Hongkong Post e-Cert
香港郵政電子核證

e-Cert (Server) User Guide

For Apache Web Server

Revision Date: January 2026

Contents

A. Guidelines for e-Cert (Server) Applicant

After receipt and approval of an e-Cert (Server) application, Hongkong Post Certification Authority will send an e-mail with subject “Submission of Certificate Signing Request (CSR)” to request the Authorized Representative to submit the CSR at the Hongkong Post CA web site.

This user guide is for reference by applicants of e-Cert (Server) in generating their key pair and Certificate Signing Request (CSR) using Apache Web Server. 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)**.

B. Generating Certificate Signing Request (CSR)

1. This user guide uses the utility "openssl" that comes with the OpenSSL package as an example to generate the key pair and Certificate Signing Request (CSR). Since the directory path of the utility differs from one server to another, applicants should therefore refer to their server documentation for details.

   Type the following command at the prompt to generate a 2048-bit RSA private key (myserver.key) encrypted in AES-256. You will be prompted to enter and confirm a password.

   Note: Bit length smaller than 2048 may not be strong enough, while greater than 2048 may be incompatible with certain web browsers. It is recommended the bit length of the encryption key to be 2048 in order to support better security strength.

   Note: It is very important that you remember this password. You are required to provide this password when you start your Apache server.

   ```
   openssl genrsa –aes256 –out myserver.key 2048
   ```

2. Type the following command at the prompt to generate the Certificate Signing Request (CSR) (myserver.csr) using the private key (myserver.key) generated above. You will be prompted for the password.

   ```
   openssl req –new –key myserver.key –out myserver.csr
   ```

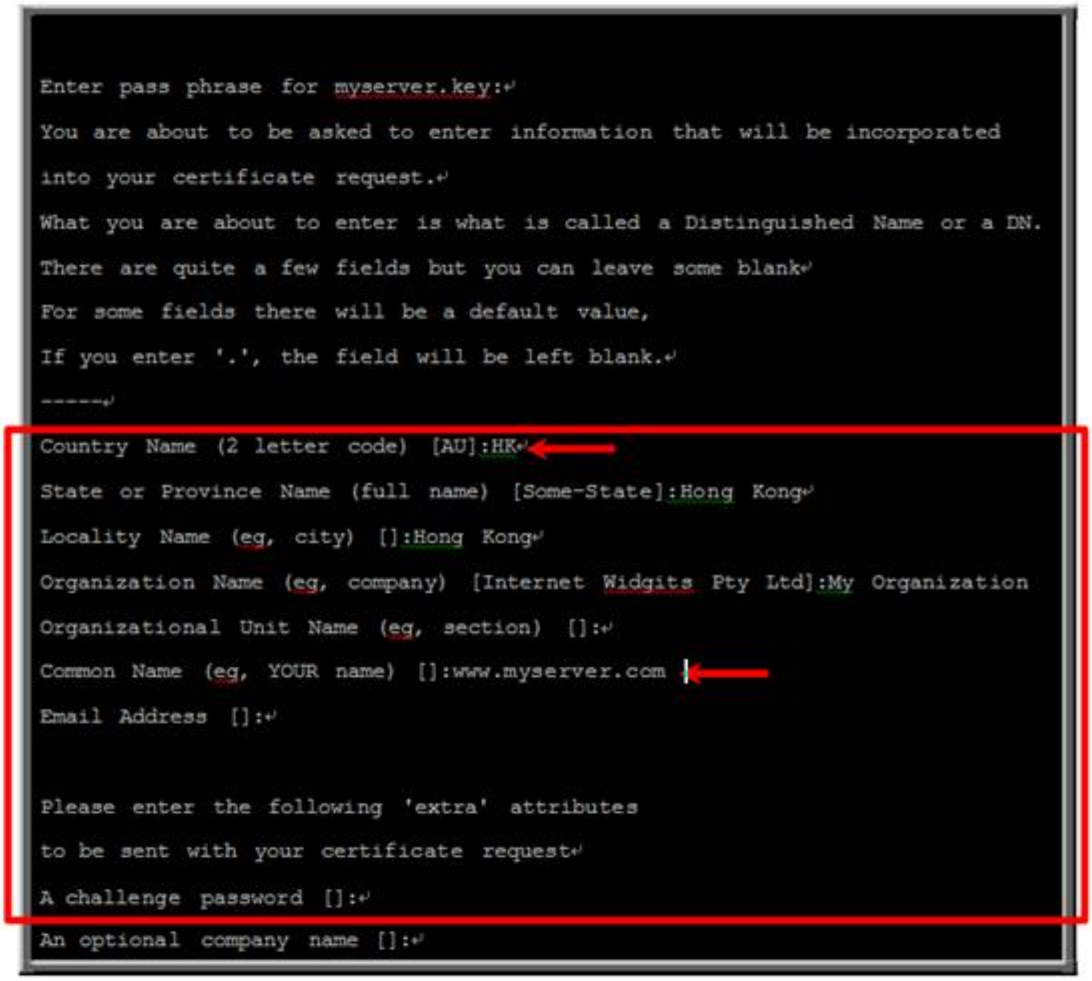
   Enter the following information when prompted for the following X.509 attributes of the certificate:

Attribute	Description	Example
Country	Specify "HK"	HK
State or Province	Specify "Hong Kong"	Hong Kong
Locality	Specify "Hong Kong"	Hong Kong
Organization	Specify organization name	My Organization
Organizational Unit	Hit <Enter> to leave blank	
Common Name	Specify server name	www.myserver.com
Email Address	Hit <Enter> to leave blank	

You will be prompted for extra attributes (i.e. challenge password and optional company name). Hit <Enter> to leave these attributes blank.

> *Note: Please make sure that the correct server name is entered in the "Common Name" field and "HK" in the "Country Name" field.*

> *Note: **For application of e-Cert (Server) with "Multi-domain" feature or EV e-Cert (Server) with "Multi-domain" feature**, please input the "Common Name" field with "Server name used as Subject Name in the Certificate" being filled in the application form. It is not necessary to specify any "Additional Server Name(s)" in the Subject Alternative Name of the CSR to be generated. It will be assigned by the Hongkong Post CA system automatically based on the information applied in the application form when the certificate is issued.*
>
> ***For application of e-Cert (Server) with "Wildcard" feature,** please input the "Common Name" field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk '*', in the left-most component of the server name), e.g. *.myserver.com, being filled in the application form.*

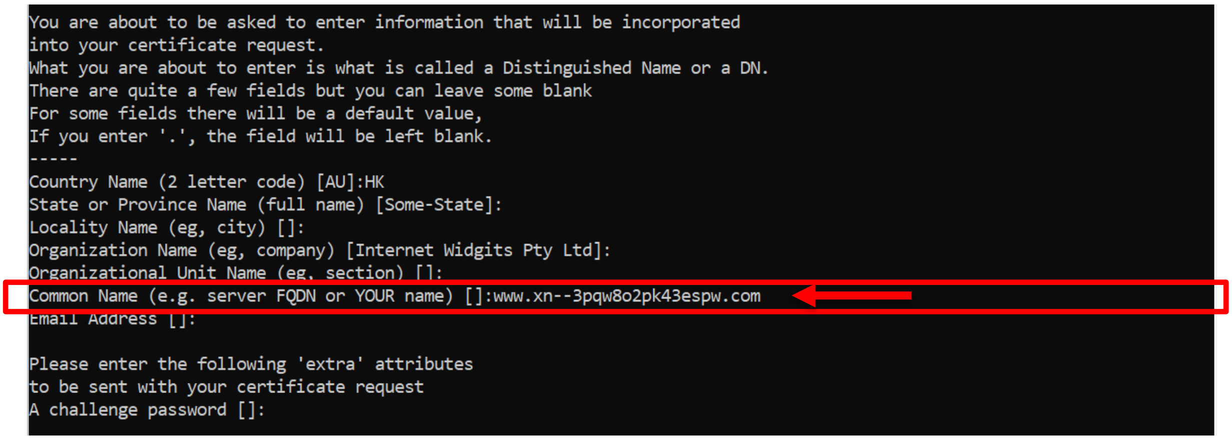


```
Enter pass phrase for myserver.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:HK
State or Province Name (full name) [Some-State]:Hong Kong
Locality Name (eg, city) []:Hong Kong
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Organization
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []:www.myserver.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Note: To generate Certificate Signing Request (CSR) with Chinese Domain Name, use IDN conversion tool to convert Chinese Domain Name into ASCII characters and input the converted name in the "Common Name" field.

Before Conversion	After Conversion
www.我的伺服器.com	www.xn--3pqw8o2pk43espw.com

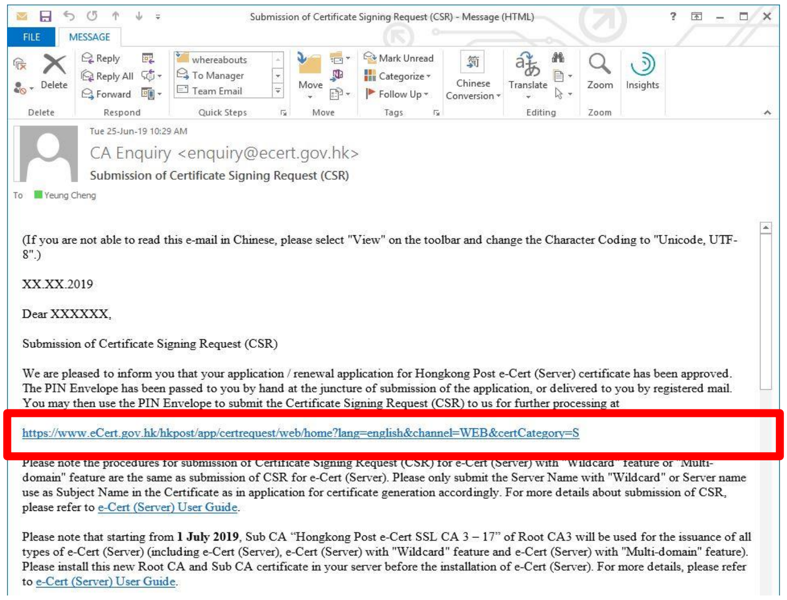


```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:HK
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.xn--3pqw8o2pk43espw.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

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.



Tue 25-Jun-19 10:29 AM

CA Enquiry <enquiry@ecert.gov.hk>

Submission of Certificate Signing Request (CSR)

To Yeung Cheng

(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)

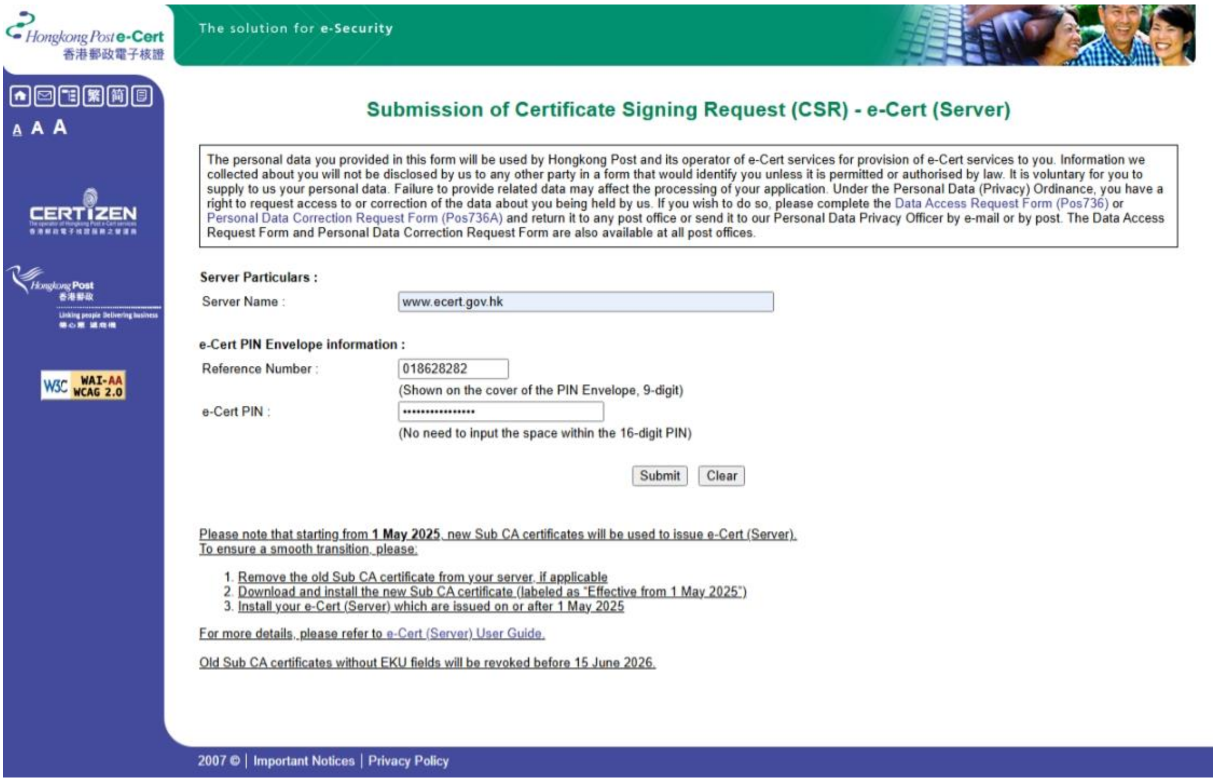
We are pleased to inform you that your application / renewal application for Hongkong Post e-Cert (Server) certificate has been approved. The PIN Envelope has been passed to you by hand at the juncture of submission of the application, or delivered to you by registered mail. You may then use the PIN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

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. 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 : www.ecert.gov.hk

e-Cert PIN Envelope information :

Reference Number : 018628282
(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

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:

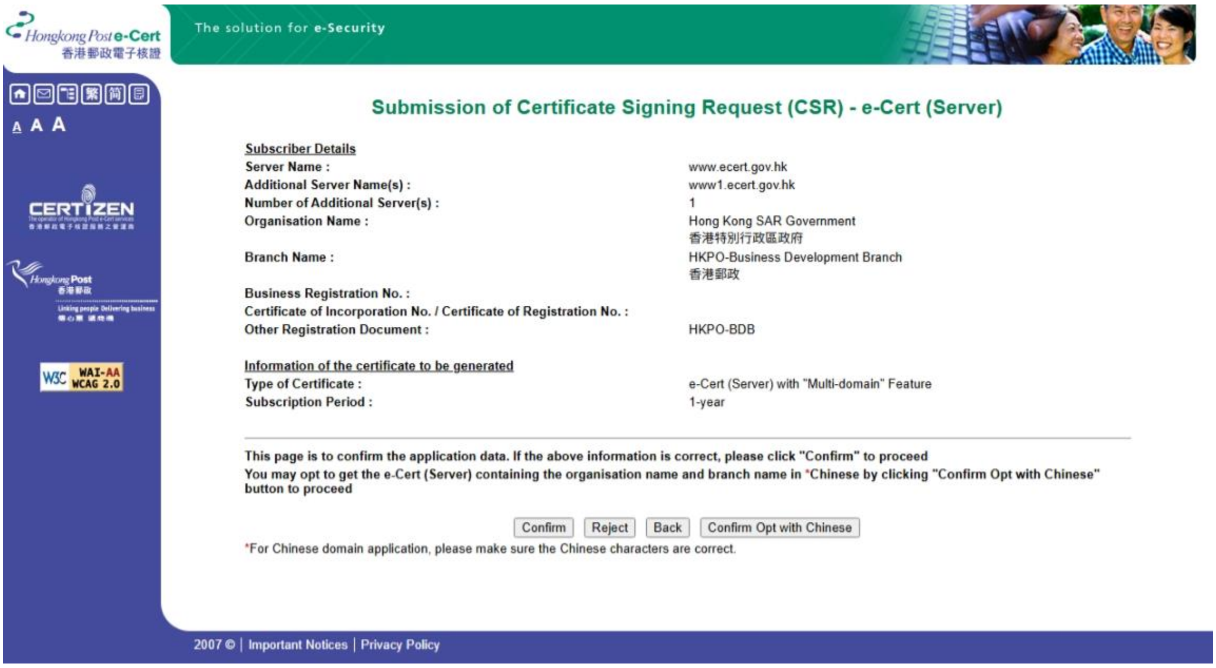
1. Remove the old Sub CA certificate from your server, if applicable
2. Download and install the new Sub CA certificate (labeled as "Effective from 1 May 2025")
3. Install your e-Cert (Server) which are issued on or after 1 May 2025

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.)


Hongkong Post e-Cert 香港郵政電子核證
The solution for e-Security
A A A
CERTIZEN
Hongkong Post 香港郵政
W3C WAI-AA WCAG 2.0

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

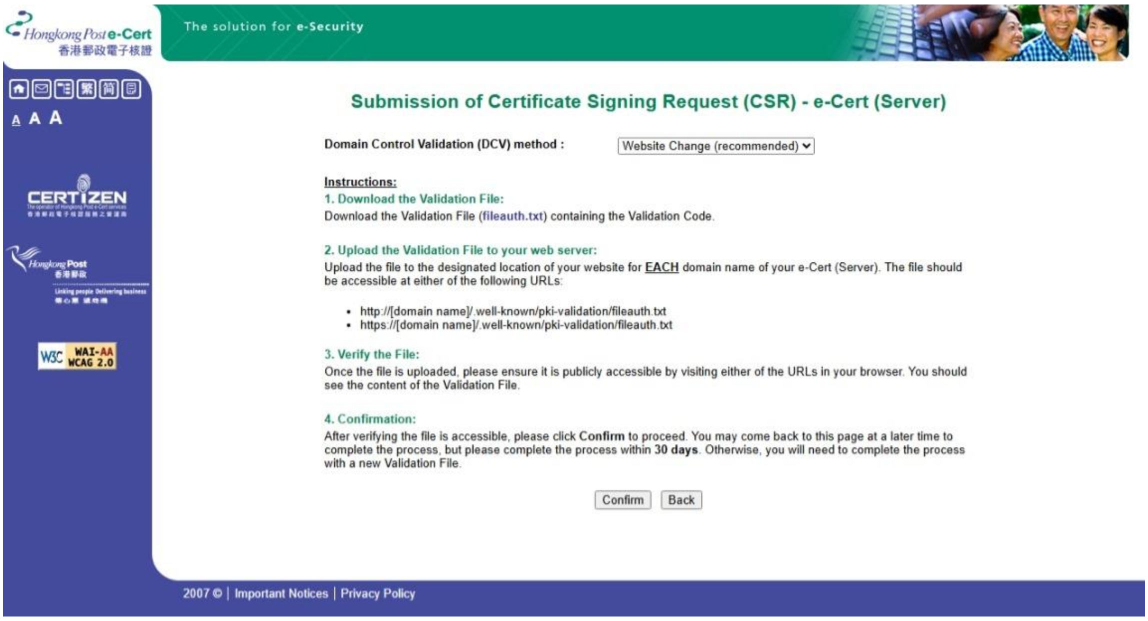
*For Chinese domain application, please make sure the Chinese characters are correct.

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

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

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

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



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

Domain Control Validation (DCV) method : Website Change (recommended)

<u>Instructions:</u>

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 <u>EACH</u> 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
- https://[domain name]/.well-known/pki-validation/fileauth.txt

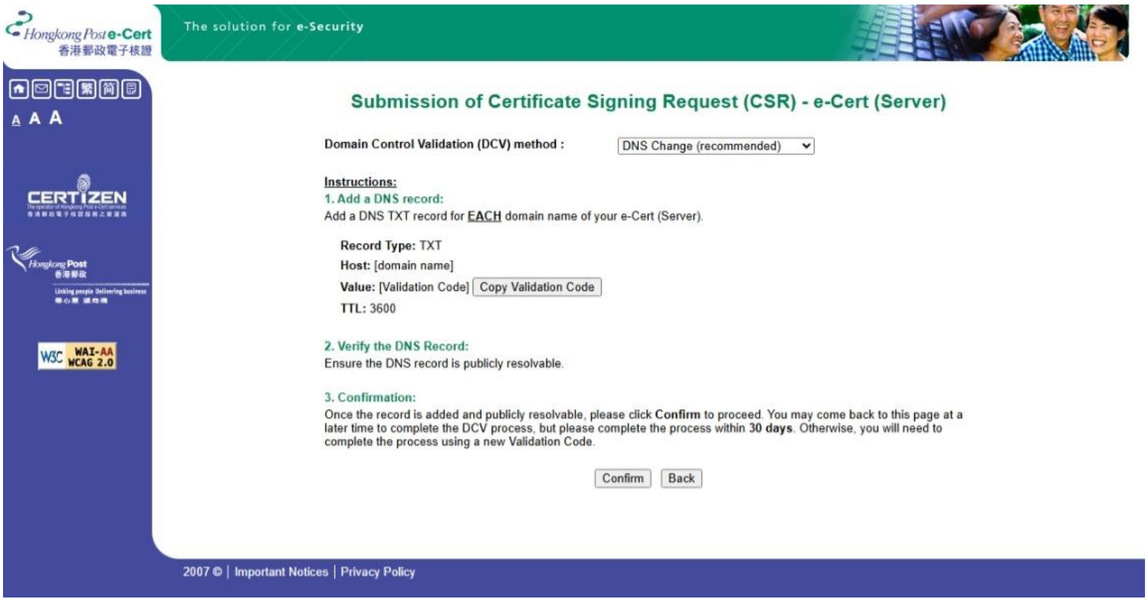
3. Verify the File:

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.

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.


Hongkong Post e-Cert 香港郵政電子核證
The solution for e-Security
A A A
CERTIZEN
Hongkong Post 香港郵政
W3C WAI-AA WCAG 2.0
2007 © | Important Notices | Privacy Policy

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

Domain Control Validation (DCV) method : DNS Change (recommended)

Instructions:

1. Add a DNS record:
Add a DNS TXT record for EACH domain name of your e-Cert (Server).

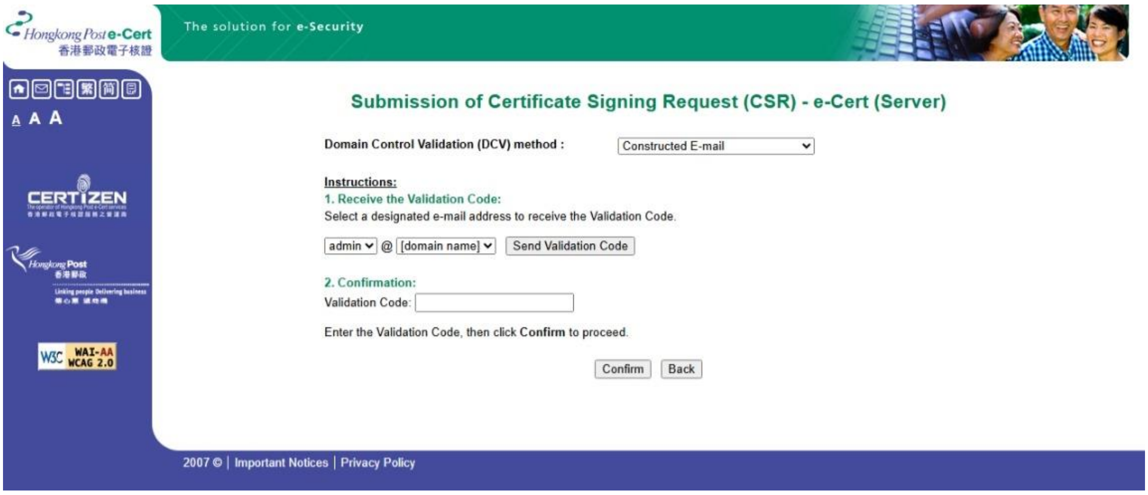
Record Type: TXT
Host: [domain name]
Value: [Validation Code] Copy Validation Code
TTL: 3600

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.

Confirm Back

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.


Hongkong Post e-Cert 香港郵政電子核證
The solution for e-Security
A A A
CERTIZEN
Hongkong Post 香港郵政
W3C WAI-AA WCAG 2.0
2007 © | Important Notices | Privacy Policy

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

Domain Control Validation (DCV) method : Constructed E-mail

Instructions:

1. Receive the Validation Code:
Select a designated e-mail address to receive the Validation Code.

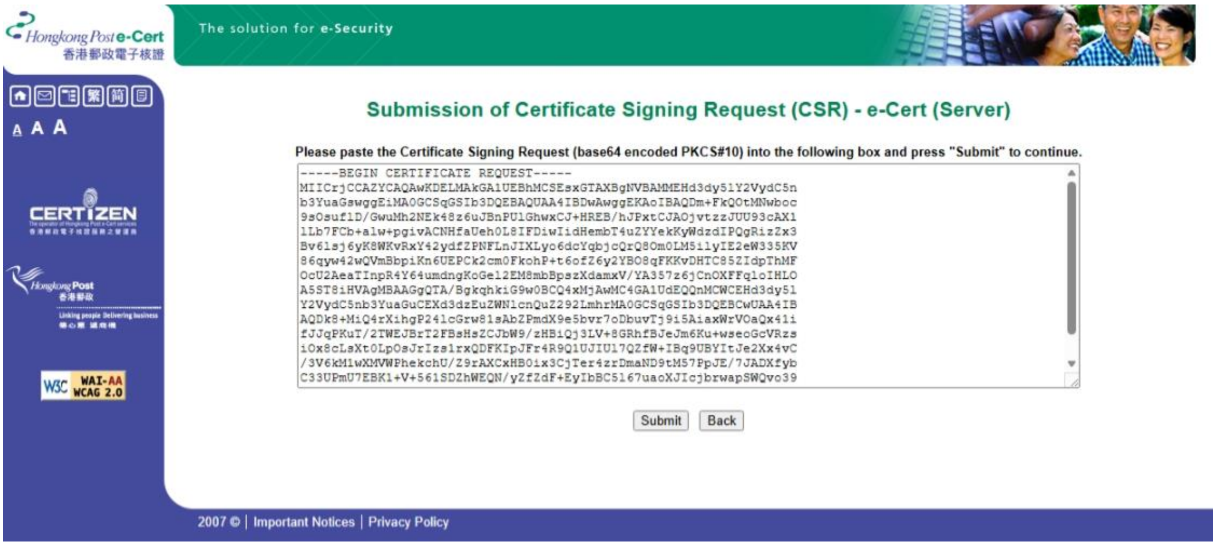
admin @ [domain name] Send Validation Code

2. Confirmation:
Validation Code:

Enter the Validation Code, then click **Confirm** to proceed.

Confirm Back

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".



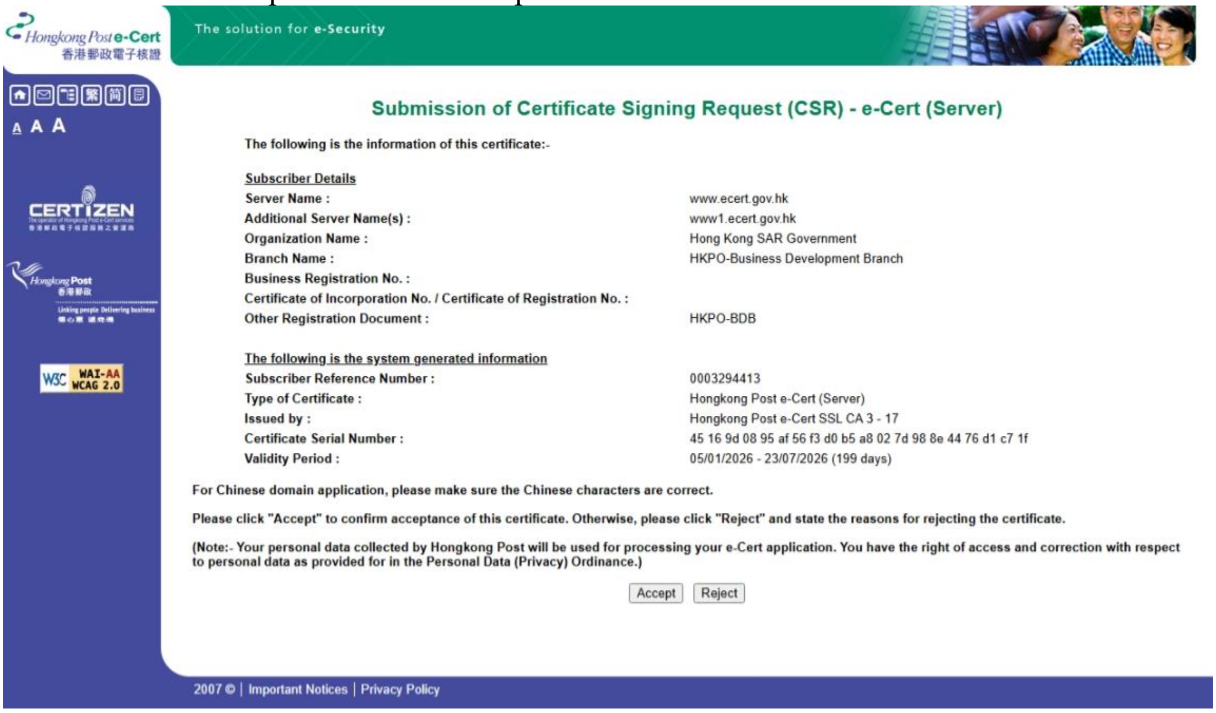
Submission of Certificate Signing Request (CSR) - e-Cert (Server)

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIICrjCCAZYCAQAwKDELMAkGA1UEBhMCSEsxGTAXBgNVBAMMEHd3dy51Y2VydC5n
b3YuaGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDm+FkQOtMNwboc
9sOsuflD/GwuMh2NEk48z6uJBnPUlGhwxCJ+HREB/hJPxtCJAOjvtzzJUU93cAX1
lLb7FCb+alw+pgivACNHfaUeh0L8IFDiwIidHembT4uZYYekKyWdzdIPQgRizZx3
Bv6lsj6yK8WKvRxY42ydfZPNFLnJIXLyo6dcYqbjcQrQ8Om0LM5ilyIE2eW335KV
86qyw42wQVmBbpiKn6UEPCk2cm0FkohP+t6ofZ6y2YBO8qFKKvDHTC85ZIdpThMF
OcU2AeaTInpR4Y64umdngKoGel2EM8mbBpszXdamxV/YA357z6jCnOXFFqloIHLO
A5ST8iHVAgMBAAGgQTA/BgkqhkiG9w0BCQ4xMjAwMC4GA1UdEQQnMCWCEHd3dy51
Y2VydC5nb3YuaGuCEXd3dzEuZWNlcnQuZ292LmhrMA0GCSqGSIb3DQEBCwUAA4IB
AQDk8+MiQ4rXihgP24lcGrw81sAbZPmdX9e5bvr7oDbuvTj9i5AiaxWrVOaQx41i
fJJqPKuT/2TWEJBrT2FBsHsZCJbW9/zHBiQj3LV+8GRhfBJeJm6Ku+wseoGcVRzs
iOx8cLsXt0LpOsJrIzslrxQDFKIpJFr4R9Q1UJIUl7QZfW+IBq9UBYItJe2Xx4vC
/3V6kM1wXMVWPhekchU/Z9rAXCxHB0ix3CjTer4zrDmaND9tM57PpJE/7JADXfyb
C33UPmU7EBK1+V+561SDZhWEQN/yZfZdF+EyIbBC5l67uaoXJIcjbrwapSWQvo39
```

Submit Back

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.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)

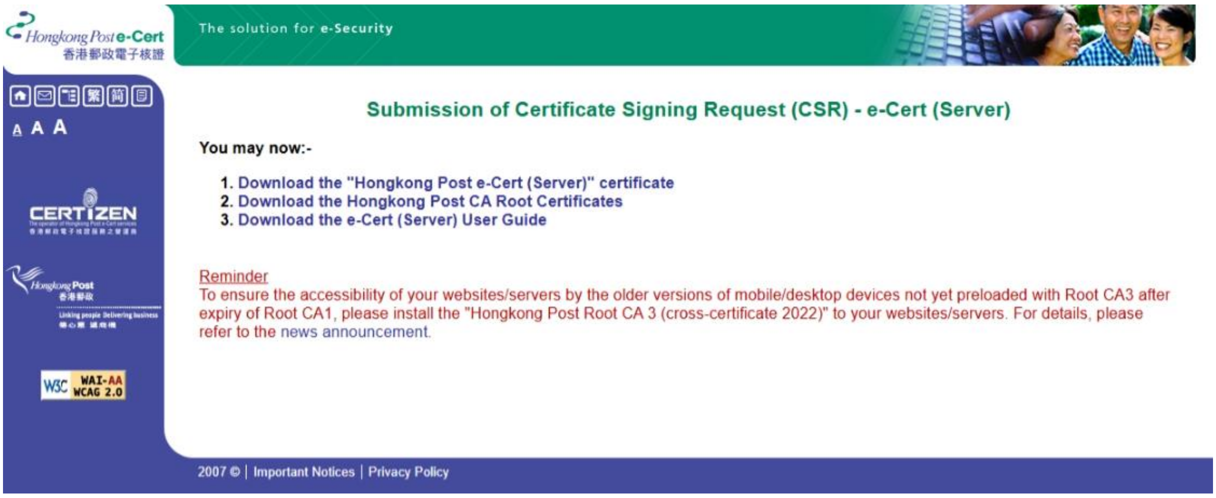
For Chinese domain application, please make sure the Chinese characters are correct.

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.)

Accept Reject

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

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 Server Certificate

1. Copy the private key that you previously generated in Part B Step 1 and the three certificate files that you downloaded in Part C Step 7 to the following Apache server directories. (The directory path may vary depending on your system.)

   For example:

   a) For installation of **e-Cert (Server)** issued by **“Hongkong Post e-Cert SSL CA 3 - 17”**:

   ```
   /usr/local/apache/conf/ssl.key/myserver.key
   /usr/local/apache/conf/ssl.crt/cert0000812104.cer
   /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) For installation of **EV e-Cert (Server)** issued by **“Hongkong Post e-Cert EV SSL CA 3 - 17”**:

   ```
   /usr/local/apache/conf/ssl.key/myserver.key
   /usr/local/apache/conf/ssl.crt/cert0000812104.cer
   /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.crt) containing the Sub CA certificate and cross-certificate.

   For example:

   a) For installation of **e-Cert (Server)** issued by **“Hongkong Post e-Cert SSL CA 3 - 17”**:

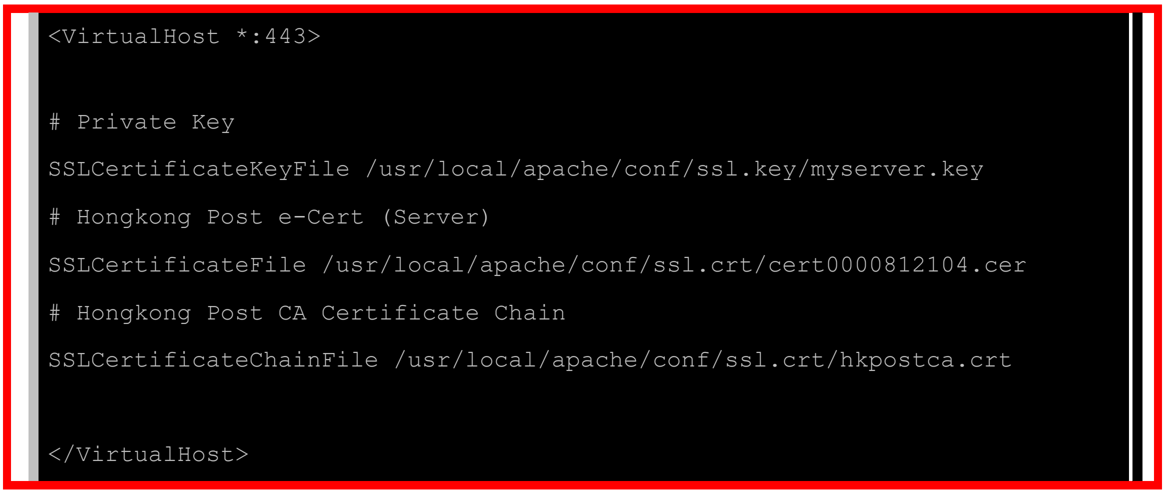
   ```
   cat ecert_ssl_ca_3-17_pem.crt root_ca_3_x_gsca_r3_pem.crt >
   hkpostca.crt
   ```

   b) For installation of **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.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 directives within the virtual host. Please add them if they are not present.



```
<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.crt

</VirtualHost>
```

5. Save the changes and exit the editor.

6. Restart your Apache server using the following commands.

```
apachectl stop
apachectl start
```