e-Cert (Server) User Guide

For Replacement of the Existing Cross-Certificate with the New Cross-Certificate

Version 1.0

Contents

A. Background

In 2019, Hongkong Post Certification Authority ("HKPCA") has completed the rollover of Hongkong Post Root CA1 ("Root CA1") to Hongkong Post Root CA3 ("Root CA3") for issuance of e-Cert (Server). At that time, HKPCA has also deployed a cross-certificate ("Existing Cross-Cert", also known as "Cross-Cert 2019") signed by Root CA1 for installation by subscribers on their websites/servers adopting e-Cert (Server) to ensure the accessibility by "older versions of mobile/desktop devices not yet preloaded with Root CA3" ("Older Devices")

Root CA1 and the Existing Cross-Cert will expire on 15 May 2023. After the expiry, end-users / client processes using Older Devices may encounter problems when making connections to Internet sources installed with e-Cert (Server), such as:

- Mobile apps may fail to work
- Website may not be accessible by web browsers under some older versions of OS platforms
- System-to-System communication may fail between servers.

To ensure the above accessibility by the Older Devices after the expiry date, HKPCA has made ready a new cross-certificate signed by "GlobalSign Root CA - R3" ("New Cross-Cert", also known as "Cross-Cert 2022") in establishing a trust relationship from Root CA 3 to the "GlobalSign Root CA - R3". GlobalSign is a WebTrust-accredited Certification Authority with its root certificate "GlobalSign Root CA - R3" of validity up to 18 March 2029 trusted by major platforms of Older Devices according to the compatibility information[1] as summarised below:

- **Google Chrome** and other supported web browsers on Android 3 or above.
- **Microsoft Internet Explorer / Edge** and other supported web browsers on Windows XP or above.
- **Apple Safari** and other supported web browsers on iOS 4 or above, MacOS X 10.6.4 or above.
- **Mozilla Firefox** version 3.6.12 or above on all supported platforms.

This user guide aims to provide e-Cert (Server) subscribers with necessary procedures for replacement of the Existing Cross-Cert with the New Cross-Cert on their servers, and verification of ensuring successful changes. For other guidelines for generation of key pairs and Certificate Signing Request ("CSR"), and installation of e-Cert (Server), you may refer to e-Cert (Server) User Guide.

[1] Full support list of GlobalSign Root CA – R3 can be found at: https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-ubiquity

B. Details of Existing Cross-Cert, New Cross-Cert and their compatibility with major platforms

Root Certificate:	Existing Cross-Cert	New Cross-Cert
Valid from:	2017-08-12	2022-11-16
Valid to:	2023-05-15	2029-03-18
Signed by:	Hongkong Post Root CA 1	GlobalSign Root CA – R3
Root included in Android since:	4	3
Root included in iOS since:	4	4
Root included in Windows since:	XP	XP
Root included in MacOS since:	10.5.8	10.6.4
Root included in Firefox since:	3.5.9	3.6.12

The New Cross-Cert can adequately support the Older Devices covered by the Existing Cross-Cert.

C. Stock-taking the Existing Cross-Cert

HKPCA would provide each subscriber organisation via email attached with a list of all its subscribed valid e-Cert (Server) as of 1 December 2022 in representation of domain name(s) under responsibility of each related Authorised Representative ("AR"). The list is in the order of AR(s) and domain names.

There are common system architectures that subscriber organisations may have deployed their e-Cert (Server) in multiple domains or multiple servers. The list of domain names are provided in the following format:

Authorised Representative	Subscriber ref. no. ("SRN")	Cert Type (Single / Wildcard/ Multi-domain)	Domain Name (Note)	Date of Subscription expiry

Note:

- For e-Cert (Server) with single domain name, one entry for the Server Name in the certificate is shown.

  It is important to note that, subject to installation and configuration, if the certificate has been deployed in multiple servers, each server that the domain name is related to should be checked for the replacement of the Existing Cross-Cert. Conversely, if multiple certificates have been deployed in a single server to support their respective domain names, each installation of the certificate that the domain name is related to should be checked for the replacement of the Existing Cross-Cert.
- For e-Cert (Server) with Wildcard feature, one entry of the Server Name in the certificate is shown, where a wildcard character (i.e. an asterisk character '*') appears in the left-most component of the domain name, such as *.DEPT1.gov.hk.
- For e-Cert (Server) with multi-domain feature, multiple entries of domain names in the Subject Alternative Name extension of the certificate are shown.

Every e-Cert Subscriber is reminded to stock-take all occurrences of Existing Cross-Cert in relation to the domain names supported by current server configuration and scalability in accordance with the configuration management / inventory records of your organisation. A handful of free tools, such as OpenSSL are readily available for verifying whether the Existing Cross-Cert is being utilized in the certificate chain, based on a specified domain name.

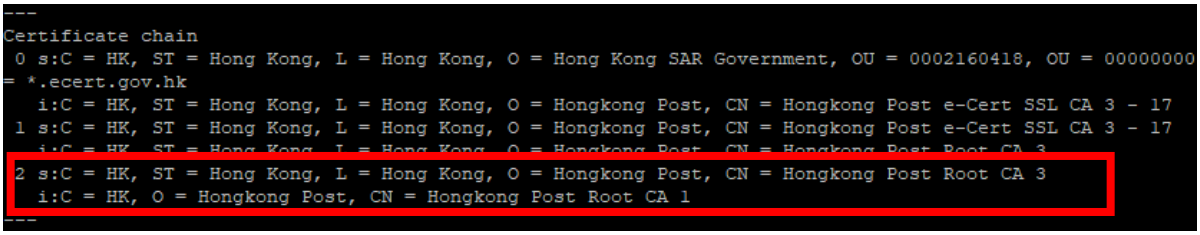
In the ensuing paragraphs, we will provide some guidelines of how to use OpenSSL as an example to examine the certificate chain based on a specified domain name.

For every domain name, please identify where the web server(s) is located, and check if the Existing Cross-Cert has been installed on the web server(s). You can search out every occurrence of the Existing Cross-Cert for replacement by running the following procedures:

1. On a device where OpenSSL (version 1.1.1 or later) is installed, type the following command to check every domain name:

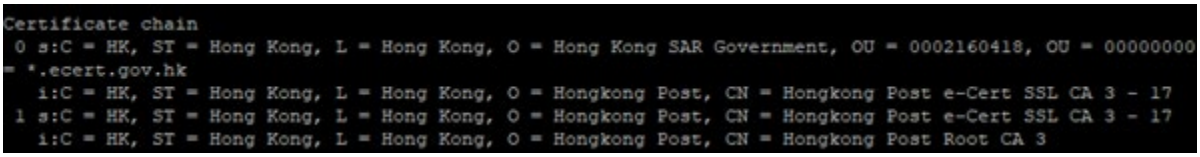
   openssl s_client -connect [domain name of e-Cert (Server)]:443

2. If the Existing Cross-Cert is installed for the domain name, you should see the Old Certificate Chain. Please stock-take the Existing Cross-Cert and its related web servers for follow-up at **Section D**.



Old Certificate Chain
(with Existing Cross-Cert installed)

3. If no Existing Cross-Cert is installed for the domain name, indicating that the related web server is not affected by the expiry of the Existing Cross-Cert, you should see the Certificate Chain below. In this case, for a domain name not using the Existing Cross-Cert, there is no need to install a New Cross-Cert on the related web server.



Certificate Chain
(NO Existing Cross-Cert installed)

If you have any problems in using the OpenSSL tool, please feel free to contact our customer service at Section G.

D. Replacement of the Existing Cross-Cert with the New Cross-Cert

Note: It is assumed that you have identified an occurrence of the Existing Cross-Cert signed by Root CA1 on a web server, i.e. by inspecting the Old Certificate Chain based on the stock-taking exercise at Section C.

Please download the New Cross-Cert (i.e. root_ca_3_x_gsca_r3_pem.crt) and copy it to the web servers where Existing Cross-Certs are installed.

For every web server with occurrence(s) of Existing Cross-Cert identified, please conduct the following procedures, either (A) or (B) depending on an Apache Web Server or Microsoft Web Server:

(A) On Apache Web Server

1. Please make ready the following files:

   a) If you are using **e-Cert (Server)** issued by **"Hongkong Post e-Cert SSL CA 3 - 17"**:

   ```
   /usr/local/apache/conf/ssl.crt/ecert_ssl_ca_3-17_pem.crt
   /usr/local/apache/conf/ssl.crt/root_ca_3_x_gsca_r3_pem.crt
   ```

   b) If you are using **EV e-Cert (Server)** issued by **"Hongkong Post e-Cert EV SSL CA 3 - 17"**:

   ```
   /usr/local/apache/conf/ssl.crt/ecert_ev_ssl_ca_3-17_pem.crt
   /usr/local/apache/conf/ssl.crt/root_ca_3_x_gsca_r3_pem.crt
   ```

2. Change to the Apache server directory containing the certificate files (e.g. /usr/local/apache/conf/ssl.crt/), and then type the following command at the prompt to create a certificate chain file (hkpostca_2022.crt):

   a) If you are using **e-Cert (Server)** issued by **"Hongkong Post e-Cert SSL CA 3 - 17"**:

   ```
   cat ecert_ssl_ca_3-17_pem.crt root_ca_3_x_gsca_r3_pem.crt >
   hkpostca_2022.crt
   ```

   b) If you are using **EV e-Cert (Server)** issued by **"Hongkong Post e-Cert EV SSL CA 3 - 17"**:

   ```
   cat ecert_ev_ssl_ca_3-17_pem.crt root_ca_3_x_gsca_r3_pem.crt >
   hkpostca_2022.crt
   ```

3. Open the Apache SSL configuration file (e.g. /usr/local/apache/conf/ssl.conf) with a text editor.

4. Locate your SSL VirtualHost container, and then modify the following line of code:

   From:

```
# Hongkong Post Root CA Certificate Chain
SSLCertificateChainFile /usr/local/apache/conf/ssl.crt/hkpostca.crt
```

   To:

```
# Hongkong Post CA Certificate Chain
SSLCertificateChainFile /usr/local/apache/conf/ssl.crt/hkpostca_2022.crt
```

   The modified config should be similar to below:

```
<VirtualHost *:443>

# Private Key
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/myserver.key
# Hongkong Post e-Cert (Server)
SSLCertificateFile /usr/local/apache/conf/ssl.crt/cert0000812104.cer
# Hongkong Post CA Certificate Chain
SSLCertificateChainFile /usr/local/apache/conf/ssl.crt/hkpostca_2022.crt

</VirtualHost>
```

5. Save the changes and exit the editor.

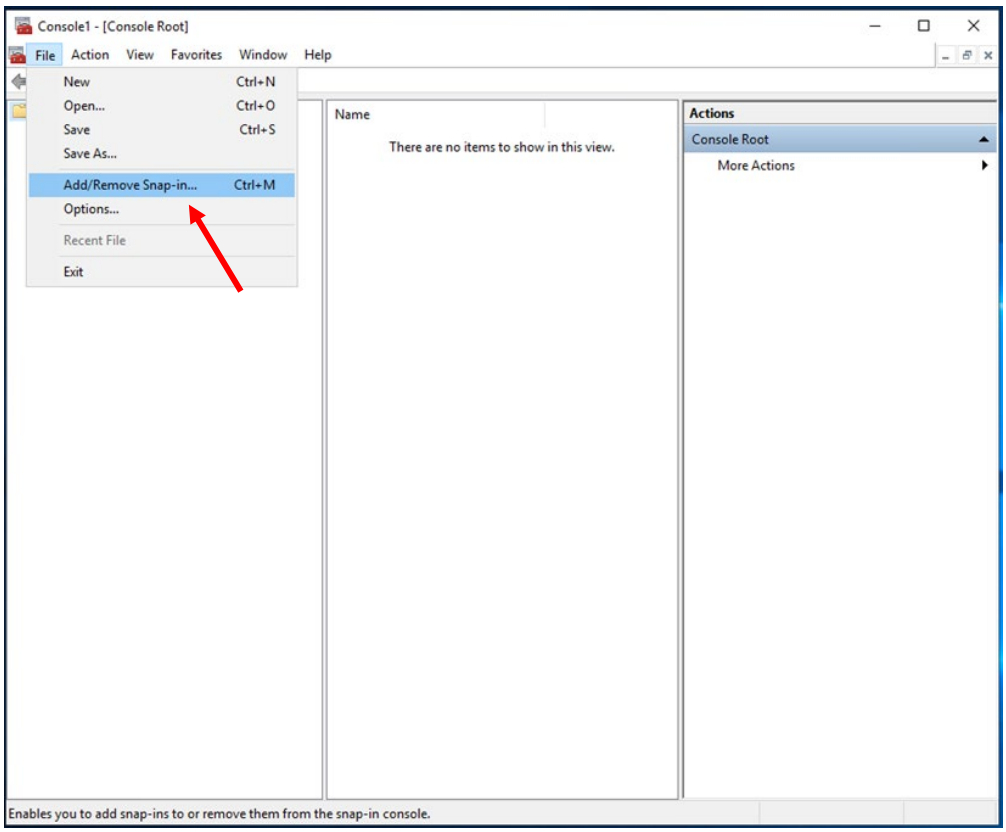
6. Restart your Apache server using the following commands.

```
apachectl stop
apachectl start
```

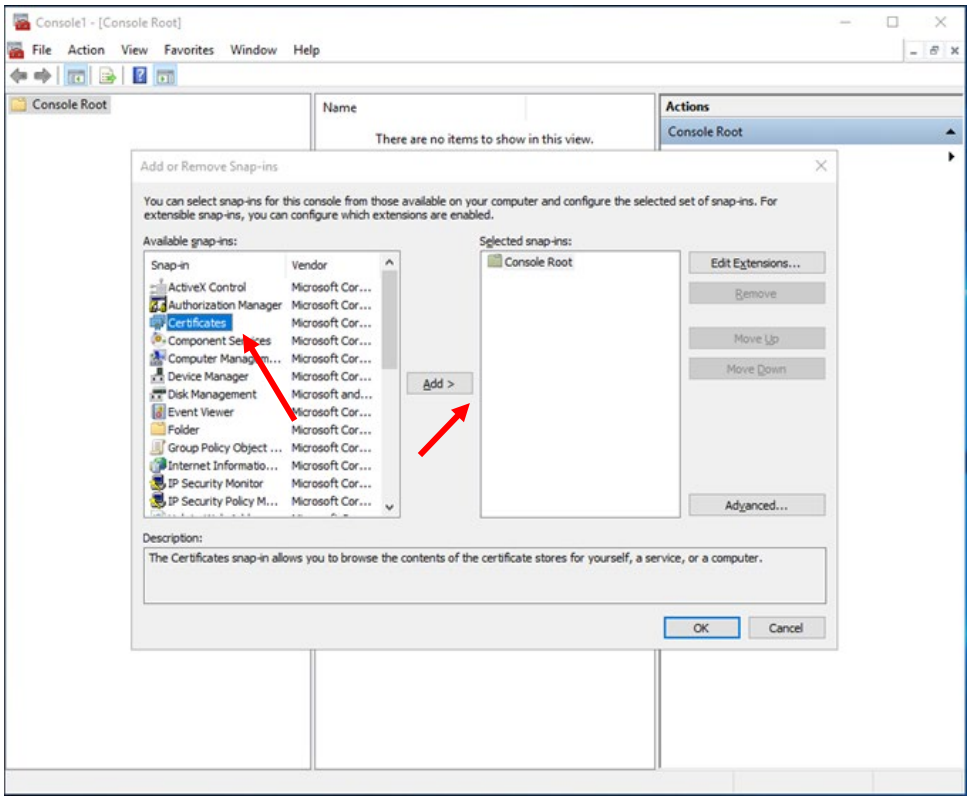
(B) <u>On Microsoft IIS / Microsoft Exchange Server</u>

1. On your Windows Server when Microsoft IIS / Microsoft Exchange Server is installed, Start **Microsoft Management Console (MMC)** by clicking "**Start**" > "**Run**", type "**mmc**" and click **OK**, and then select "**Add/Remove Snap-in**"

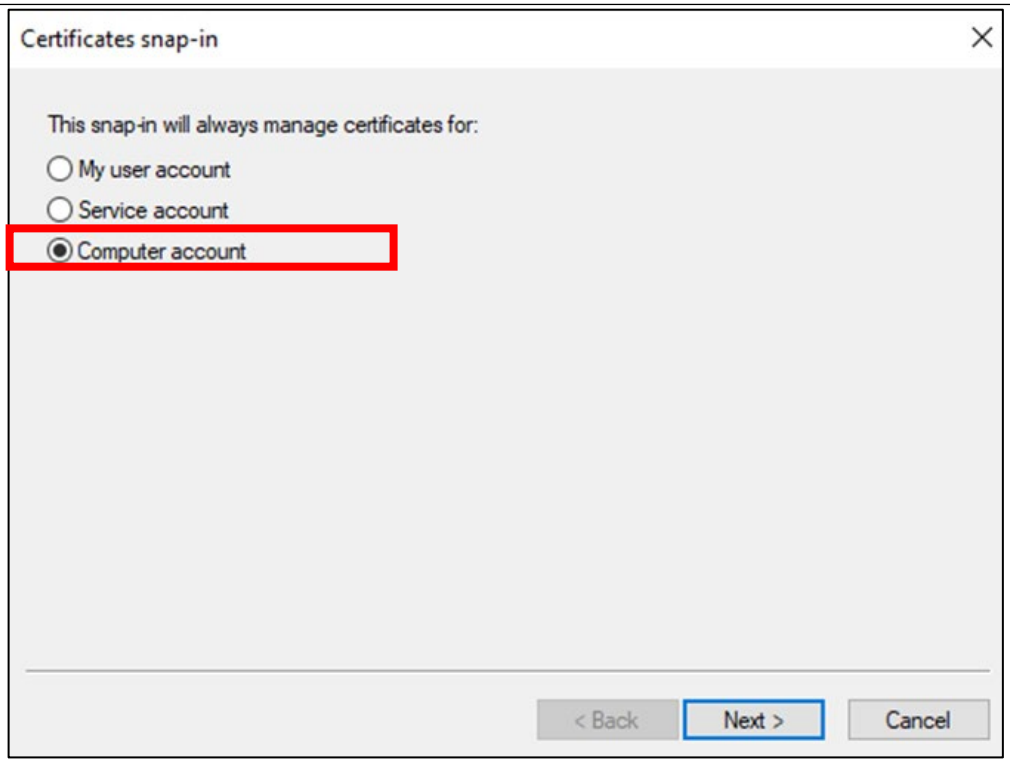
from the "**File**" menu.



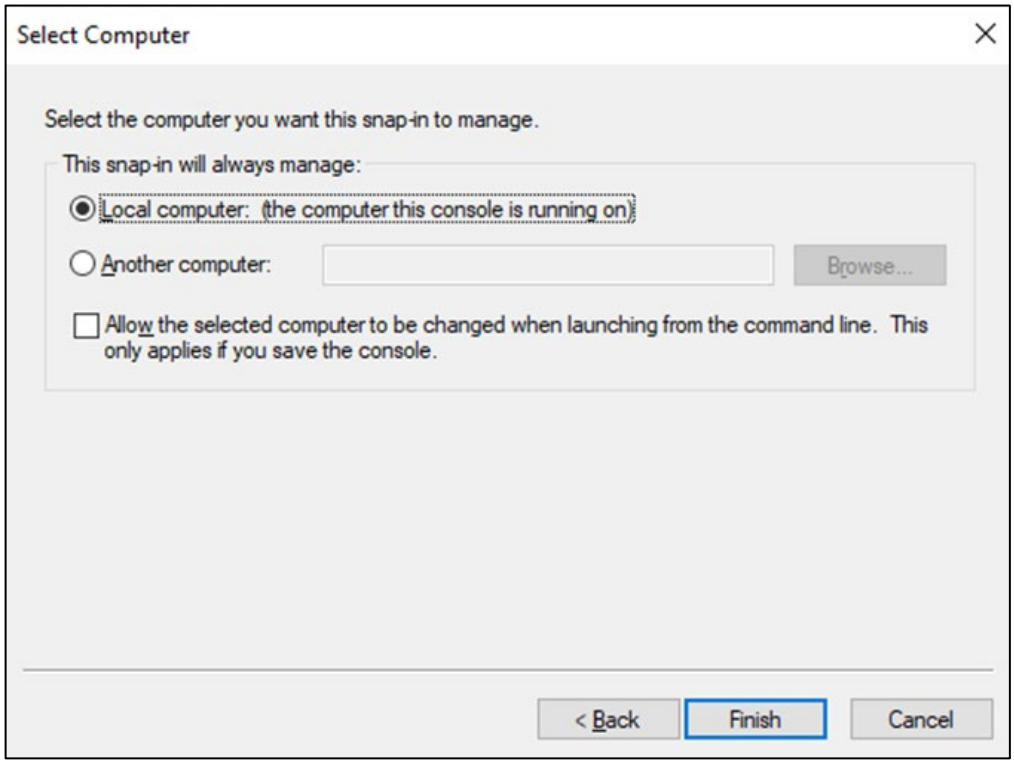
2. Select "**Certificate**" then Click "**Add**".



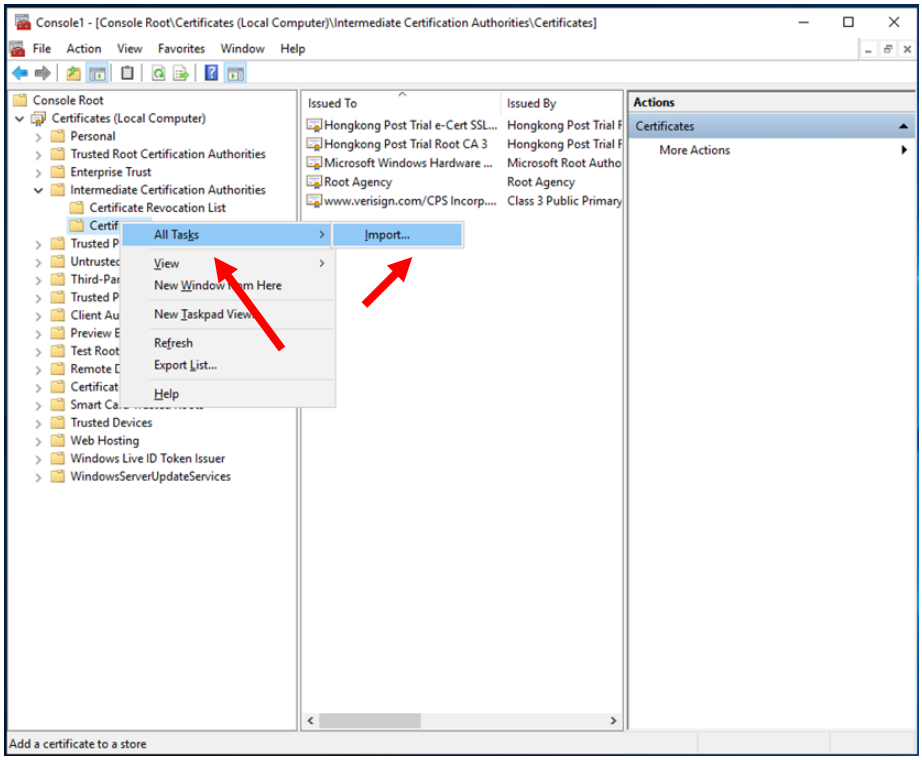
3. Select "**Computer account**", and then click "**Next**".


Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel

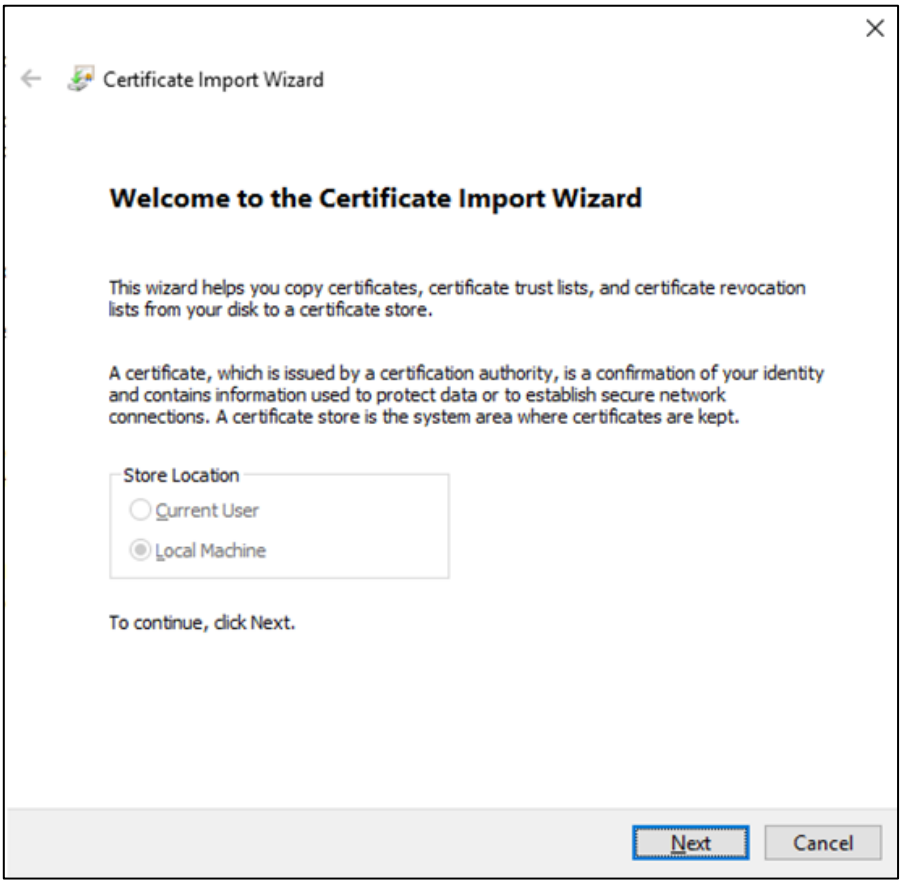
4. Select "**Local computer**", and then click "**Finish**".



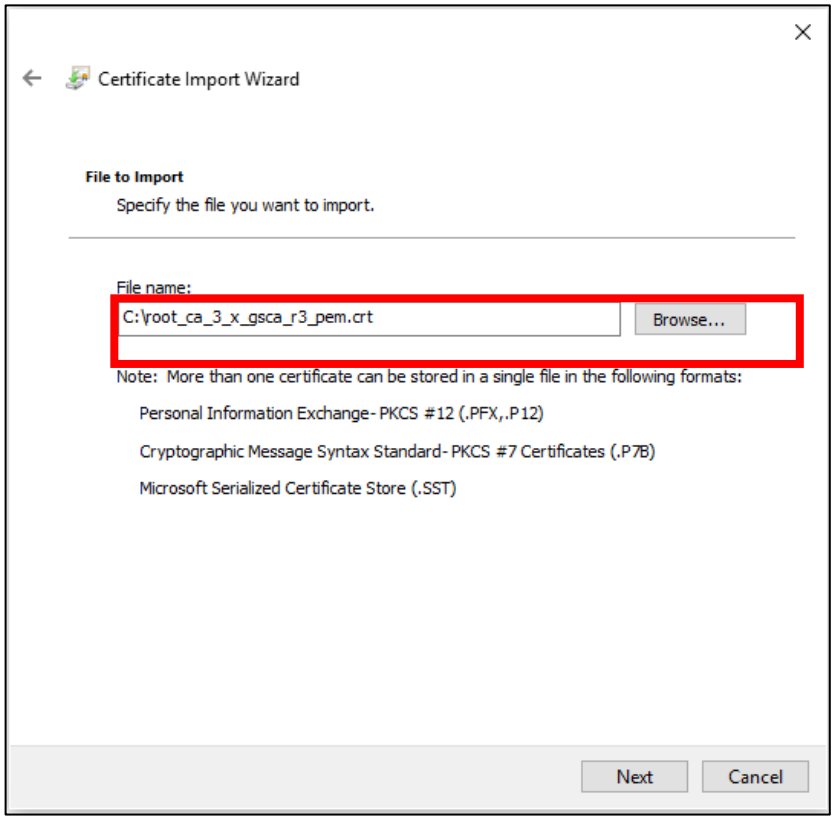
5. Expand the **Certificates (Local Computer)** node, then right-click the **Intermediate Certification Authorities** and then select **All Tasks > Import**.



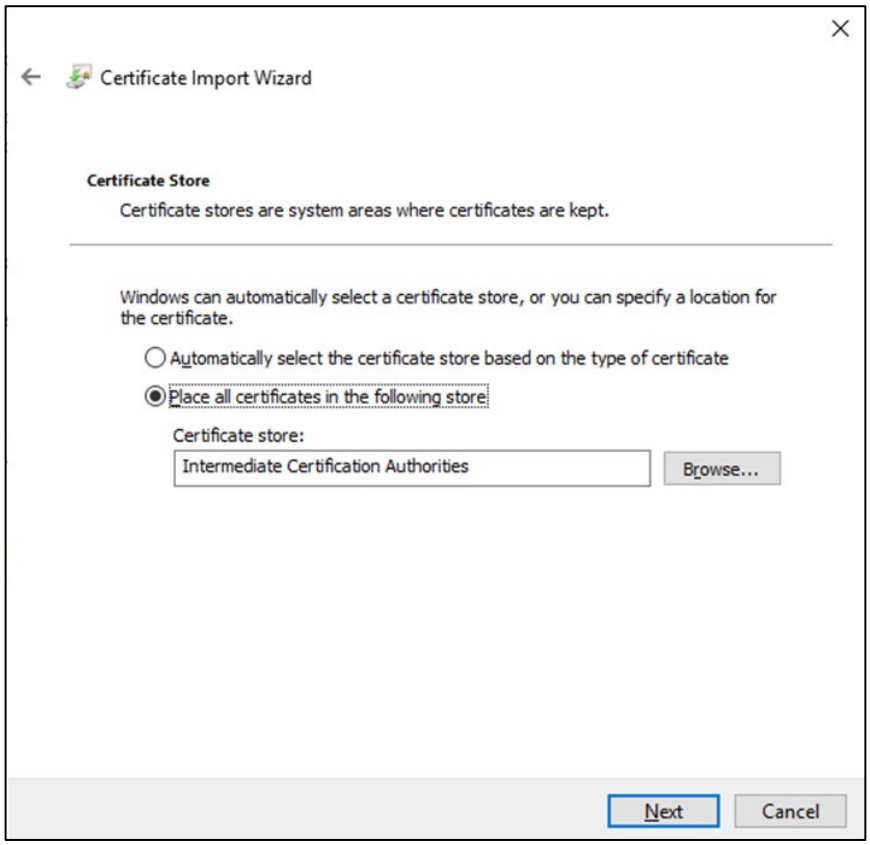
6. In the **Certificate Import Wizard**, click **Next** to continue.



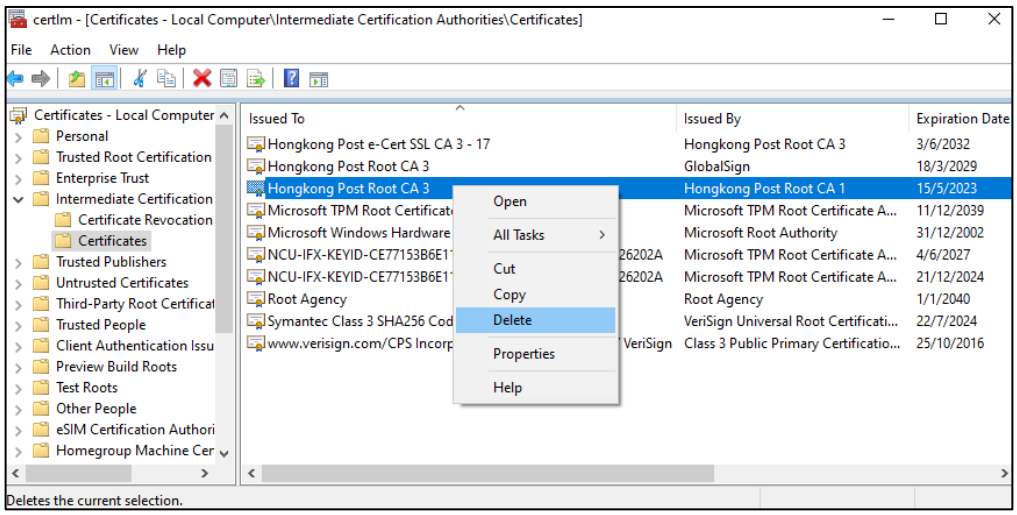
7. Click **Browse** to locate the **New Cross-Cert** certificate that you downloaded in the beginning of this Section D (i.e. root_ca_3_x_gsca_r3_pem.crt), and then click **Next**.



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



9. Delete the **Existing Cross-Cert** (i.e. "Hongkong Post Root CA 3" signed by "Hongkong Post Root CA 1") in **Intermediate Certification Authorities** > **Certificates**.



10. Verify the **New Cross-Cert** has been imported to **Intermediate Certification Authorities** > **Certificates** and the Existing Cross-Cert cannot be found.

11. Reboot the server.

E. Post-replacement test

After the replacement exercise completed in Section D, please perform the post-replacement test below to ensure each New Cross-Cert installed relating to the domain name(s) is now functional.

1. On a device where OpenSSL (version 1.1.1 or later) is installed, type the following commands for each domain name after replacement:

   openssl s_client -connect [domain name of e-Cert (Server)]:443

2. Confirm the New Cross-Cert with the following issuer information has been included in the Certificate Chain:
   i: OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign

```
---
Certificate chain
 0 s:C = HK, ST = Hong Kong, L = Hong Kong, O = Hong Kong SAR Government, CN = www.ecert.gov.hk
   i:C = HK, ST = Hong Kong, L = Hong Kong, O = Hongkong Post, CN = Hongkong Post e-Cert SSL CA 3 - 17
 1 s:C = HK, ST = Hong Kong, L = Hong Kong, O = Hongkong Post, CN = Hongkong Post e-Cert SSL CA 3 - 17
   i:C = HK, ST = Hong Kong, L = Hong Kong, O = Hongkong Post, CN = Hongkong Post Root CA 3
 2 s:C = HK, ST = Hong Kong, L = Hong Kong, O = Hongkong Post, CN = Hongkong Post Root CA 3
   i:OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
---
```

New Certificate Chain
(with New Cross-Cert installed)

If you have any problems in using the OpenSSL tool, please feel free to contact our customer service at Section G.

F. Accessibility test on Older Devices

With installation of the New Cross-Cert, web servers using e-Cert (Server) under Root CA 3 can be accessible by Older Devices. Please test the accessibility of the domain names by browsers or mobile apps with the Older Devices.

A testing setup is provided below for your reference.

1. Checking if all Certificates are in order

Item	Name	Validity	Remark
1-1	Hongkong Post Root CA 3 (New Cross Cert)	16 Nov 2022 – 18 Mar 2029	This is signed by GlobalSign Root CA – R3 and included in the Certificate Chain
1-2a	Hongkong Post e-Cert SSL CA 3-17	3 Jun 2017 – 3 Jun 2032	This should be included in the Certificate Chain if **e-Cert (Server)** is used.
1-2b	Hongkong Post e-Cert EV SSL CA 3 - 17		This should be included in the Certificate Chain if **EV e-Cert (Server)** is used.
1-3a	e-Cert (Server)	Please ensure its "Valid to" date is after 15 May 2023 (i.e. the expiry date of Root CA1).	This should be included in the Certificate Chain if **e-Cert (Server)** is used.
1-3b	EV e-Cert (Server)		This should be included in the Certificate Chain if **EV e-Cert (Server)** is used.

2. Test Cases – For Browsers

Domain Names Tested: www.organisation.com adopting e-Cert (Server)

Case	Type	Suggested Testing	System clock set at testing devices	
			2023-05-14 00:00	2023-05-17 00:00
2-1	Browser	You may browse www.organisation.com using Chrome browser under any one Android device of version 10 or below	Positive	Positive
2-2	Browser	You may browse www.organisation.com using Safari browser under any one iOS device of version 14 or below	Positive	Positive
2-3	Browser	You may browse www.organisation.com using IE browser under any one Windows device of version 8.1 or below	Positive	Positive
2-4	Browser	You may browse www.organisation.com using Safari browser under any one macOS devices of version 11 or below	Positive	Positive
2-5	Browser	You may browse www.organisation.com using Firefox browser version 67 or below under any Windows/Android/iOS/macOS devices	Positive	Positive

The table above is not an exhaustive list of test cases. You may include testing of other device platforms, such as Harmony OS, if applicable.

3. Test Cases – For Mobile Apps

App: Organisation-App

Domain Names Tested: www.organisation.com adopting e-Cert (Server)

Case	Type	Suggested Testing	System clock set at testing devices	
			2023-05-14 00:00	2023-05-17 00:00
3-1	Android App -> Out-of-App Browser Calls	You may click the link or icon in the "Organisation-App" which will open an Out-of-App browser to browse www.organisation.com using Chrome browser under any one Android device of version 10 or below	Positive	Positive
3-2	Android App	You may check if the In-App WebView which links to www.organisation.com displays correctly in the "Organisation-App" any one Android device of version 10 or below	Positive	Positive
3-3	Android App	You may check if the data returned from an API call to www.organisation.com displays correctly in the "Organisation-App" under any one Android device of version 10 or below	Positive	Positive
3-4	iOS App -> Out-of-App Browser Calls	You may click the link or icon in the "Organisation-App" which will open an Out-of-App browser to browse www.organisation.com using Safari browser under any one iOS device of version 14 or below	Positive	Positive

3-5	iOS App	You may check if the In-App WebView which links to www.organisation.com displays correctly in the "Organisation-App" under any one iOS device of version 14 or below	Positive	Positive
3-6	iOS App	You may check if the data returned from an API call to www.organisation.com displays correctly in the "Organisation-App" under any one iOS device of version 14 or below	Positive	Positive

The table above is not an exhaustive list of test cases. You may include testing of other device platforms, such as Harmony OS, if applicable.

4. Test for System-to-System Communications

For system-to-system communications in which client processes may verify and trust the server processes installed with e-Cert (Server) through the Existing Cross-Cert (e.g. connections between web servers / middleware for B2B applications, internal server-to-server calls with an organisation), please examine thoroughly both client and server configurations / OS versions whether to adopt the New Cross-Cert in server process or to directly trust the Root CA3 in client process, and conduct testing of the related client-to-server processes.

G. HKPCA Support

For enquiries, please call HKPCA e-Cert Customer Service at 2921 6633 or email to crosscert-support@ecert.gov.hk.