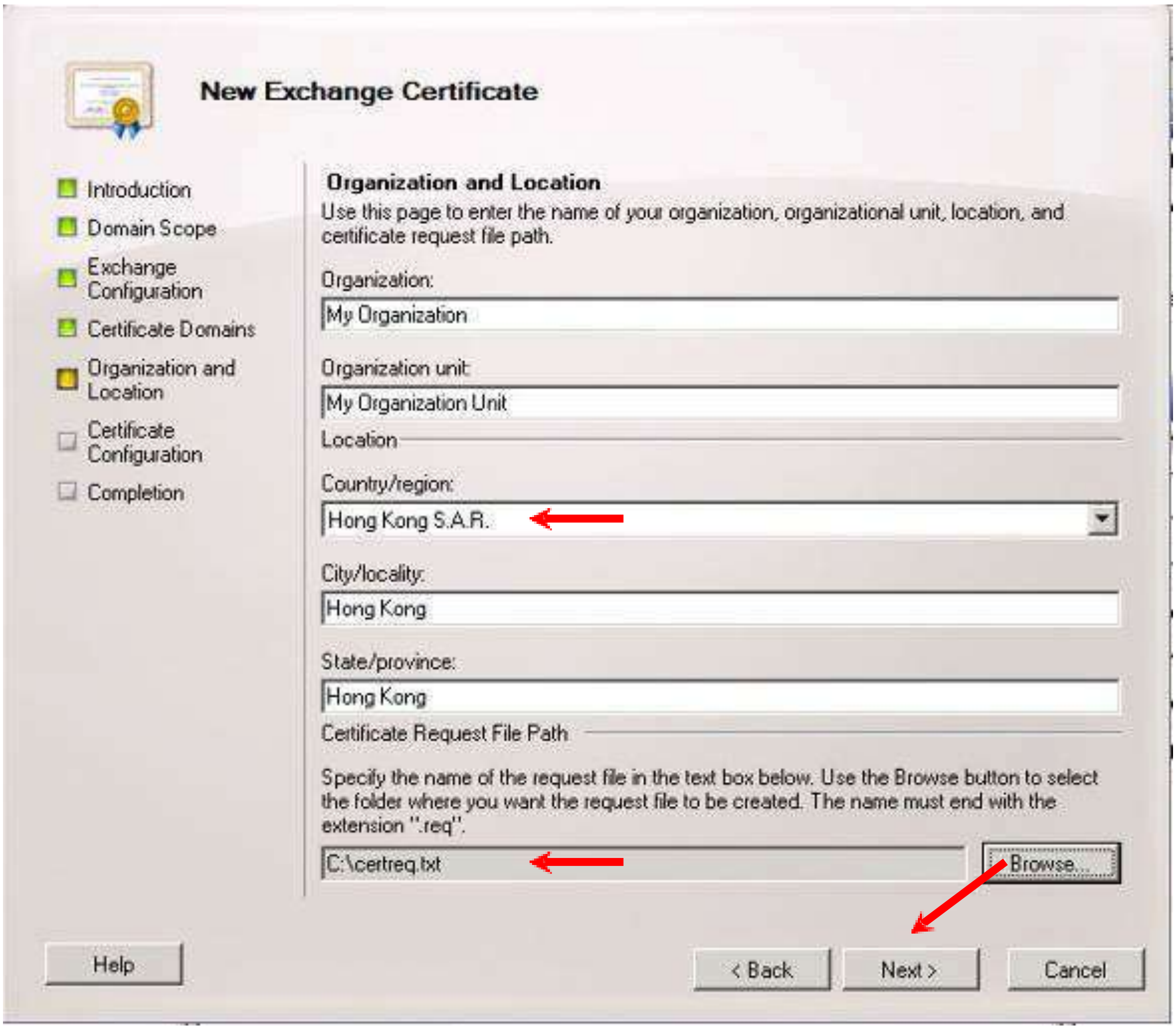
Certificate Domains

Review the list of domains that will be added to this certificate.

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.*



New Exchange Certificate

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

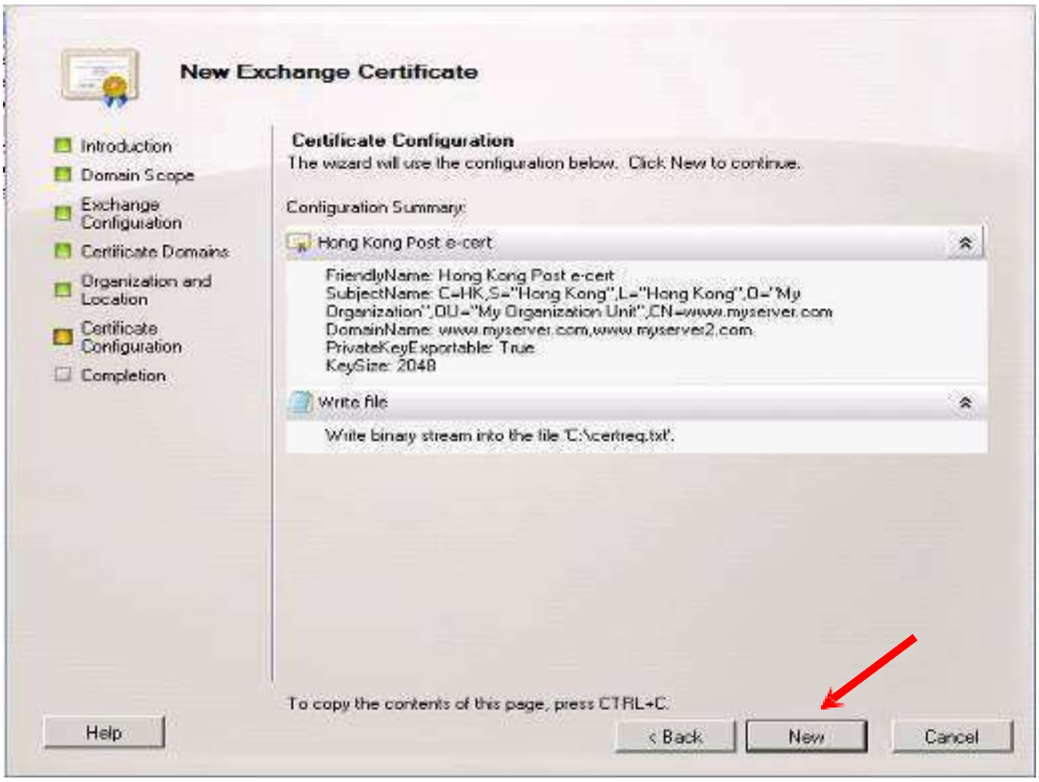
State/province: Hong Kong

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

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



Certificate Configuration

The wizard will use the configuration below. Click New to continue.

Configuration Summary:

Hong Kong Post e-cert

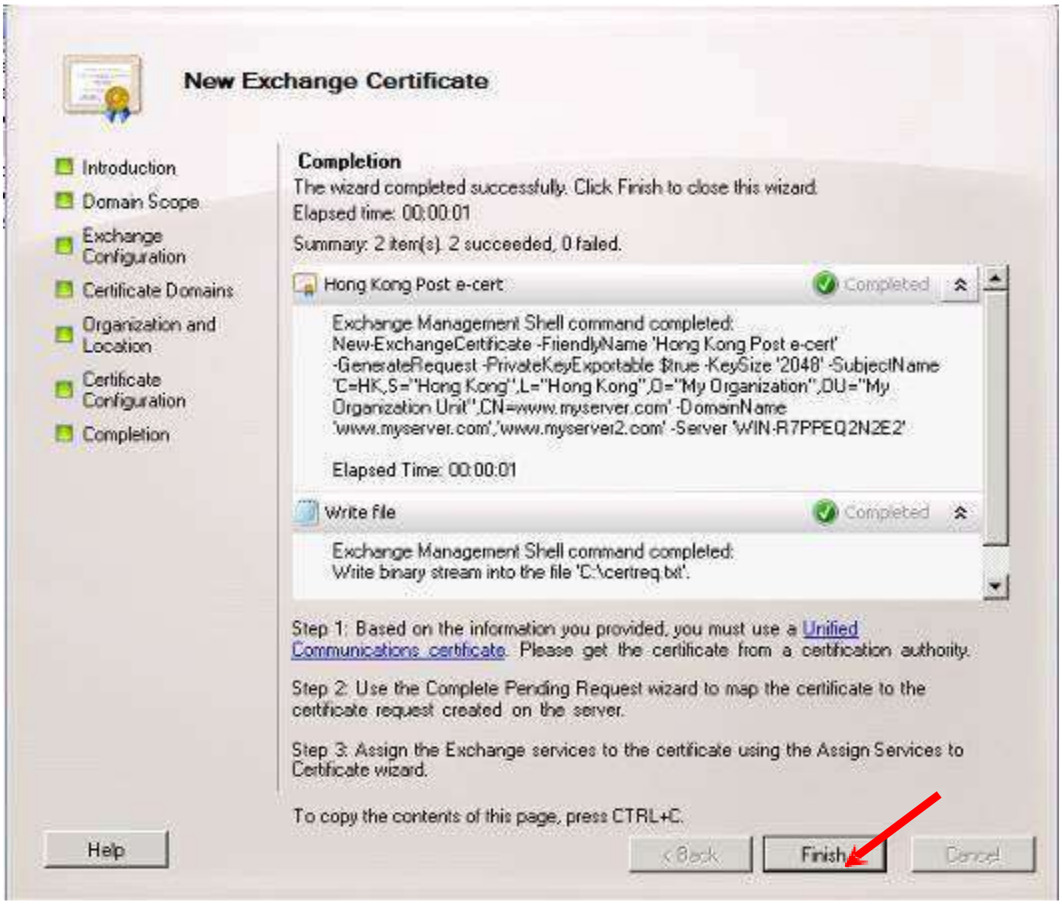
```
FriendlyName: Hong Kong Post e-cert
SubjectName: C=HK,S="Hong Kong",L="Hong Kong",O="My
Organization",OU="My Organization Unit",CN=www.myserver.com
DomainName: www.myserver.com,www.myserver2.com
PrivateKeyExportable: True
KeySize: 2048
```

Write file

Write binary stream into the file 'C:\certreq.txt'.

To copy the contents of this page, press CTRL+C.

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



Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:01

Summary: 2 item(s). 2 succeeded, 0 failed.

Hong Kong Post e-cert — Completed

```
Exchange Management Shell command completed:
New-ExchangeCertificate -FriendlyName 'Hong Kong Post e-cert'
-GenerateRequest -PrivateKeyExportable $true -KeySize '2048' -SubjectName
'C=HK,S="Hong Kong",L="Hong Kong",O="My Organization",OU="My
Organization Unit",CN=www.myserver.com' -DomainName
'www.myserver.com','www.myserver2.com' -Server 'WIN-R7PPEQ2N2E2'

Elapsed Time: 00:00:01
```

Write file — Completed

```
Exchange Management Shell command completed:
Write binary stream into the file 'C:\certreq.txt'.
```

Step 1: Based on the information you provided, you must use a Unified Communications certificate. Please get the certificate from a certification authority.

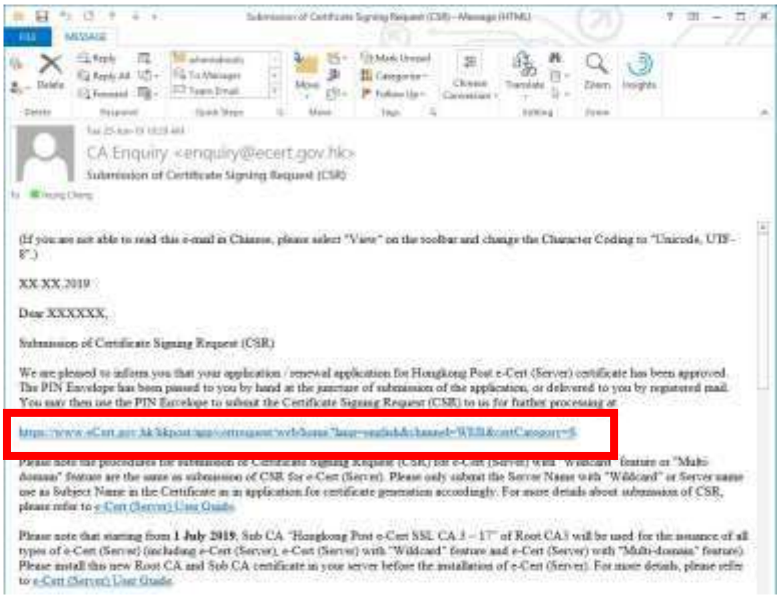
Step 2: Use the Complete Pending Request wizard to map the certificate to the certificate request created on the server.

Step 3: Assign the Exchange services to the certificate using the Assign Services to Certificate wizard.

To copy the contents of this page, press CTRL+C.

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.



CA Enquiry <enquiry@ecert.gov.hk>

Submission of Certificate Signing Request (CSR)

(If you are not able to read this e-mail in Chinese, please select "View" on the toolbar and change the Character Coding to "Unicode, UTF-8".)

XX XX 2019

Dear XXXXXX,

Submission of Certificate Signing Request (CSR)

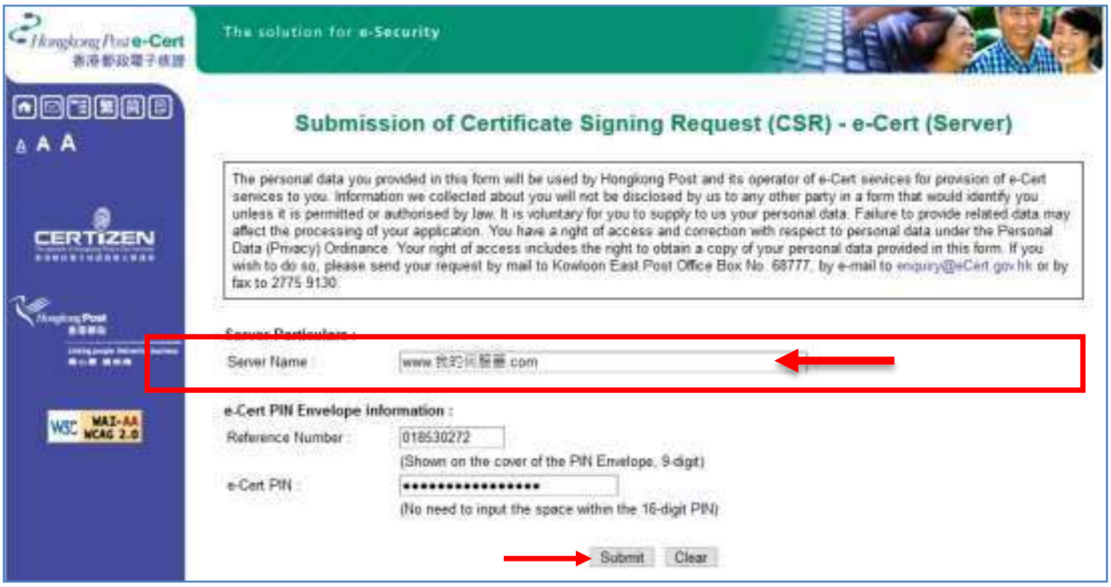
We are pleased to inform you that your application / renewal application for Hongkong Post e-Cert (Server) certificate has been approved. The PIN Envelope has been passed to you by hand at the juncture of submission of the application, or delivered to you by registered mail. You may then use the PIN Envelope to submit the Certificate Signing Request (CSR) to us for further processing at

https://www.eCert.gov.hk/hkpost/app/certrequest/web/home?lang=english&channel=WEB&certCategory=5

Please note the procedures for submission of Certificate Signing Request (CSR) for e-Cert (Server) with "Wildcard" feature or "Multi-domain" feature are the same as submission of CSR for e-Cert (Server). Please only submit the Server Name with "Wildcard" or Server name use as Subject Name in the Certificate as in application for certificate generation accordingly. For more details about submission of CSR, please refer to e-Cert (Server) User Guide.

Please note that 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) (including e-Cert (Server), e-Cert (Server) with "Wildcard" feature and e-Cert (Server) with "Multi-domain" feature). Please install this new Root CA and Sub CA certificate in your server before the installation of e-Cert (Server). For more details, please refer to e-Cert (Server) User Guide.

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**.



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. You have a right of access and correction with respect to personal data under the Personal Data (Privacy) Ordinance. Your right of access includes the right to obtain a copy of your personal data provided in this form. If you wish to do so, please send your request by mail to Kowloon East Post Office Box No. 68777, by e-mail to enquiry@eCert.gov.hk or by fax to 2775 9130.

Server Particulars :

Server Name : www.我的伺服器.com

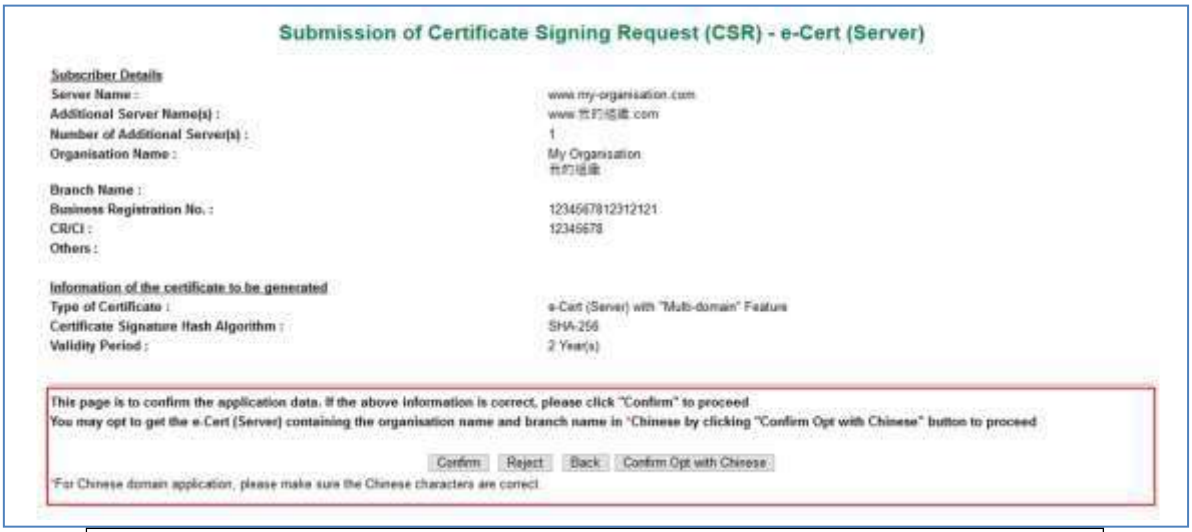
e-Cert PIN Envelope Information :

Reference Number : 018530272
(Shown on the cover of the PIN Envelope, 9-digit)

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

Submit Clear

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.)



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

Subscriber Details	
Server Name :	www.my-organisation.com
Additional Server Name(s) :	www.我的組織.com
Number of Additional Server(s) :	1
Organisation Name :	My Organisation 我的組織
Branch Name :	
Business Registration No. :	1234567812312121
CR/CI :	12345678
Others :	
Information of the certificate to be generated	
Type of Certificate :	e-Cert (Server) with "Multi-domain" Feature
Certificate Signature Hash Algorithm :	SHA-256
Validity Period :	2 Year(s)

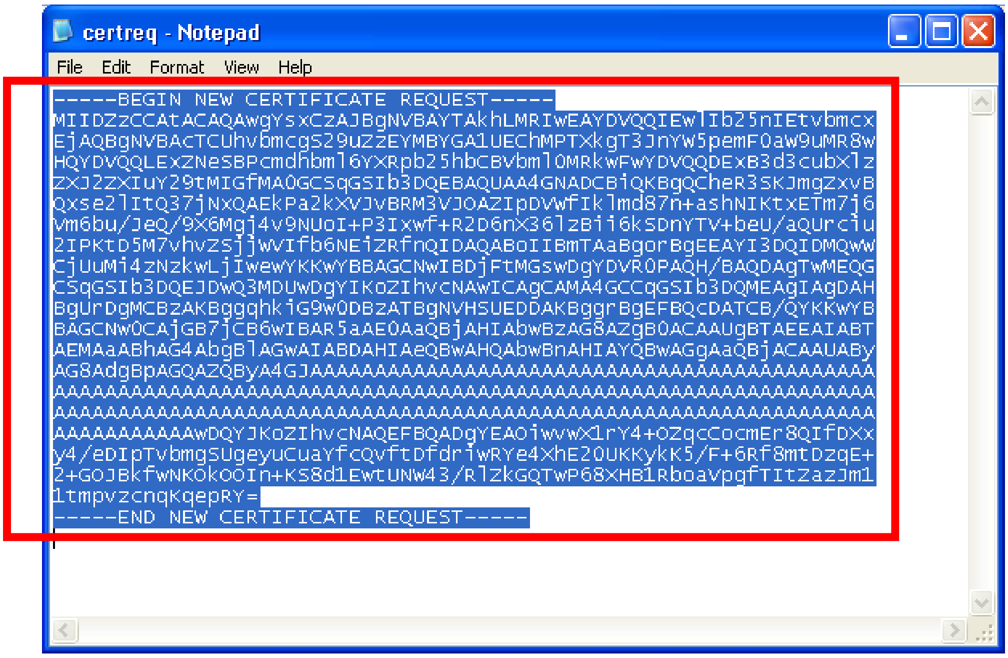
This page is to confirm the application data. If the above information is correct, please click "Confirm" to proceed

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.

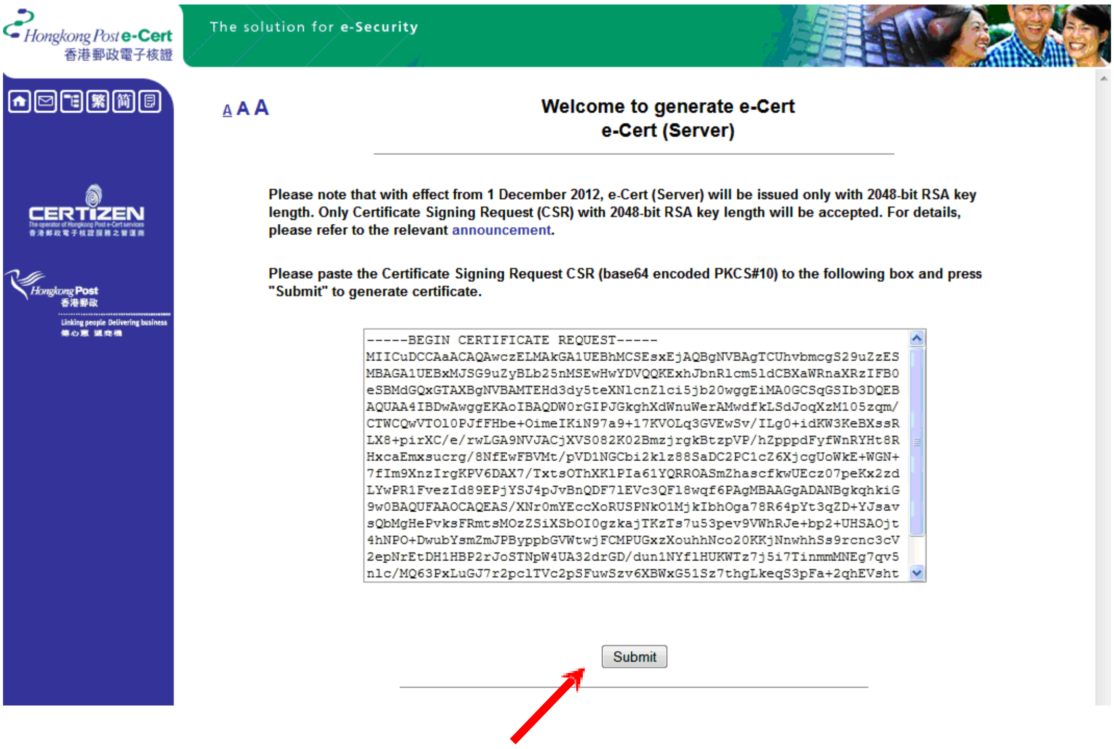
*Note: If English and Chinese organisation name and/or branch name have been provided at the application form, in order to generate e-Cert (Server) with Chinese organisation name at Subject O field, click the button "**Confirm Opt with Chinese**" to proceed.*

4. 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 6 for the location of certificate request file.)



```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDZzCCAtACAQAwgYsxCzAJBgNVBAYTAkhLMRIwEAYDVQQIEwlIb25nIEtvbmcx
EjAQBgNVBAcTCUhvbmcgS29uZzEYMBYGA1UEChMPTXkgT3JnYW5pemF0aW9uMR8w
HQYDVQQLExZNeSBPcmdhbml6YXRpb25hbCBVbml0MRkwFwYDVQQDExB3d3cubXlz
ZXJ2ZXIuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCheR3SKJmgZxvB
Qxse2lItQ37jNxQAEkPa2kXVJvBRM3VJOAZIpDVwfIklmd87n+ashNIKtxETm7j6
Vm6bu/JeQ/9X6Mgj4v9NUoI+P3Ixwf+R2D6nX36lzBii6kSDnYTV+beU/aQUrciu
2IPKtD5M7vhvzSjjwVIfb6NEizRfnQIDAQABoIIBmTAaBgorBgEEAYI3DQIDMQwW
CjUuMi4zNzkwLjIwewYKKwYBBAGCNwIBDjFtMGswDgYDVR0PAQH/BAQDAgTwMEQG
CSqGSIb3DQEJDwQ3MDUwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDAH
BgUrDgMCBzAKBggqhkiG9w0DBzATBgNVHSUEDDAKBggrBgEFBQcDATCB/QYKKwYB
BAGCNw0CAjGB7jCB6wIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAAUgBTAEEAIABT
AEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgAaQBjACAAUABy
AG8AdgBpAGQAZQByA4GJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAwDQYJKoZIhvcNAQEFBQADgYEAOiwvwX1rY4+OZqcCocmEr8QIfDXx
y4/eDIpTvbmgSUgeyuCuaYfcQvftDfdriwRYe4XhE2OUKKykK5/F+6Rf8mtDzqE+
2+GOJBkfwNKOkOOIn+KS8d1EwtUNW43/RlZkGQTwP68XHB1RboavpgfTItZazJm1
1tmpvzcnqKqepRY=
-----END NEW CERTIFICATE REQUEST-----
```

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



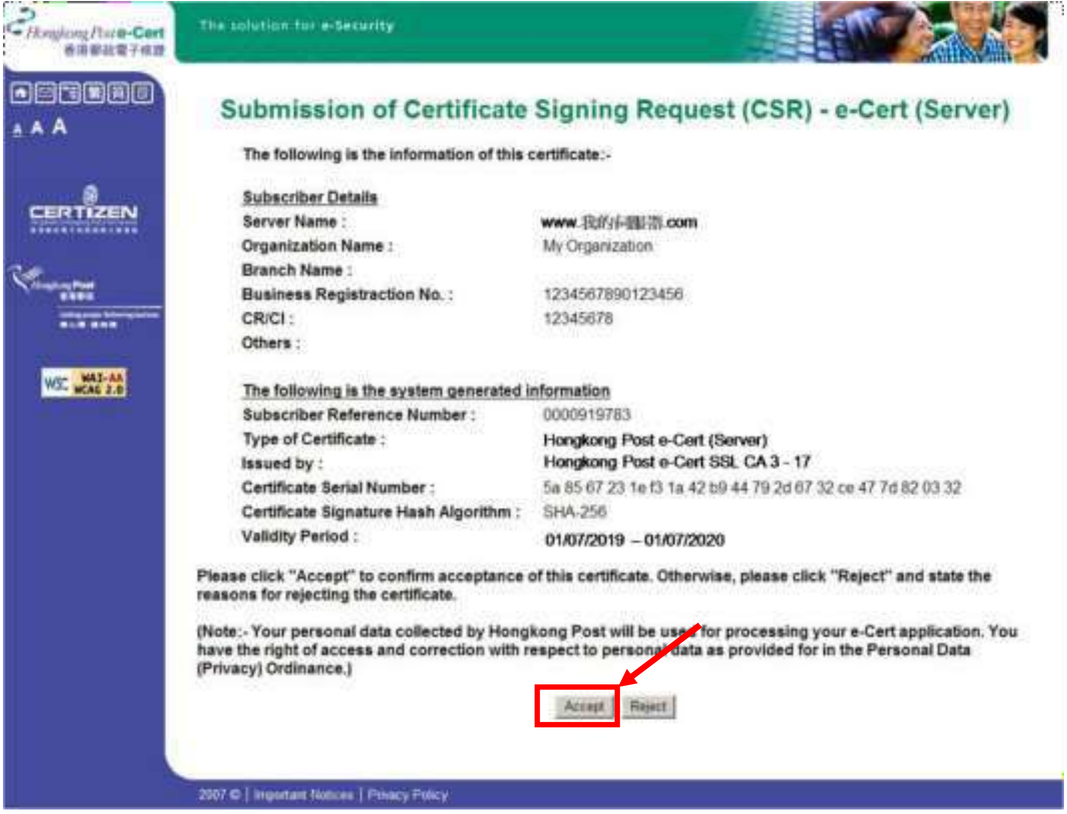
Welcome to generate e-Cert
e-Cert (Server)

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-----
MIICuDCCAaACAQAwczELMAkGA1UEBhMCSEsxEjAQBgNVBAgTCUhvbmcgS29uZzES
MBAGA1UEBxMJSG9uZyBLb25nMSEwHwYDVQQKExhJbnRlcm5ldCBXaWRnaXRzIFB0
eSBMdGQxGTAXBgNVBAMTEHd3dy5teXNlcnZlci5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQDW0rGIPJGkghXdWnuWerAMwdfkLSdJoqXzM105zqm/
CTWCQwVTOl0PJfFHbe+OimeIKiN97a9+17KVOLq3GVEwSv/ILg0+idKW3KeBXssR
LX8+pirXC/e/rwLGA9NVJACjXVS082K02BmzjrgkBtzpVP/hZpppdFyfWnRYHt8R
HxcaEmxsucrg/8NfEwFBVMt/pVD1NGCbi2klz88SaDC2PC1cZ6XjcgUoWkE+WGN+
7fIm9XnzIrgKPV6DAX7/TxtsOThXKlPIa61YQRROASmZhascfkwUEcz07peKx2zd
LYwPR1FvezId89EPjYSJ4pJvBnQDF7lEVc3QFl8wqf6PAgMBAAGgADANBgkqhkiG
9w0BAQUFAAOCAQEAS/XNr0mYEccXoRUSPNkO1MjkIbhOga78R64pYt3qZD+YJsav
sQbMgHePvksFRmtsMOzZSiXSbOI0gzkajTKzTs7u53pev9VWhRJe+bp2+UHSAOjt
4hNPO+DwubYsmZmJPByppbGVWtwjFCMPUGxzXouhhNco20KKjNnwhhSs9rcnc3cV
2epNrEtDH1HBP2rJoSTNpW4UA32drGD/dun1NYflHUKWTz7j5i7TinmmMNEg7qv5
nlc/MQ63PxLuGJ7r2pclTVc2pSFuwSzv6XBWxG51Sz7thgLkeqS3pFa+2qhEVsht
```

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



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

The following is the information of this certificate:-

Subscriber Details

Server Name :	www.我的小圖形.com
Organization Name :	My Organization
Branch Name :	
Business Registraction No. :	1234567890123456
CR/CI :	12345678
Others :	

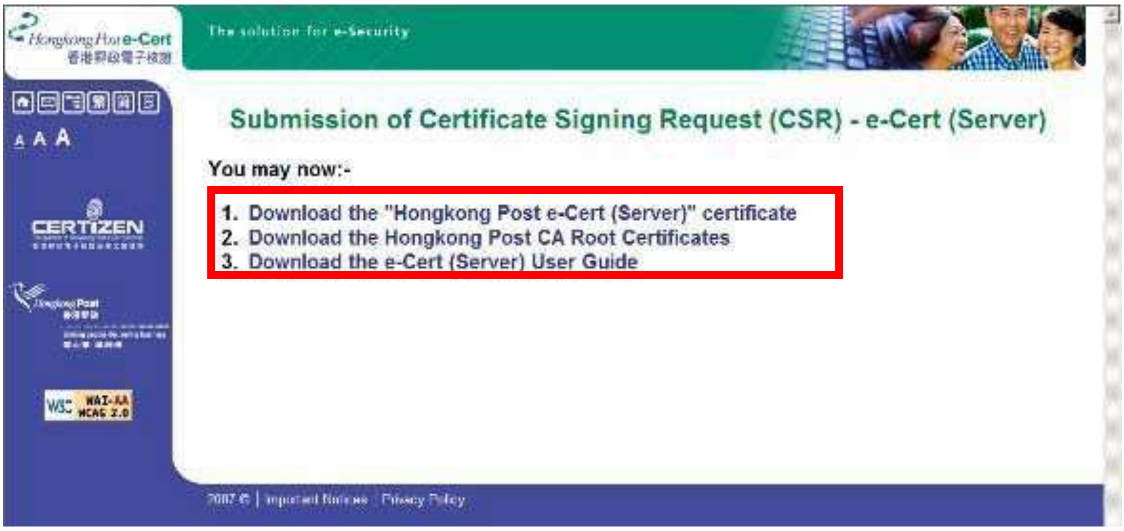
The following is the system generated information

Subscriber Reference Number :	0000919783
Type of Certificate :	Hongkong Post e-Cert (Server)
Issued by :	Hongkong Post e-Cert SSL CA 3 - 17
Certificate Serial Number :	5a 85 67 23 1e f3 1a 42 b9 44 79 2d 67 32 ce 47 7d 82 03 32
Certificate Signature Hash Algorithm :	SHA-256
Validity Period :	01/07/2019 – 01/07/2020

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.)

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



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

<u>Note:</u>

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 byRoot 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:*

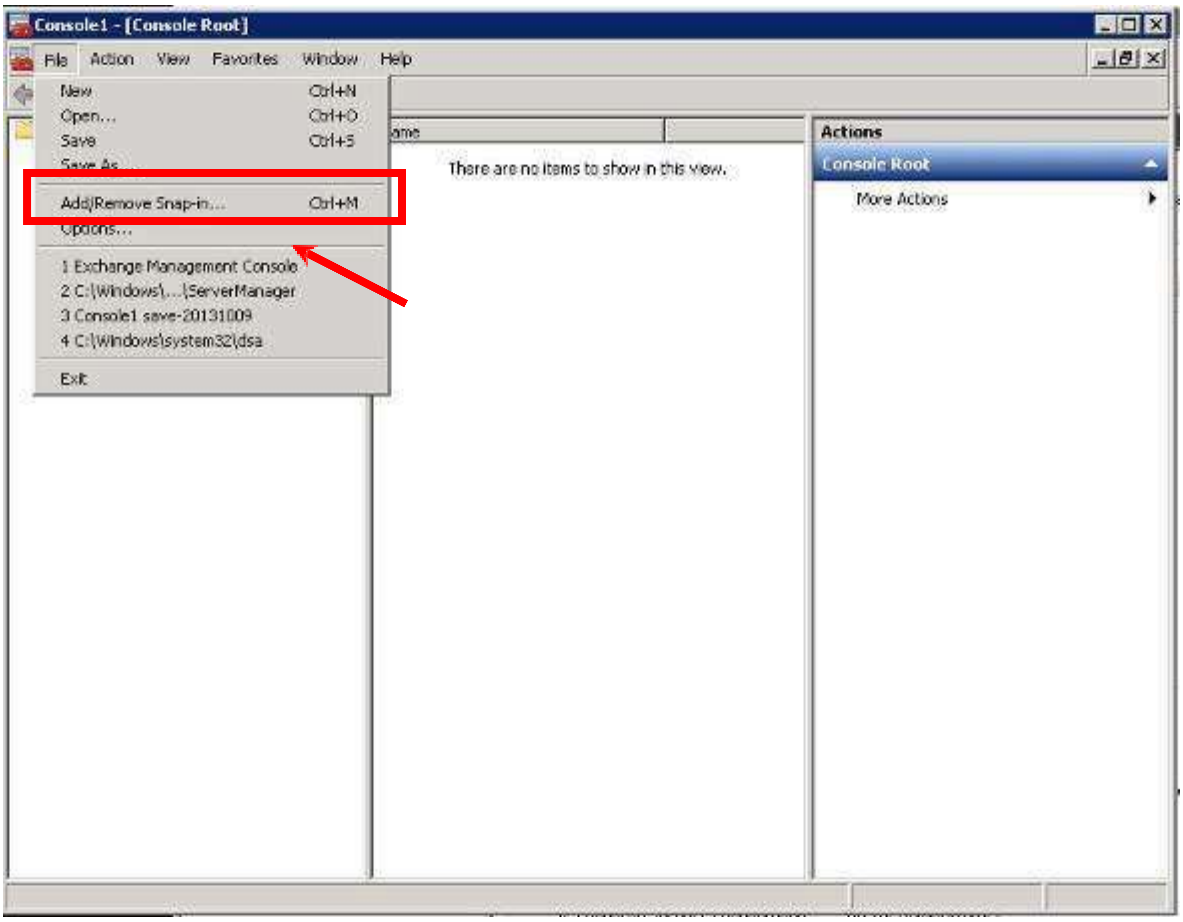
   Install the Sub CA "Hongkong Post e-Cert EV SSL CA 3 - 17" issued by Root CA3. Click the following link to download:

   http://www1.ecert.gov.hk/root/ecert_ev_ssl_ca_3-17_pem.crt

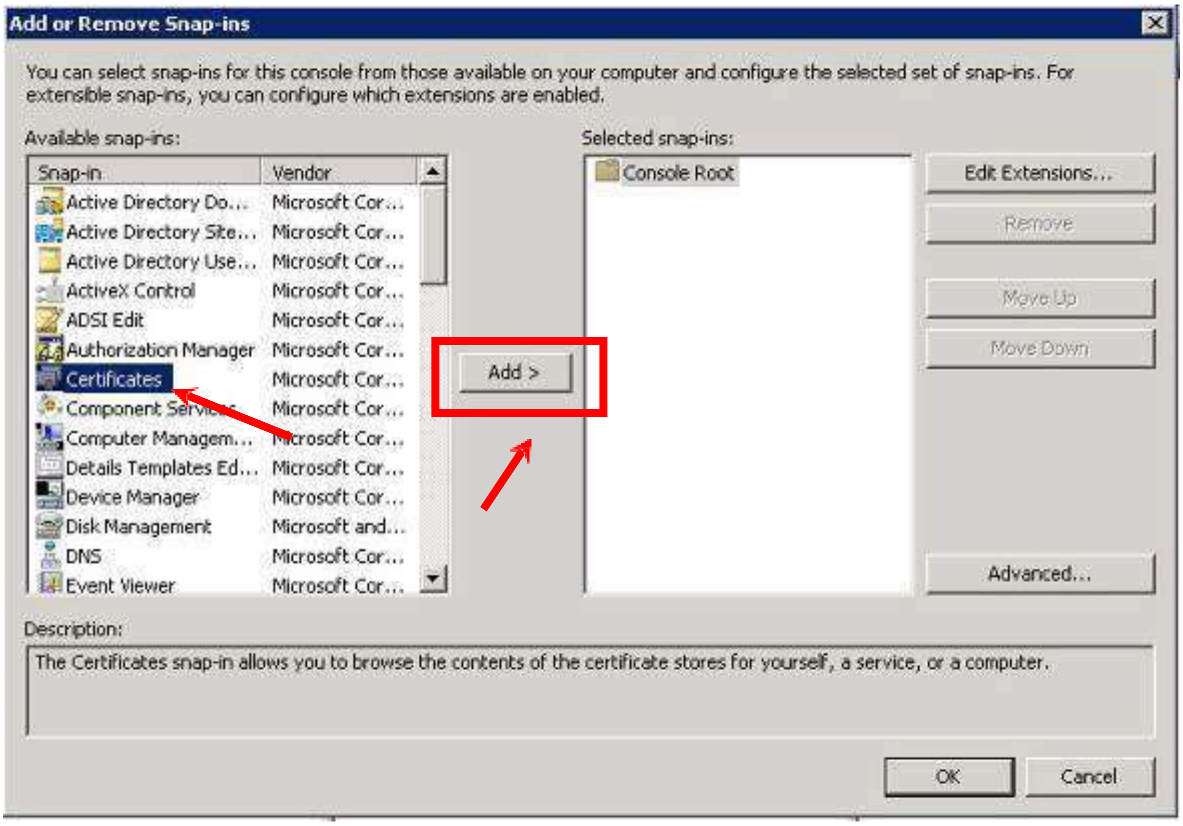
   Install the cross-certificate "Hongkong Post Root CA 3" issued by "GlobalSign Root CA - R3". Click the following link to download:
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt

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.


Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 Exchange Management Console
2 C:\Windows\...\ServerManager
3 Console1 save-20131009
4 C:\Windows\system32\dsa
Exit
Name
There are no items to show in this view.
Actions
Console Root
More Actions

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



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Details Templates Ed...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...
Event Viewer	Microsoft Cor...

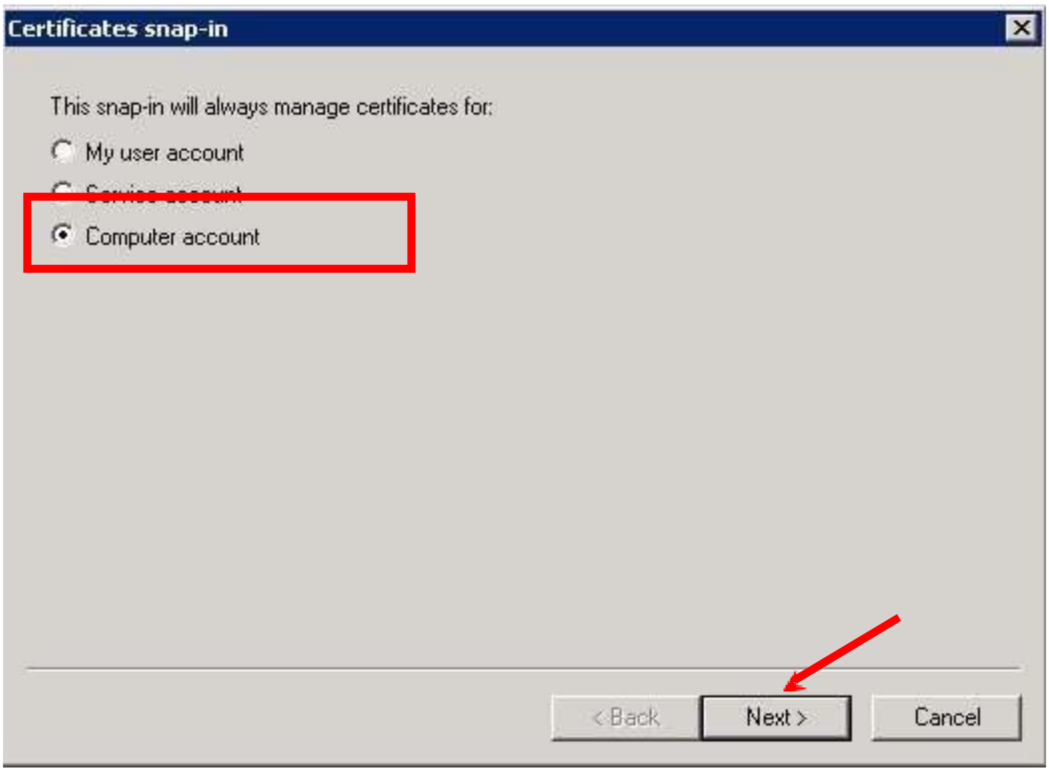
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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



Certificates snap-in

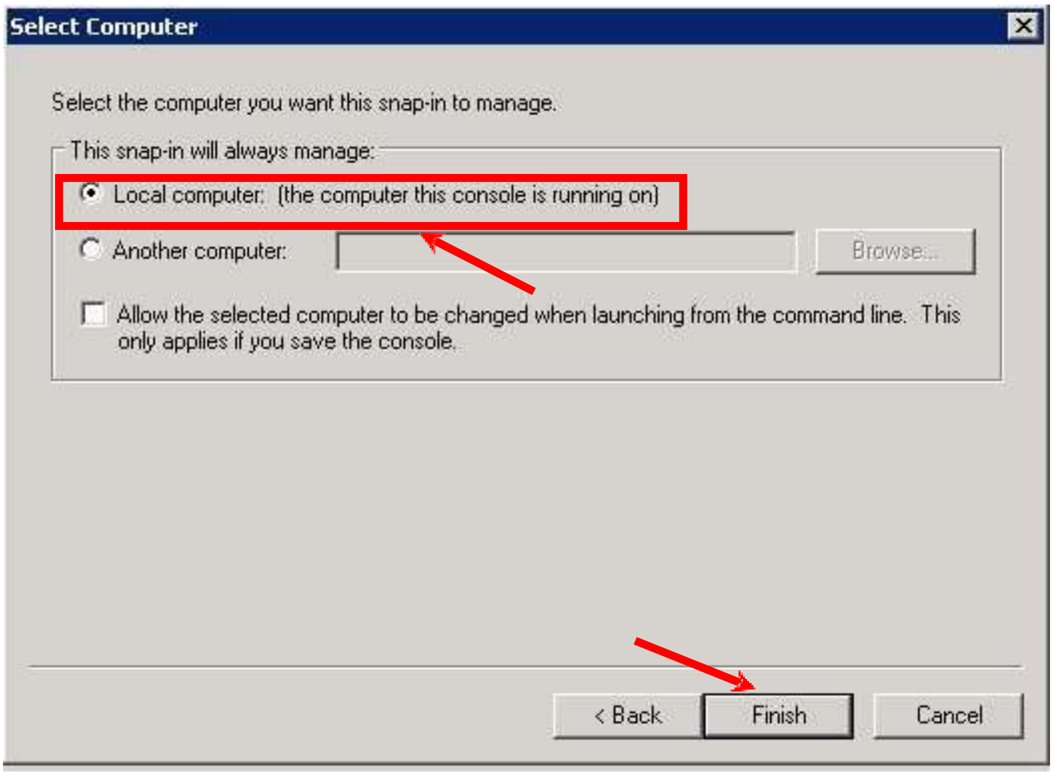
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

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



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

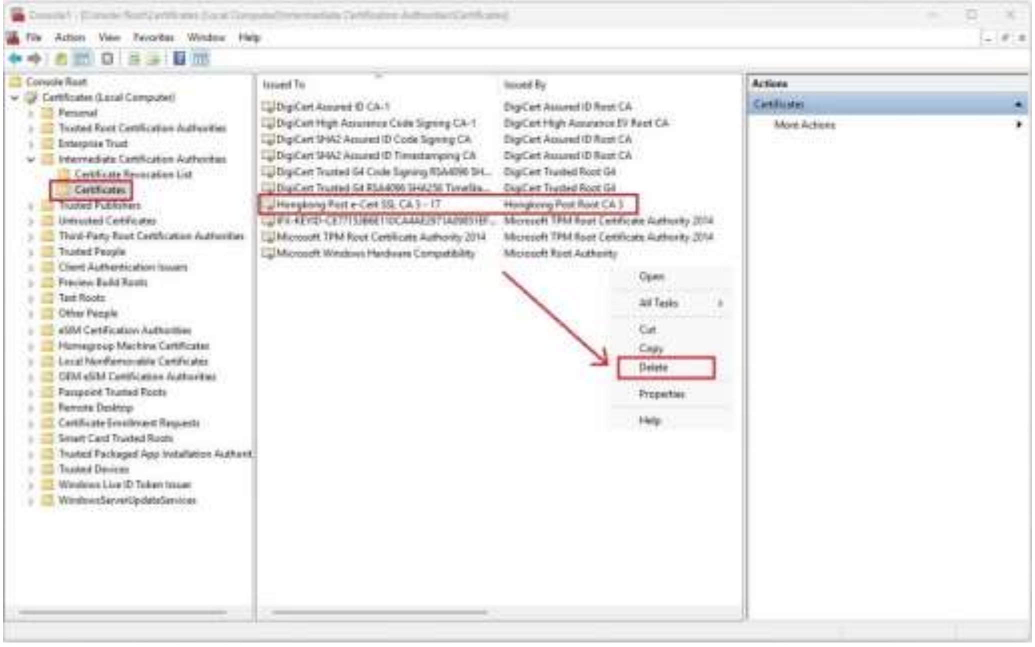
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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****.*

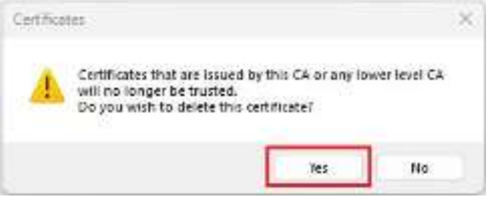
Removing the old Sub CA Certificate (if applicable)

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


Console1 - [Console Root\Certificates (Local Computer)\Intermediate Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
Other People
eSIM Certification Authorities
Homegroup Machine Certificates
Local NonRemovable Certificates
OEM eSIM Certification Authorities
Passpoint Trusted Roots
Remote Desktop
Certificate Enrollment Requests
Smart Card Trusted Roots
Trusted Packaged App Installation Authorit...
Trusted Devices
Windows Live ID Token Issuer
WindowsServerUpdateServices
Actions
Certificates
More Actions
Open
All Tasks
Cut
Copy
Delete
Properties
Help

Issued To	Issued By
DigiCert Assured ID CA-1	DigiCert Assured ID Root CA
DigiCert High Assurance Code Signing CA-1	DigiCert High Assurance EV Root CA
DigiCert SHA2 Assured ID Code Signing CA	DigiCert Assured ID Root CA
DigiCert SHA2 Assured ID Timestamping CA	DigiCert Assured ID Root CA
DigiCert Trusted G4 Code Signing RSA4096 SH...	DigiCert Trusted Root G4
DigiCert Trusted G4 RSA4096 SHA256 TimeSta...	DigiCert Trusted Root G4
Hongkong Post e-Cert SSL CA 3 - 17	Hongkong Post Root CA 3
IFX-KEYID-CE7715B6E11DCA4AE2971A0985...	Microsoft TPM Root Certificate Authority 2014
Microsoft TPM Root Certificate Authority 2014	Microsoft TPM Root Certificate Authority 2014
Microsoft Windows Hardware Compatibility	Microsoft Root Authority

Click "Yes" to delete.

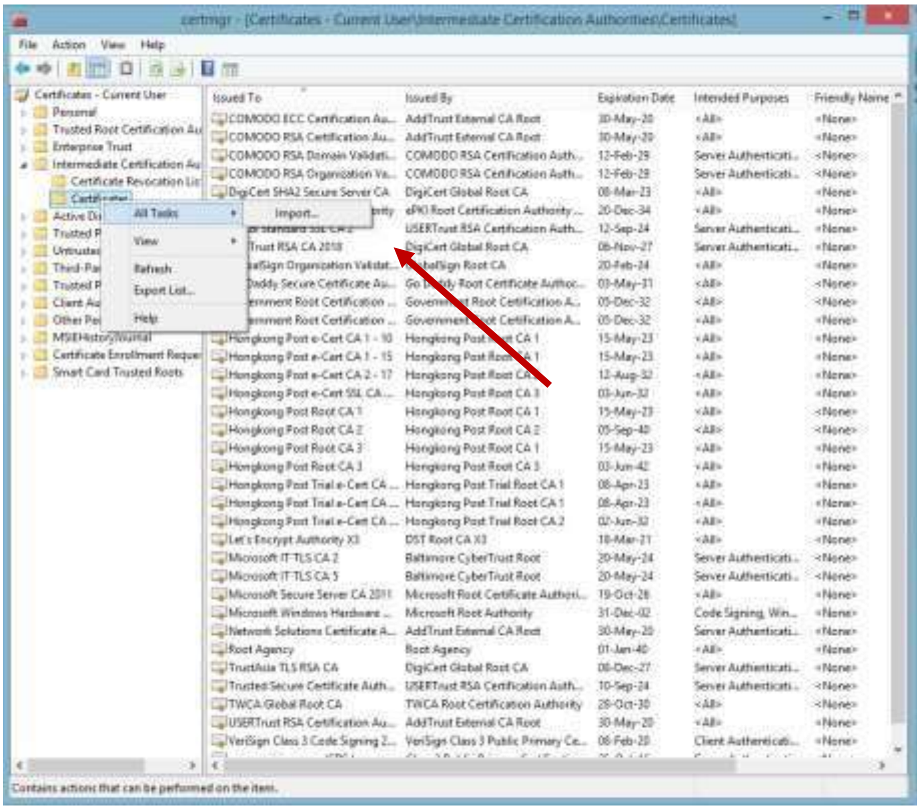


Certificates that are issued by this CA or any lower level CA will no longer be trusted.
Do you wish to delete this certificate?

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

Installing Sub CA / Cross Certificate

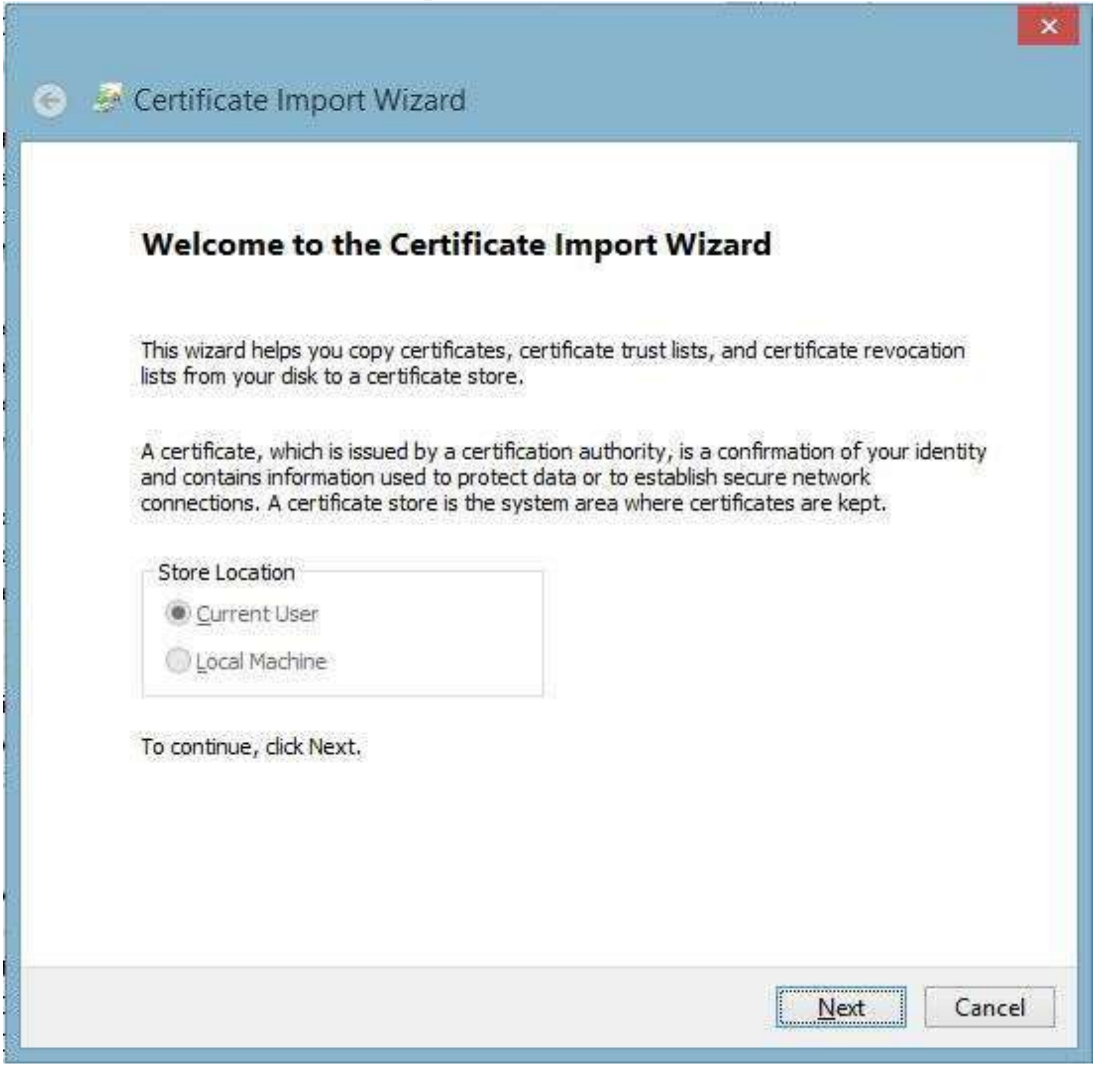
5. Expand the **Certificates (Local Computer)** node, then right-click the **Intermediate Certification Authorities** and then select **All Tasks > Import**.


certmgr - [Certificates - Current User\Intermediate Certification Authorities\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Certificate Revocation Lis
Certificates
Active Di
Trusted P
Untrusted
Third-Par
Trusted P
Client Au
Other Pe
MSIEHistoryJournal
Certificate Enrollment Reque
Smart Card Trusted Roots
All Tasks
Import...
View
Refresh
Export List...
Help

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
COMODO ECC Certification Au...	AddTrust External CA Root	30-May-20	<All>	<None>
COMODO RSA Certification Au...	AddTrust External CA Root	30-May-20	<All>	<None>
COMODO RSA Domain Validati...	COMODO RSA Certification Auth...	12-Feb-29	Server Authenticati...	<None>
COMODO RSA Organization Va...	COMODO RSA Certification Auth...	12-Feb-29	Server Authenticati...	<None>
DigiCert SHA2 Secure Server CA	DigiCert Global Root CA	08-Mar-23	<All>	<None>
rity	ePKI Root Certification Authority ...	20-Dec-34	<All>	<None>
r Standard SSL CA 2	USERTrust RSA Certification Auth...	12-Sep-24	Server Authenticati...	<None>
Trust RSA CA 2018	DigiCert Global Root CA	06-Nov-27	Server Authenticati...	<None>
alSign Organization Validat...	balSign Root CA	20-Feb-24	<All>	<None>
Daddy Secure Certificate Au...	Go D dy Root Certificate Author...	03-May-31	<All>	<None>
ernment Root Certification ...	Govern t Root Certification A...	05-Dec-32	<All>	<None>
ernment Root Certification ...	Government ot Certification A...	05-Dec-32	<All>	<None>
Hongkong Post e-Cert CA 1 - 10	Hongkong Post t CA 1	15-May-23	<All>	<None>
Hongkong Post e-Cert CA 1 - 15	Hongkong Post Roo A 1	15-May-23	<All>	<None>
Hongkong Post e-Cert CA 2 - 17	Hongkong Post Root CA	12-Aug-32	<All>	<None>
Hongkong Post e-Cert SSL CA ...	Hongkong Post Root CA 3	03-Jun-32	<All>	<None>
Hongkong Post Root CA 1	Hongkong Post Root CA 1	15-May-23	<All>	<None>
Hongkong Post Root CA 2	Hongkong Post Root CA 2	05-Sep-40	<All>	<None>
Hongkong Post Root CA 3	Hongkong Post Root CA 1	15-May-23	<All>	<None>
Hongkong Post Root CA 3	Hongkong Post Root CA 3	03-Jun-42	<All>	<None>
Hongkong Post Trial e-Cert CA ...	Hongkong Post Trial Root CA 1	08-Apr-23	<All>	<None>
Hongkong Post Trial e-Cert CA ...	Hongkong Post Trial Root CA 1	08-Apr-23	<All>	<None>
Hongkong Post Trial e-Cert CA ...	Hongkong Post Trial Root CA 2	02-Jun-32	<All>	<None>
Let's Encrypt Authority X3	DST Root CA X3	18-Mar-21	<All>	<None>
Microsoft IT TLS CA 2	Baltimore CyberTrust Root	20-May-24	Server Authenticati...	<None>
Microsoft IT TLS CA 5	Baltimore CyberTrust Root	20-May-24	Server Authenticati...	<None>
Microsoft Secure Server CA 2011	Microsoft Root Certificate Authori...	19-Oct-28	<All>	<None>
Microsoft Windows Hardware ...	Microsoft Root Authority	31-Dec-02	Code Signing, Win...	<None>
Network Solutions Certificate A...	AddTrust External CA Root	30-May-20	Server Authenticati...	<None>
Root Agency	Root Agency	01-Jan-40	<All>	<None>
TrustAsia TLS RSA CA	DigiCert Global Root CA	08-Dec-27	Server Authenticati...	<None>
Trusted Secure Certificate Auth...	USERTrust RSA Certification Auth...	10-Sep-24	Server Authenticati...	<None>
TWCA Global Root CA	TWCA Root Certification Authority	28-Oct-30	<All>	<None>
USERTrust RSA Certification Au...	AddTrust External CA Root	30-May-20	<All>	<None>
VeriSign Class 3 Code Signing 2...	VeriSign Class 3 Public Primary Ce...	08-Feb-20	Client Authenticati...	<None>

Contains actions that can be performed on the item.

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



Welcome to the Certificate Import Wizard

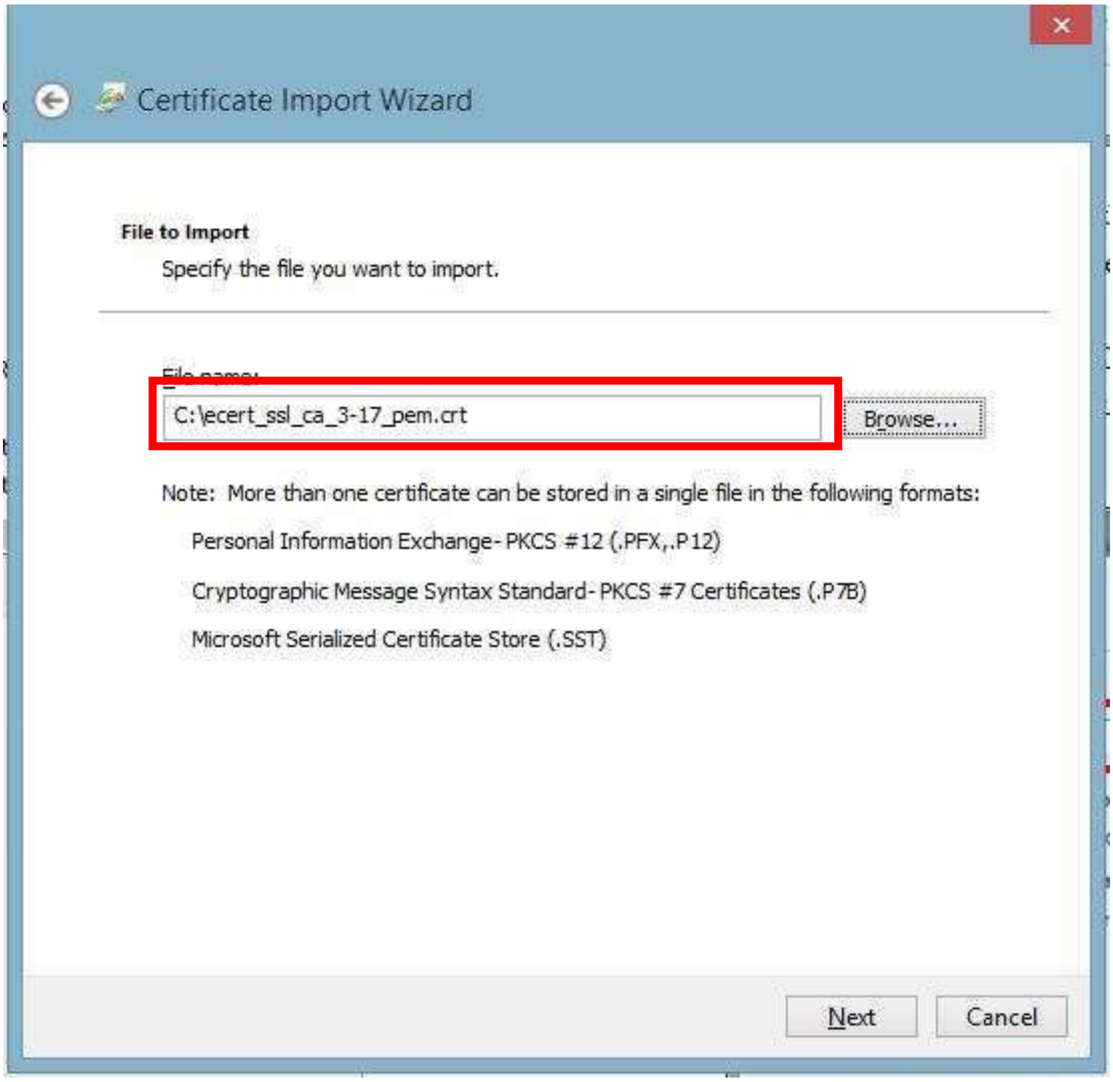
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
● Current User
○ Local Machine

To continue, click Next.

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**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\ecert_ssl_ca_3-17_pem.crt

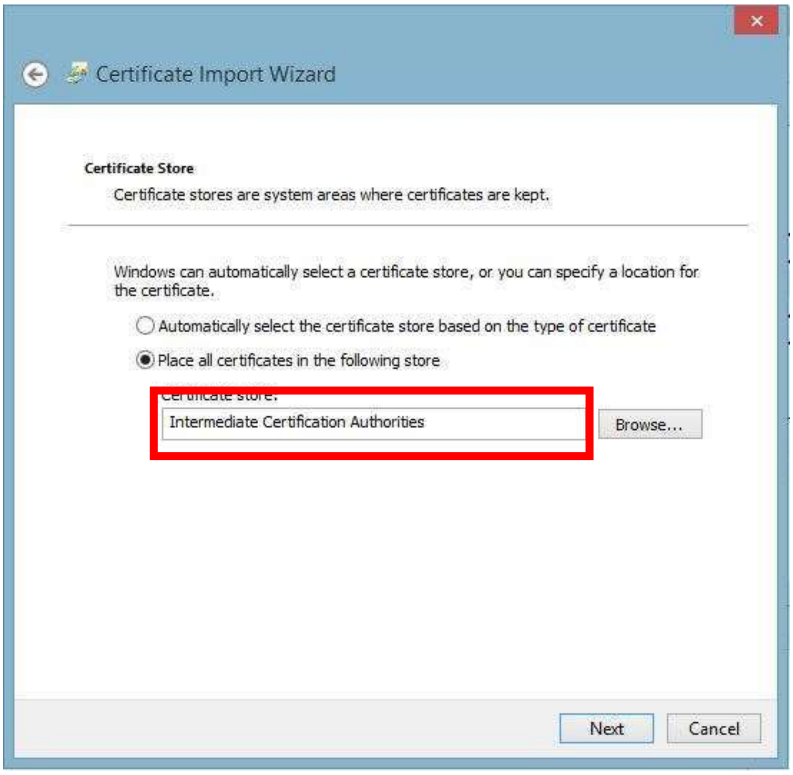
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

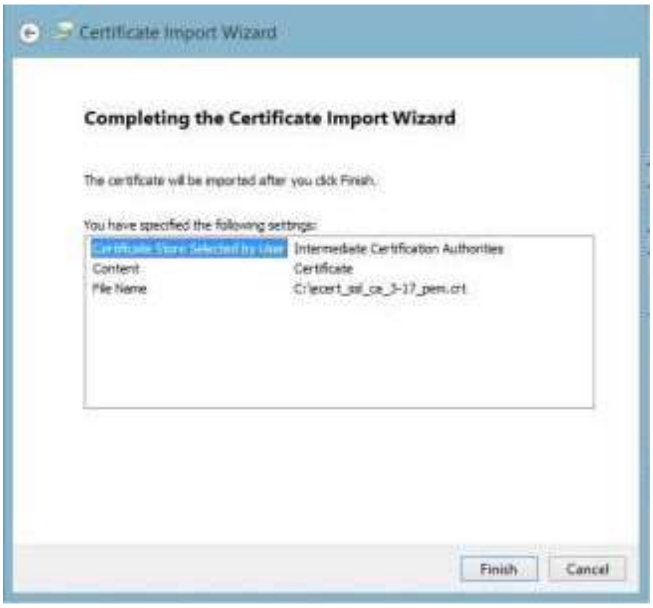
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

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



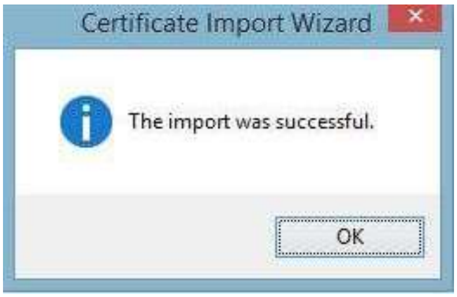
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

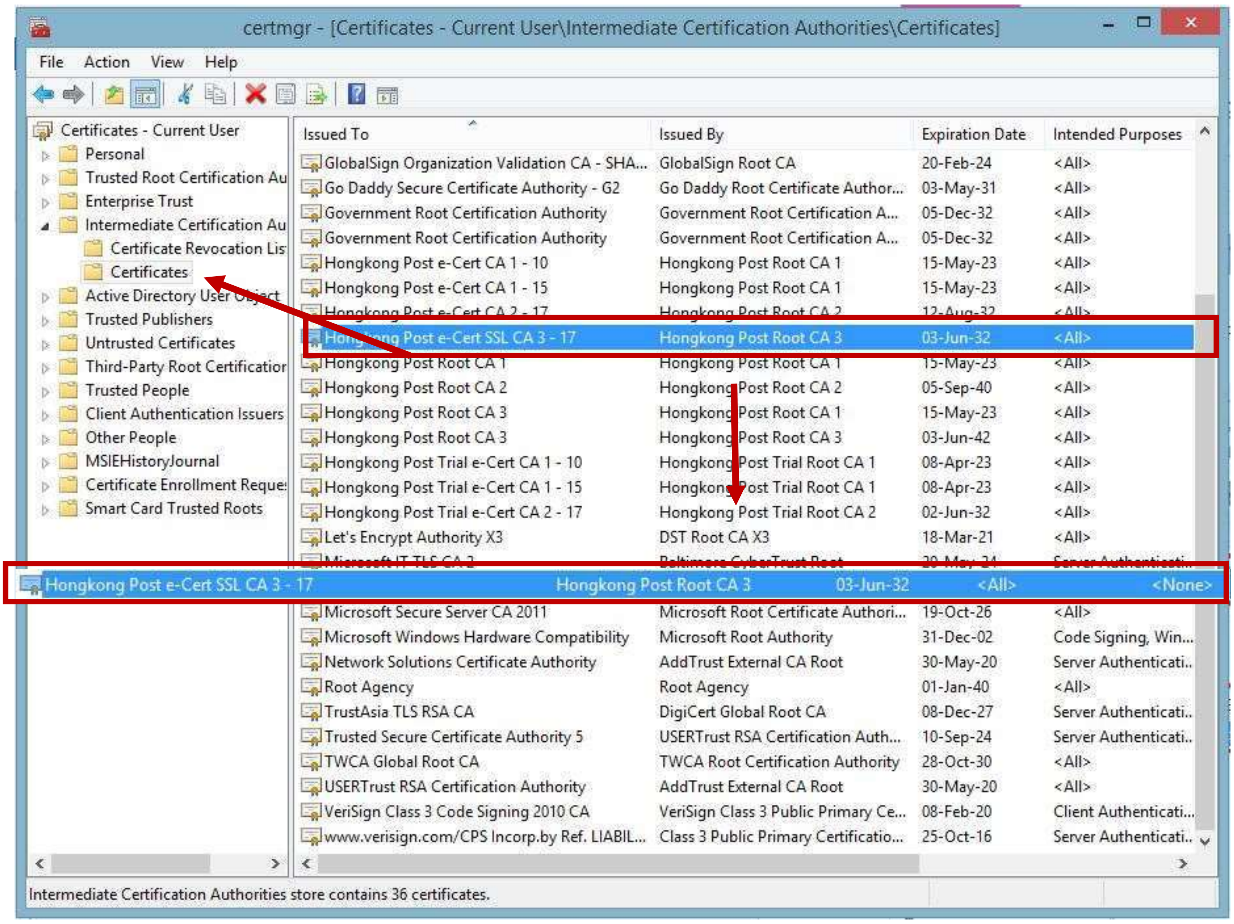
Certificate Store Selected by User	Intermediate Certification Authorities
Content	Certificate
File Name	C:\ecert_ssl_ce_3-17_pem.crt

10. Click **OK** to complete.



The import was successful.

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


certmgr - [Certificates - Current User\Intermediate Certification Authorities\Certificates]
File
Action
View
Help

- Certificates - Current User
  - Personal
  - Trusted Root Certification Au
  - Enterprise Trust
  - Intermediate Certification Au
    - Certificate Revocation Lis
    - Certificates
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certification
  - Trusted People
  - Client Authentication Issuers
  - Other People
  - MSIEHistoryJournal
  - Certificate Enrollment Reque:
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes
GlobalSign Organization Validation CA - SHA...	GlobalSign Root CA	20-Feb-24	<All>
Go Daddy Secure Certificate Authority - G2	Go Daddy Root Certificate Author...	03-May-31	<All>
Government Root Certification Authority	Government Root Certification A...	05-Dec-32	<All>
Government Root Certification Authority	Government Root Certification A...	05-Dec-32	<All>
Hongkong Post e-Cert CA 1 - 10	Hongkong Post Root CA 1	15-May-23	<All>
Hongkong Post e-Cert CA 1 - 15	Hongkong Post Root CA 1	15-May-23	<All>
Hongkong Post e-Cert CA 2 - 17	Hongkong Post Root CA 2	12-Aug-32	<All>
Hongkong Post e-Cert SSL CA 3 - 17	Hongkong Post Root CA 3	03-Jun-32	<All>
Hongkong Post Root CA 1	Hongkong Post Root CA 1	15-May-23	<All>
Hongkong Post Root CA 2	Hongkong Post Root CA 2	05-Sep-40	<All>
Hongkong Post Root CA 3	Hongkong Post Root CA 1	15-May-23	<All>
Hongkong Post Root CA 3	Hongkong Post Root CA 3	03-Jun-42	<All>
Hongkong Post Trial e-Cert CA 1 - 10	Hongkong Post Trial Root CA 1	08-Apr-23	<All>
Hongkong Post Trial e-Cert CA 1 - 15	Hongkong Post Trial Root CA 1	08-Apr-23	<All>
Hongkong Post Trial e-Cert CA 2 - 17	Hongkong Post Trial Root CA 2	02-Jun-32	<All>
Let's Encrypt Authority X3	DST Root CA X3	18-Mar-21	<All>
Microsoft IT TLS CA 2	Baltimore CyberTrust Root	20-May-24	Server Authenticati...
Microsoft Secure Server CA 2011	Microsoft Root Certificate Authori...	19-Oct-26	<All>
Microsoft Windows Hardware Compatibility	Microsoft Root Authority	31-Dec-02	Code Signing, Win...
Network Solutions Certificate Authority	AddTrust External CA Root	30-May-20	Server Authenticati..
Root Agency	Root Agency	01-Jan-40	<All>
TrustAsia TLS RSA CA	DigiCert Global Root CA	08-Dec-27	Server Authenticati..
Trusted Secure Certificate Authority 5	USERTrust RSA Certification Auth...	10-Sep-24	Server Authenticati..
TWCA Global Root CA	TWCA Root Certification Authority	28-Oct-30	<All>
USERTrust RSA Certification Authority	AddTrust External CA Root	30-May-20	<All>
VeriSign Class 3 Code Signing 2010 CA	VeriSign Class 3 Public Primary Ce...	08-Feb-20	Client Authenticati...
www.verisign.com/CPS Incorp.by Ref. LIABIL...	Class 3 Public Primary Certificatio...	25-Oct-16	Server Authenticati..

Hongkong Post e-Cert SSL CA 3 - 17 Hongkong Post Root CA 3 03-Jun-32 <All> <None>

Intermediate Certification Authorities store contains 36 certificates.

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

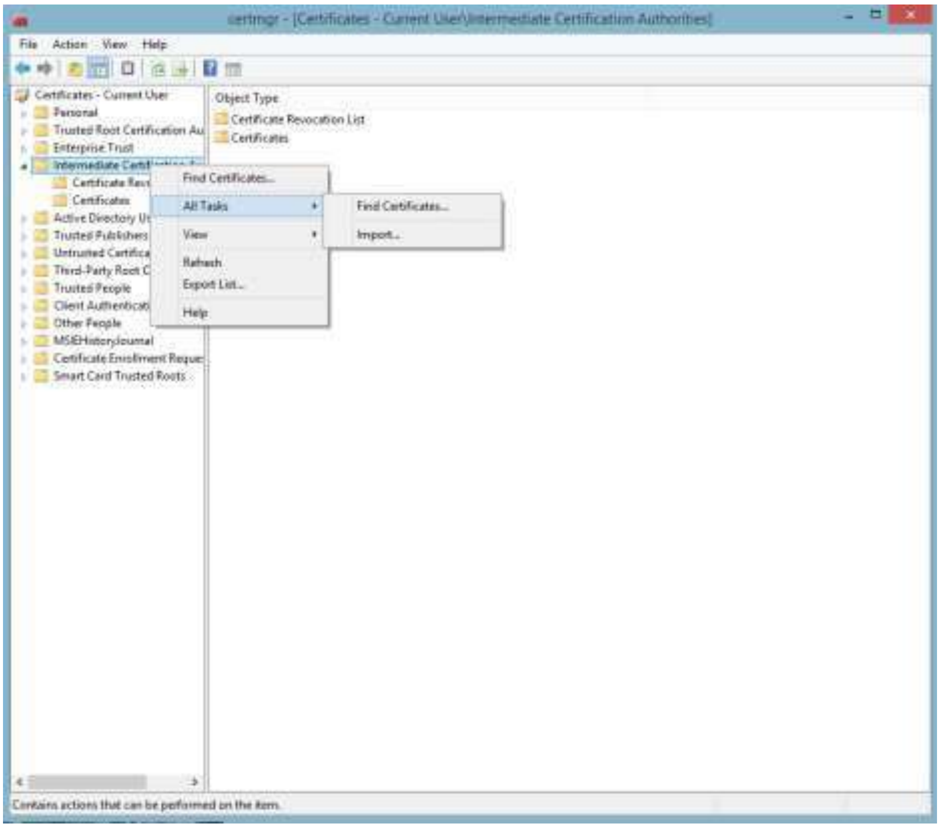
Repeat step 5 to step 10 for installation of cross-cert (root_ca_3_x_gsca_r3_pem.crt) which was downloaded in Section C step 7.

Installing Authority Revocation List (ARL)

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

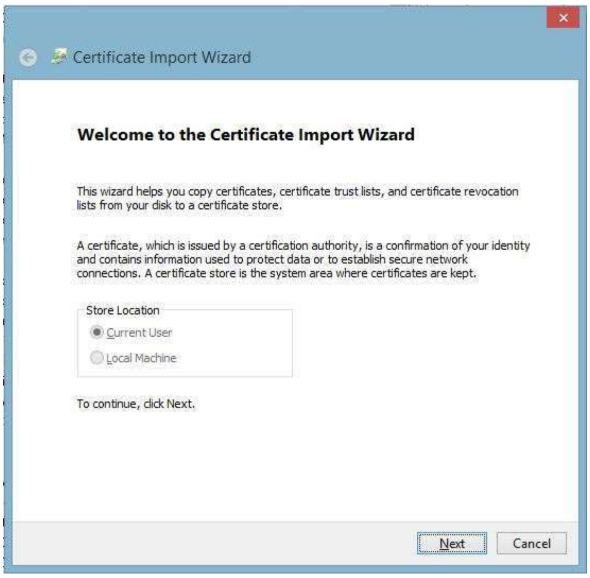
    http://crl1.eCert.gov.hk/crl/RootCA3ARL.crl

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



Contains actions that can be performed on the item.

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



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

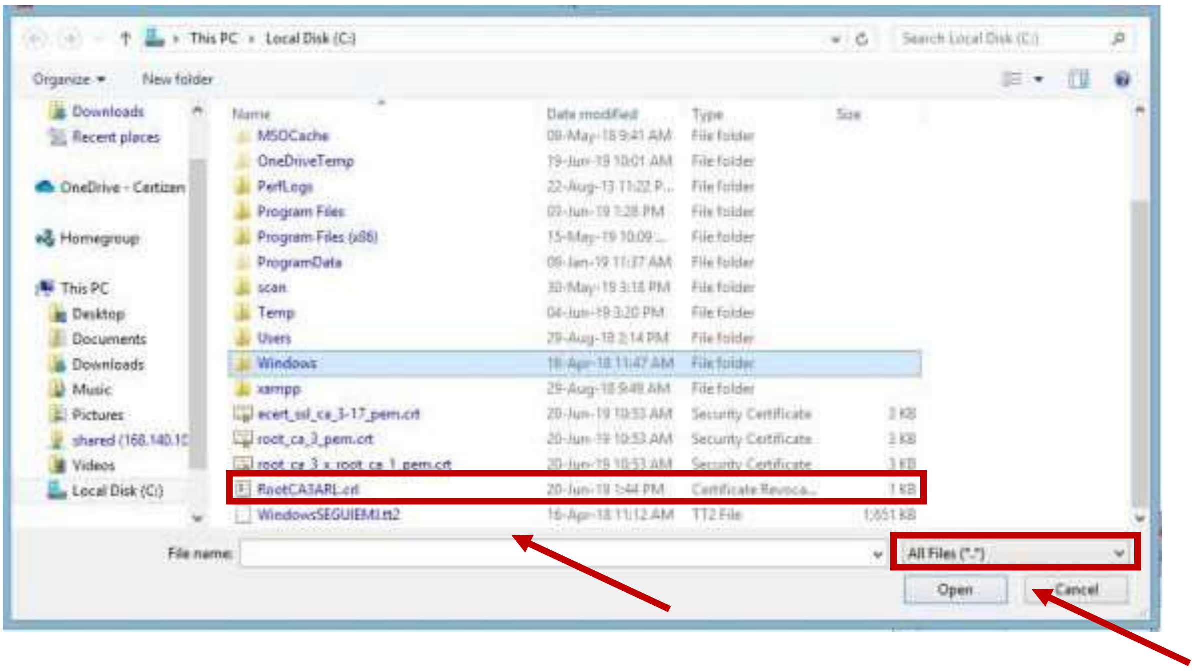
Store Location

● Current User

○ Local Machine

To continue, click Next.

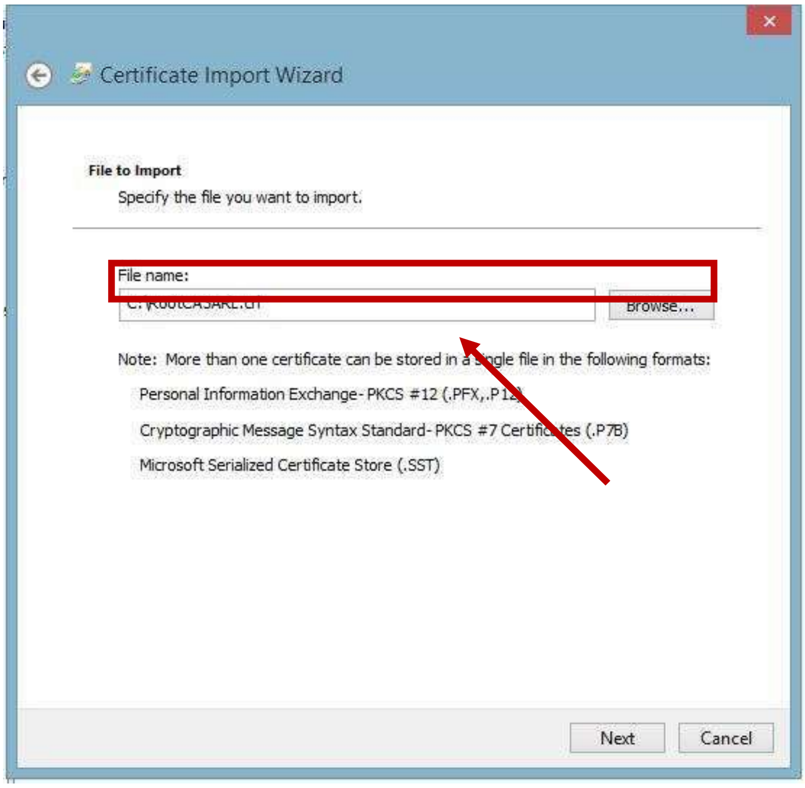
14. Click **Browse** to locate the **Hongkong Post Authority Revocation List (ARL)** that you downloaded before in Step 11 (RootCA3ARL.crl), and then click **Next**. (Tip: choose **All Files**)



Name	Date modified	Type	Size
MSOCache	08-May-18 9:41 AM	File folder	
OneDriveTemp	19-Jun-19 10:01 AM	File folder	
PerfLogs	22-Aug-13 11:22 P...	File folder	
Program Files	03-Jun-19 1:28 PM	File folder	
Program Files (x86)	15-May-19 10:09 ...	File folder	
ProgramData	08-Jan-19 11:37 AM	File folder	
scan	30-May-19 3:18 PM	File folder	
Temp	04-Jun-19 3:20 PM	File folder	
Users	29-Aug-18 2:14 PM	File folder	
Windows	18-Apr-18 11:47 AM	File folder	
xampp	29-Aug-18 9:48 AM	File folder	
ecert_ssl_ca_3-17_pem.crt	20-Jun-19 10:53 AM	Security Certificate	3 KB
root_ca_3_pem.crt	20-Jun-19 10:53 AM	Security Certificate	3 KB
root_ca_3_x_root_ca_1_pem.crt	20-Jun-19 10:53 AM	Security Certificate	3 KB
RootCA3ARL.crl	20-Jun-19 1:44 PM	Certificate Revoca...	1 KB
WindowsSEGUIEMJ.tt2	16-Apr-18 11:12 AM	TT2 File	1,651 KB

File name:

All Files (*.*)



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\RootCA3ARL.crt

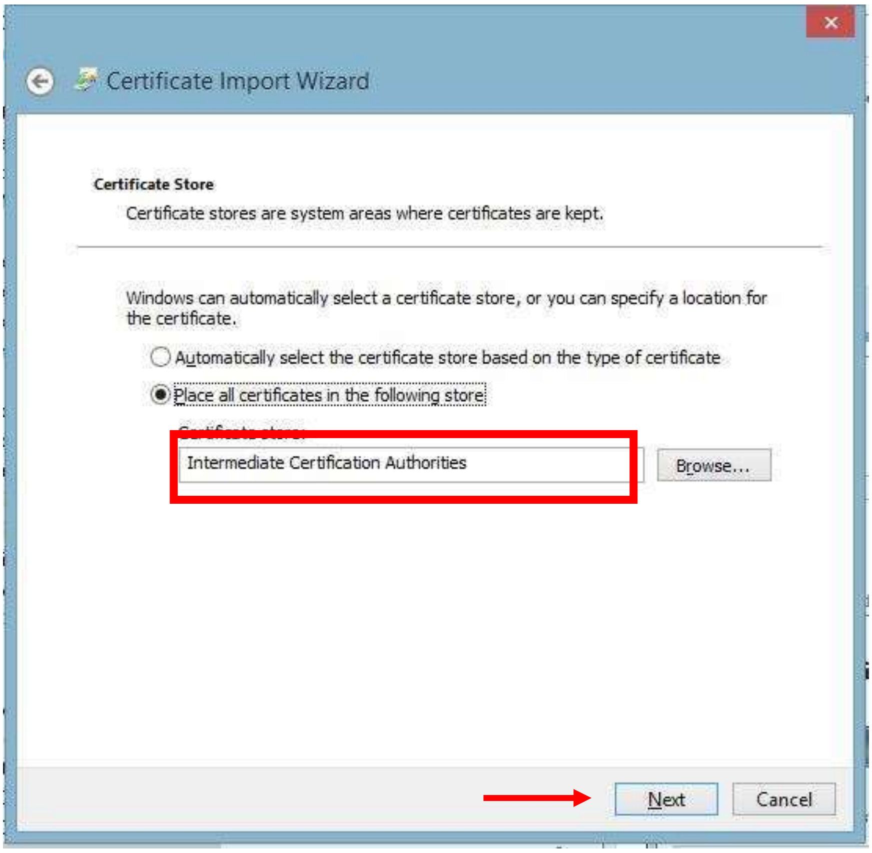
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

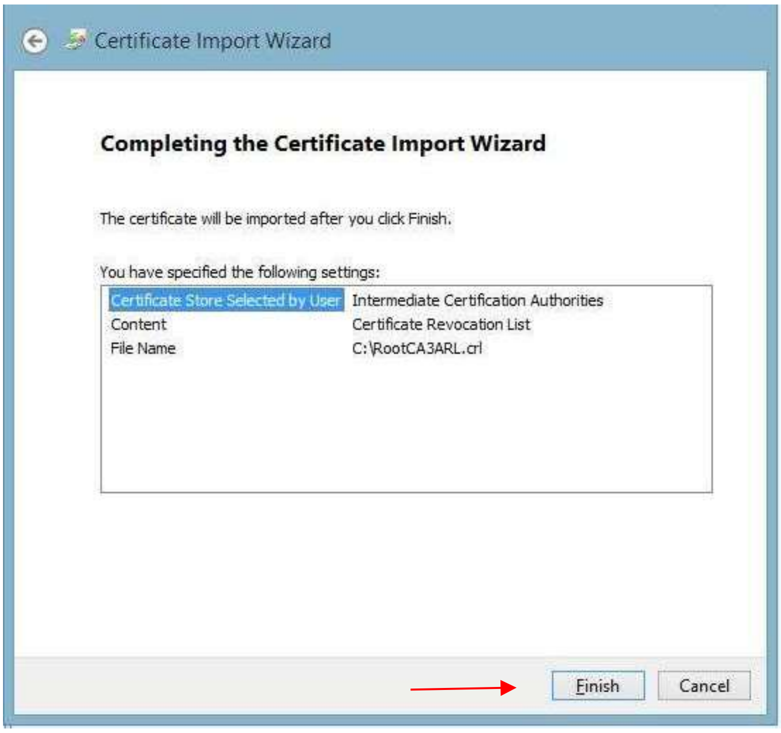
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

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



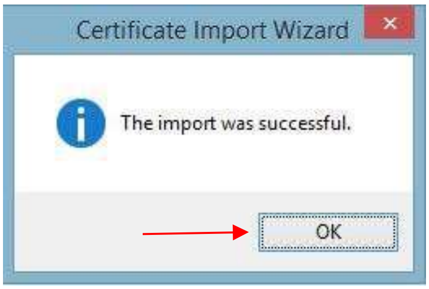
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

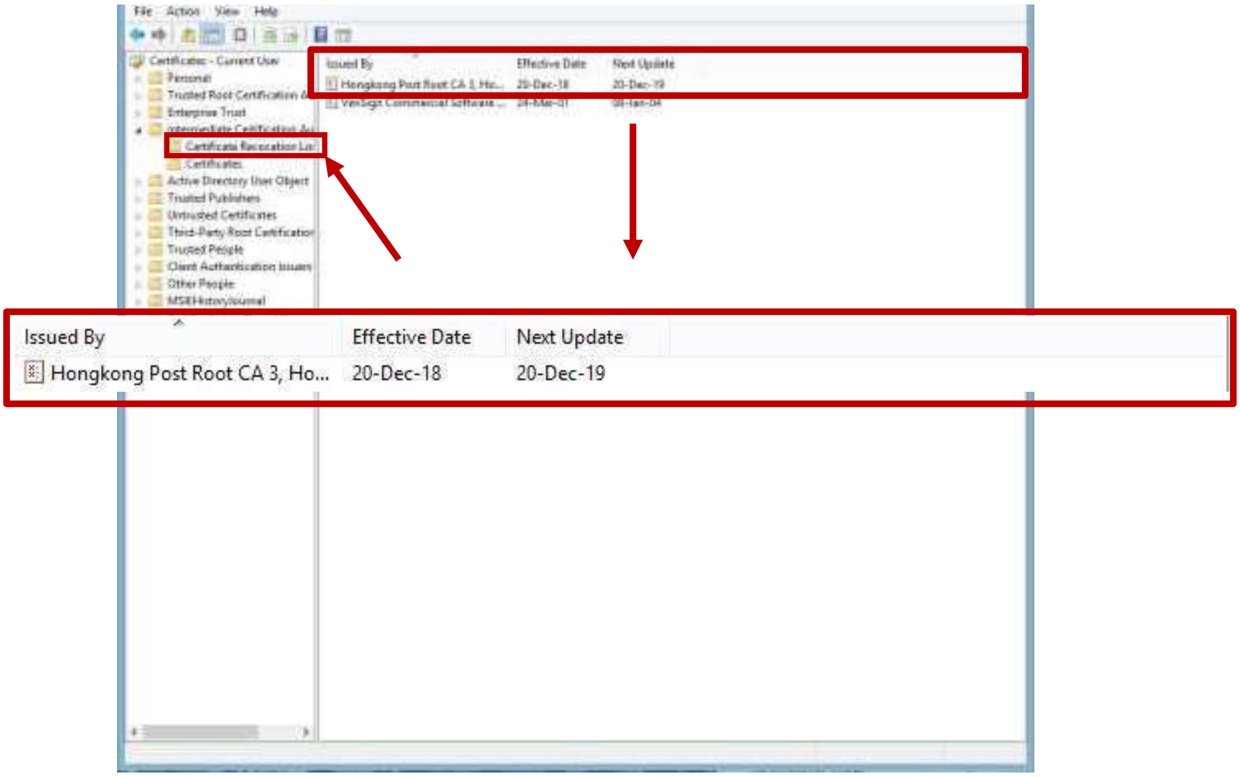
Certificate Store Selected by User	Intermediate Certification Authorities
Content	Certificate Revocation List
File Name	C:\RootCA3ARL.crl

17. Click **OK** to complete.



The import was successful.

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

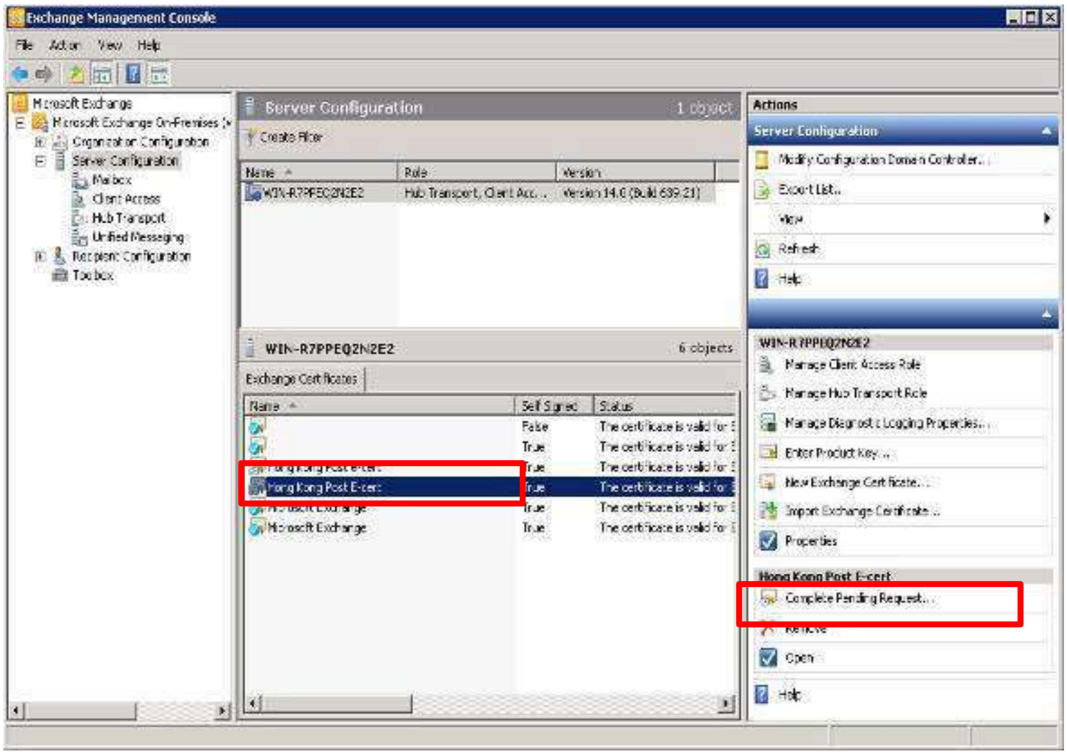

File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification A
Enterprise Trust
Intermediate Certification Au
Certificate Revocation List
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Other People
MSIEHistoryJournal

Issued By	Effective Date	Next Update
Hongkong Post Root CA 3, Ho...	20-Dec-18	20-Dec-19

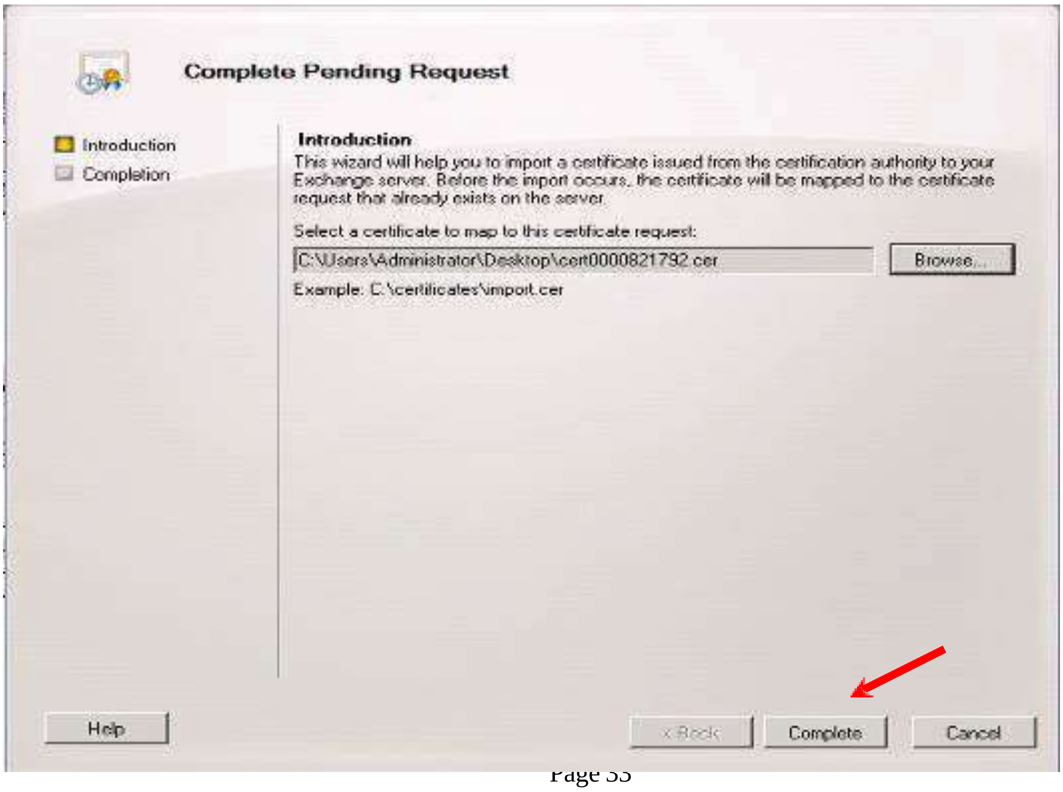
Figure 3: **Hongkong Post Authority Revocation List (ARL)** certificate has been successfully installed

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**.



Introduction

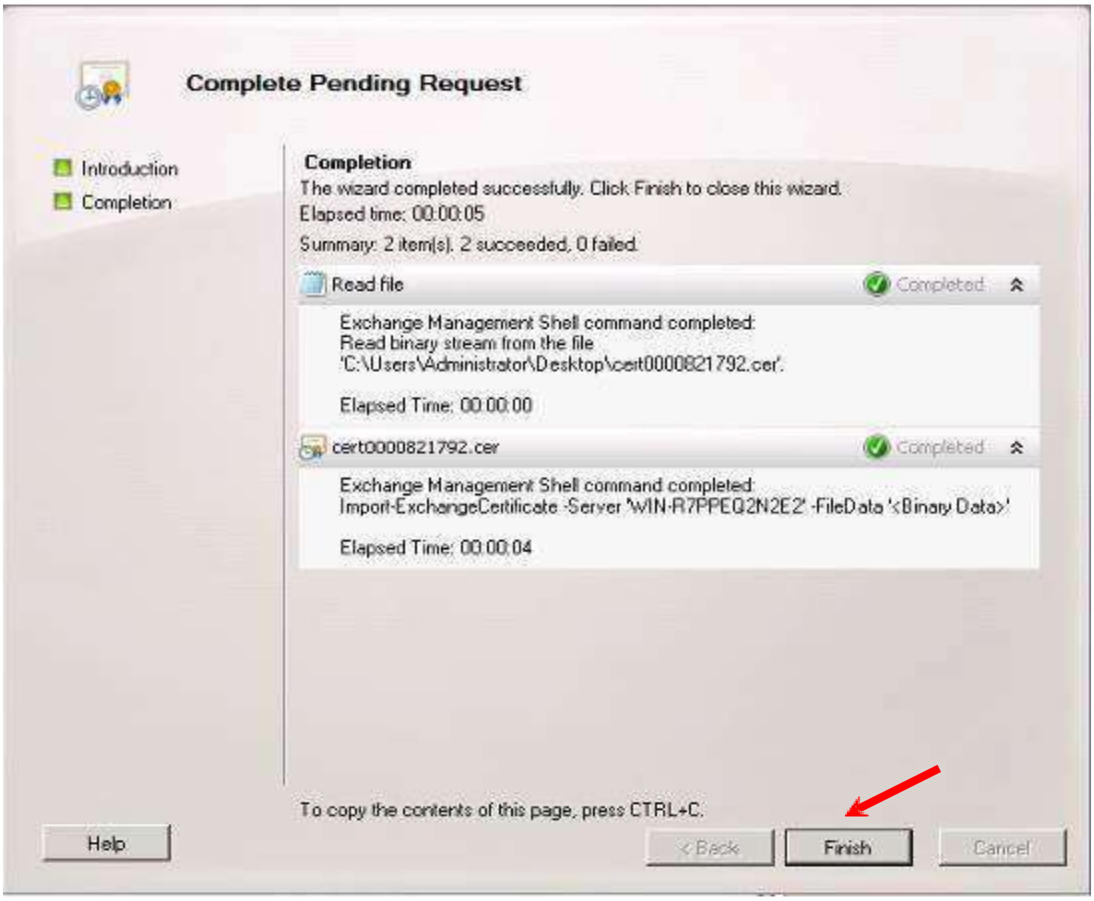
This wizard will help you to import a certificate issued from the certification authority to your Exchange server. Before the import occurs, the certificate will be mapped to the certificate request that already exists on the server.

Select a certificate to map to this certificate request:

C:\Users\Administrator\Desktop\cert0000821792.cer

Example: C:\certificates\import.cer

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



Complete Pending Request

Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:05

Summary: 2 item(s). 2 succeeded, 0 failed.

Read file — Completed

Exchange Management Shell command completed:
Read binary stream from the file
'C:\Users\Administrator\Desktop\cert0000821792.cer'.

Elapsed Time: 00:00:00

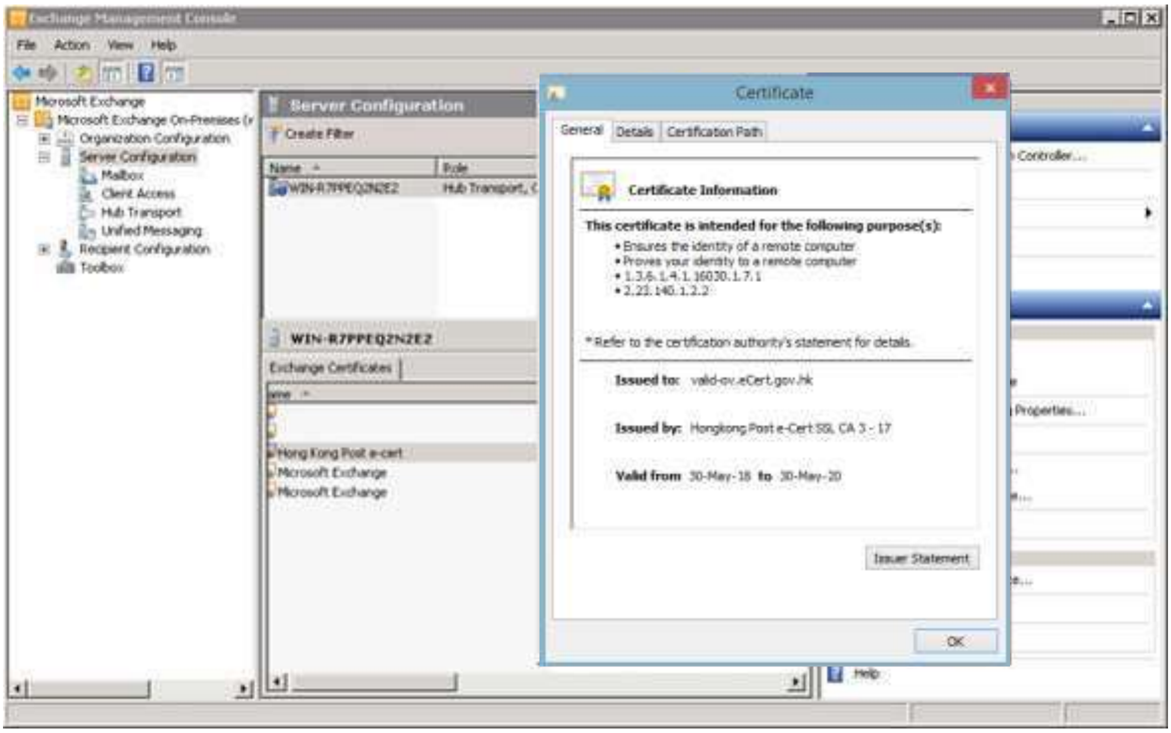
cert0000821792.cer — Completed

Exchange Management Shell command completed:
Import-ExchangeCertificate -Server 'WIN-R7PPEQ2N2E2' -FileData '<Binary Data>'

Elapsed Time: 00:00:04

To copy the contents of this page, press CTRL+C.

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



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.16030.1.7.1
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

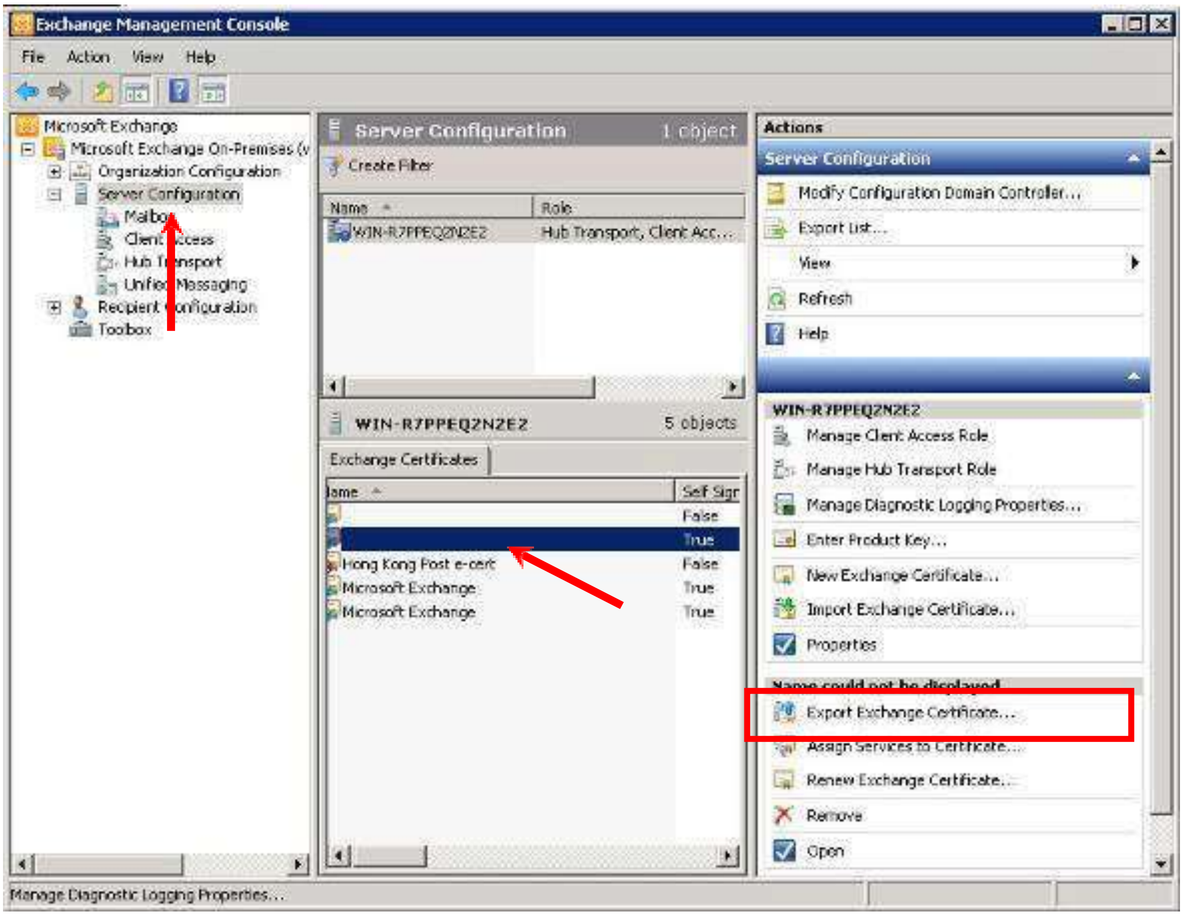
Issued to: valid-ov.eCert.gov.hk

Issued by: Hongkong Post e-Cert SSL CA 3 - 17

Valid from 30-May-18 to 30-May-20

F. Backing up the Private Key

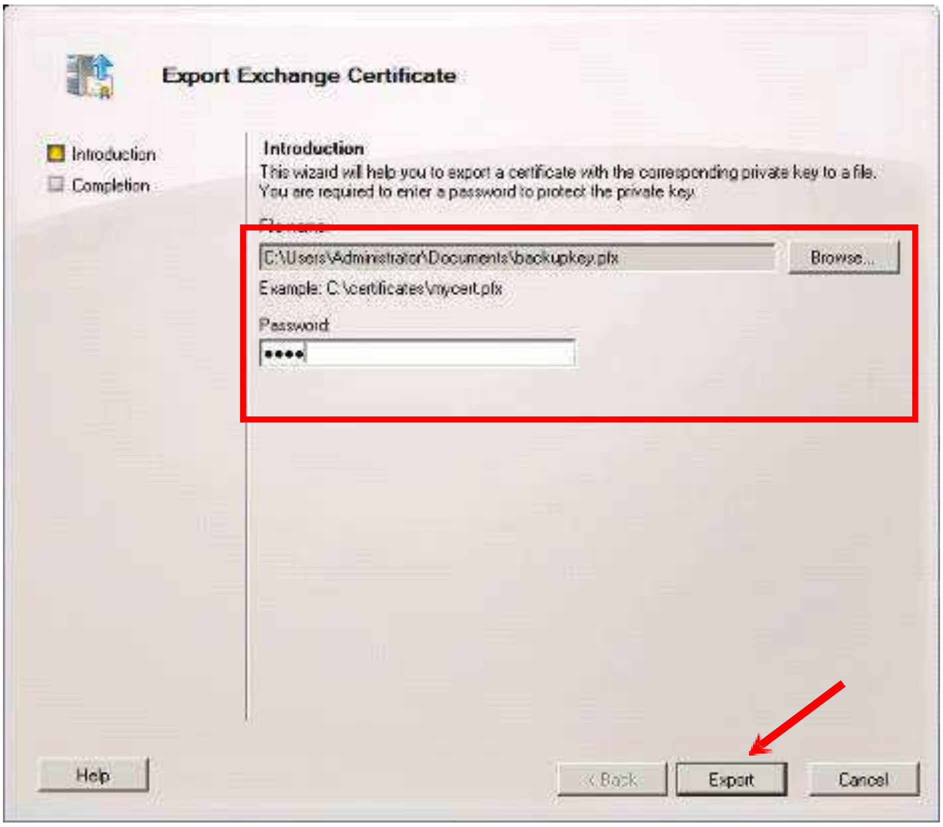
1. In **Exchange Management Console**, choose the certificate that you intend to export, and then click **Export Exchange Certificate**.


Exchange Management Console
File
Action
View
Help
Microsoft Exchange
Microsoft Exchange On-Premises (v
Organization Configuration
Server Configuration
Mailbox
Client Access
Hub Transport
Unified Messaging
Recipient Configuration
Toolbox
Server Configuration
1 object
Create Filter
WIN-R7PPEQ2NZE2
5 objects
Exchange Certificates
Actions
Server Configuration
Modify Configuration Domain Controller...
Export List...
View
Refresh
Help
WIN-R7PPEQ2NZE2
Manage Client Access Role
Manage Hub Transport Role
Manage Diagnostic Logging Properties...
Enter Product Key...
New Exchange Certificate...
Import Exchange Certificate...
Properties
Name could not be displayed
Export Exchange Certificate...
Assign Services to Certificate...
Renew Exchange Certificate...
Remove
Open
Manage Diagnostic Logging Properties...

Name	Role
WIN-R7PPEQ2NZE2	Hub Transport, Client Acc...

Name	Self Sign
	False
	True
Hong Kong Post e-cert	False
Microsoft Exchange	True
Microsoft Exchange	True

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.)



Export Exchange Certificate

Introduction

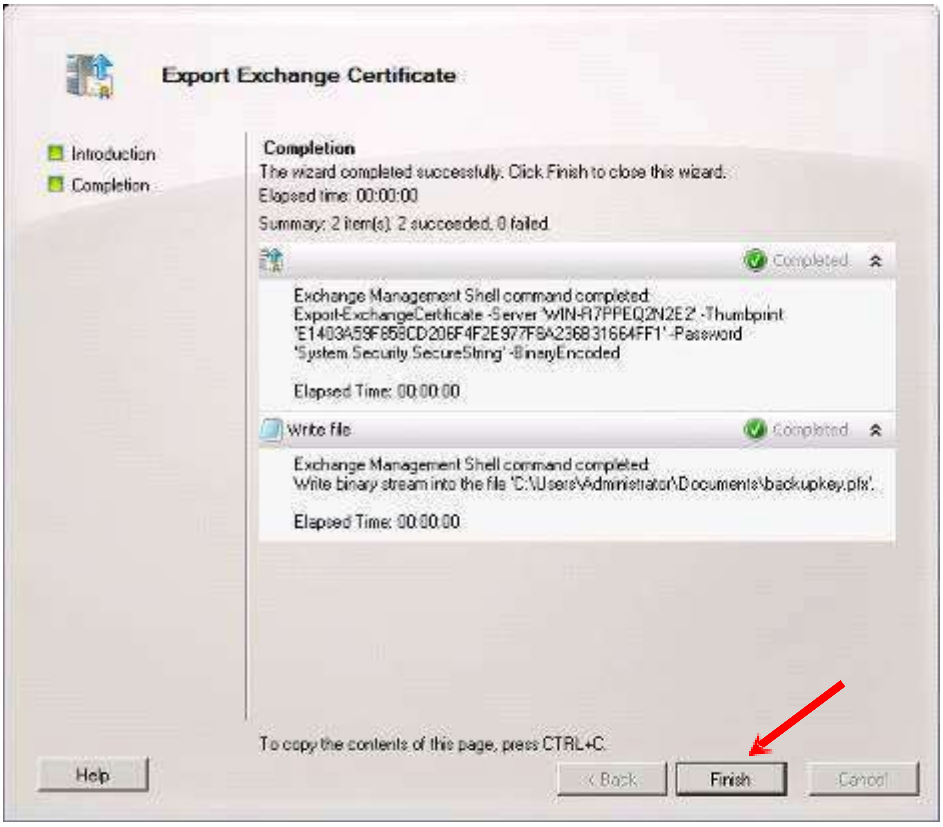
This wizard will help you to export a certificate with the corresponding private key to a file. You are required to enter a password to protect the private key.

File name:
C:\Users\Administrator\Documents\backupkey.pfx

Example: C:\certificates\mycert.pfx

Password:
••••

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



Export Exchange Certificate

Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:00

Summary: 2 item(s). 2 succeeded, 0 failed.

```
Exchange Management Shell command completed:
Export-ExchangeCertificate -Server 'WIN-R7PPEQ2N2E2' -Thumbprint
'E1403A59F858CD206F4F2E977F8A236831664FF1' -Password
'System.Security.SecureString' -BinaryEncoded

Elapsed Time: 00:00:00
```

Write file

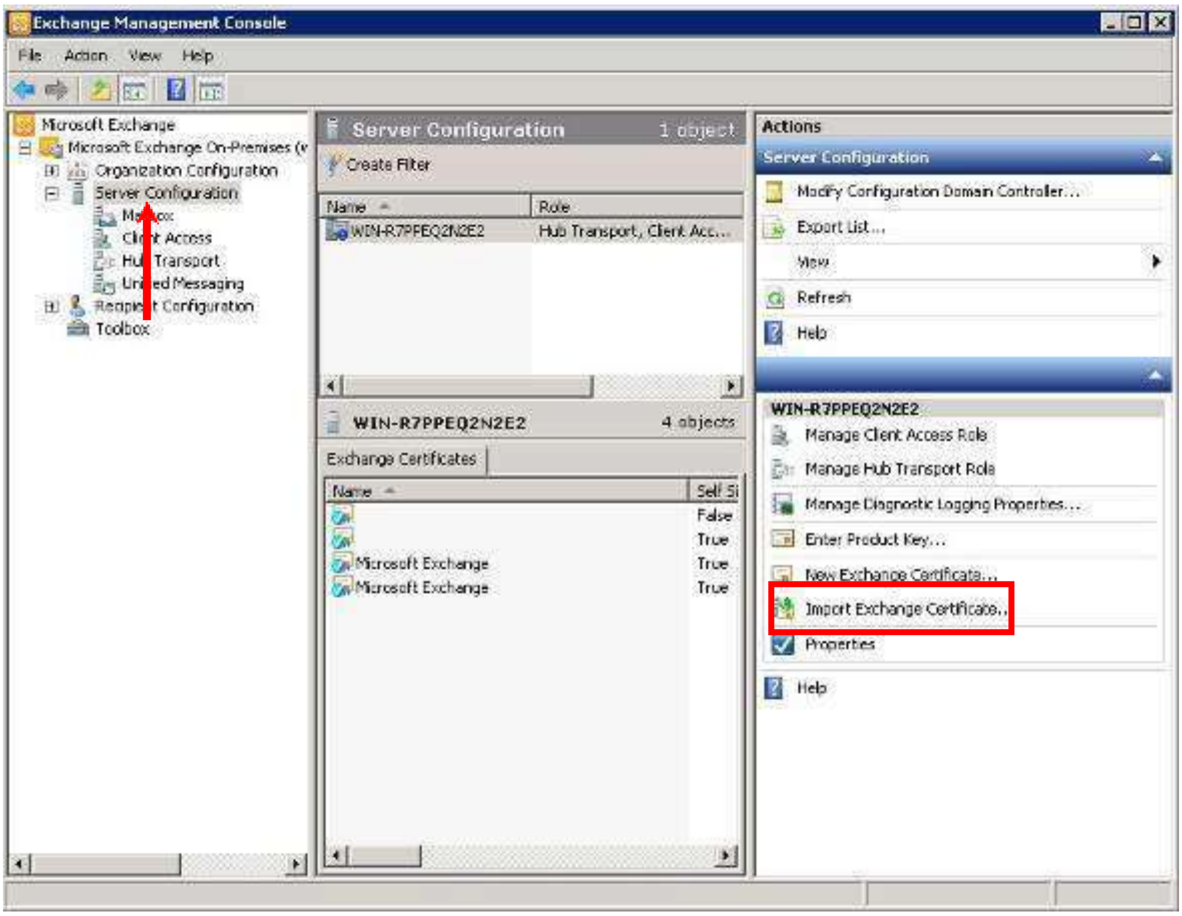
```
Exchange Management Shell command completed:
Write binary stream into the file 'C:\Users\Administrator\Documents\backupkey.pfx'.

Elapsed Time: 00:00:00
```

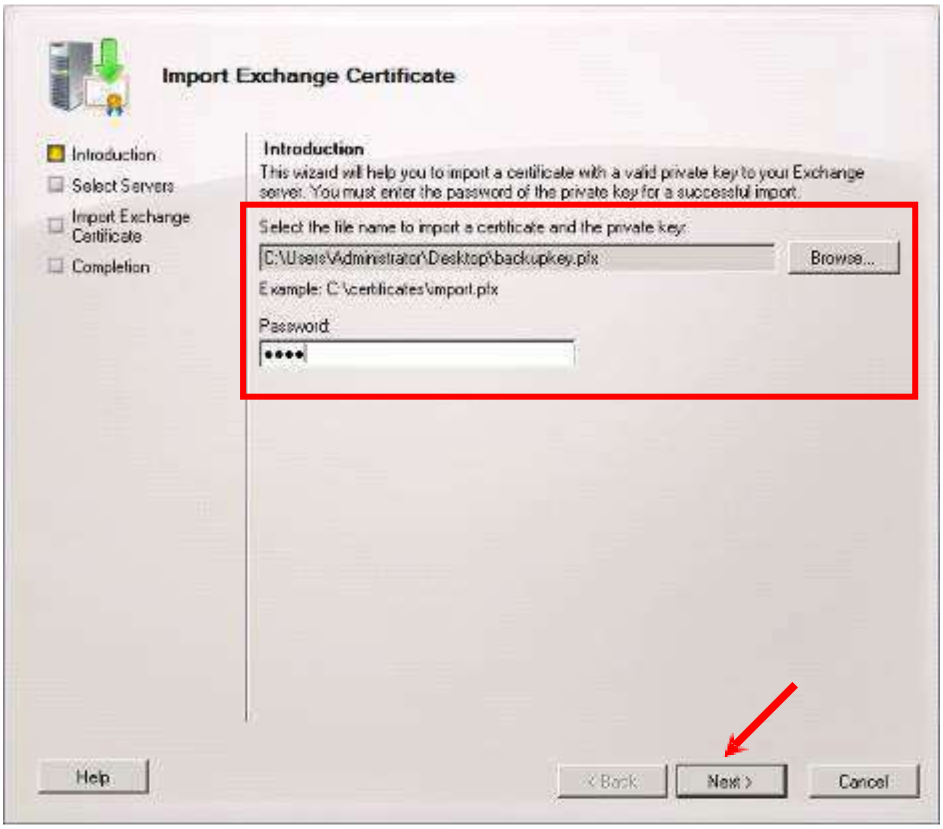
To copy the contents of this page, press CTRL+C.

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**.



Import Exchange Certificate

Introduction

This wizard will help you to import a certificate with a valid private key to your Exchange server. You must enter the password of the private key for a successful import.

Select the file name to import a certificate and the private key:

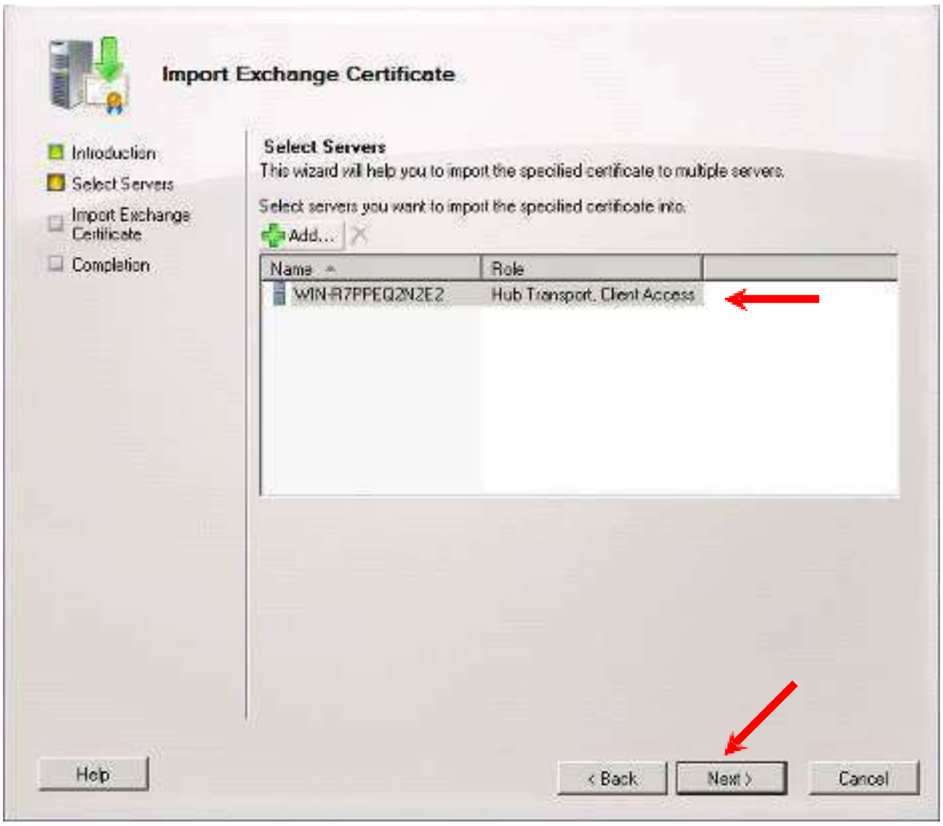
C:\Users\Administrator\Desktop\backupkey.pfx

Example: C:\certificates\import.pfx

Password:

••••

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



Import Exchange Certificate

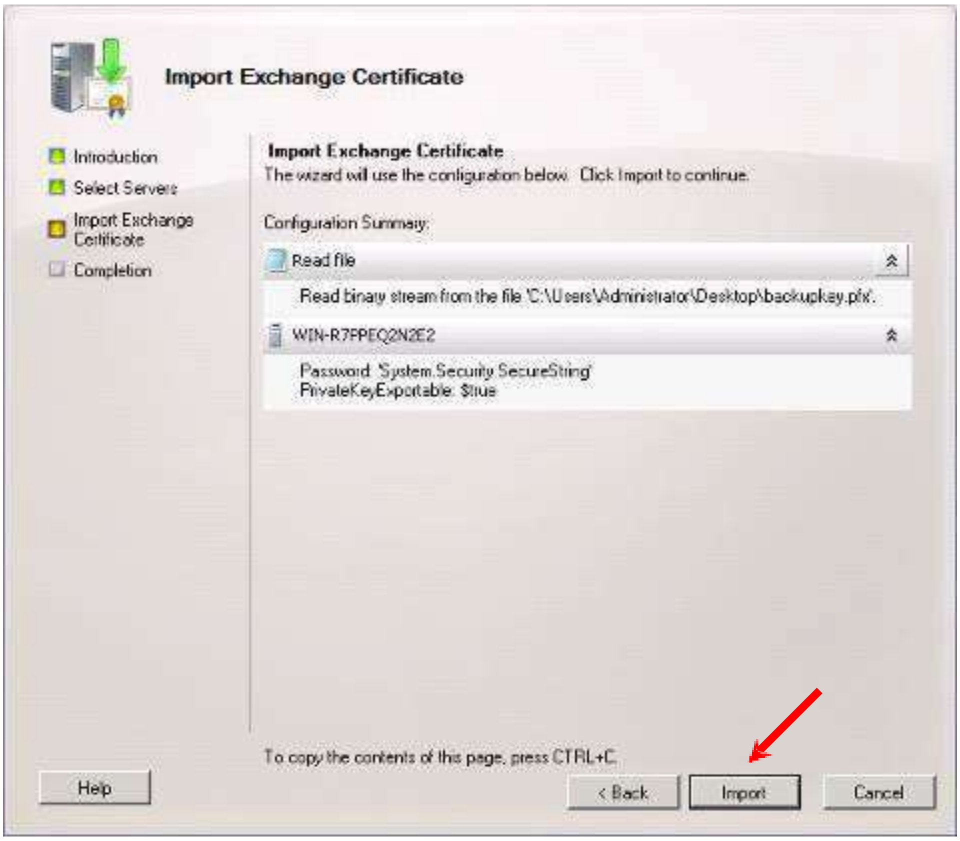
Select Servers

This wizard will help you to import the specified certificate to multiple servers.

Select servers you want to import the specified certificate into.

Name	Role
WIN-R7PPEQ2N2E2	Hub Transport, Client Access

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



Import Exchange Certificate

The wizard will use the configuration below. Click Import to continue.

Configuration Summary:

Read file

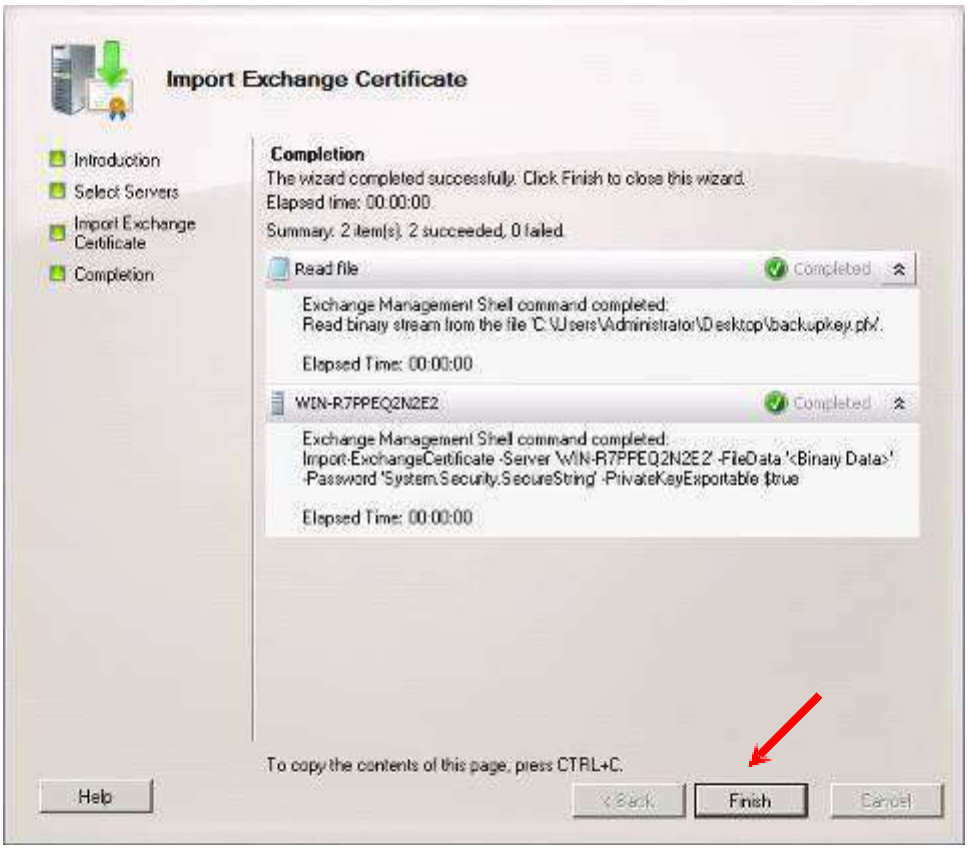
Read binary stream from the file 'C:\Users\Administrator\Desktop\backupkey.pfx'.

WIN-R7PPEQ2N2E2

Password: 'System.Security.SecureString'
PrivateKeyExportable: $true

To copy the contents of this page, press CTRL+C.

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



Completion

The wizard completed successfully. Click Finish to close this wizard.

Elapsed time: 00:00:00

Summary: 2 item(s). 2 succeeded, 0 failed.

Read file — Completed

Exchange Management Shell command completed:
Read binary stream from the file 'C:\Users\Administrator\Desktop\backupkey.pfx'.

Elapsed Time: 00:00:00

WIN-R7PPEQ2N2E2 — Completed

Exchange Management Shell command completed:
Import-ExchangeCertificate -Server 'WIN-R7PPEQ2N2E2' -FileData '<Binary Data>' -Password 'System.Security.SecureString' -PrivateKeyExportable $true

Elapsed Time: 00:00:00

To copy the contents of this page, press CTRL+C.