e-Cert (Server) User Guide

For Nginx HTTP Server

Revision Date: March 2023

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 applicant (i.e. 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 OpenSSL tools. 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 Triple-DES (3DES). 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 nginx server.

   ```
   openssl genrsa -des3 -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.*

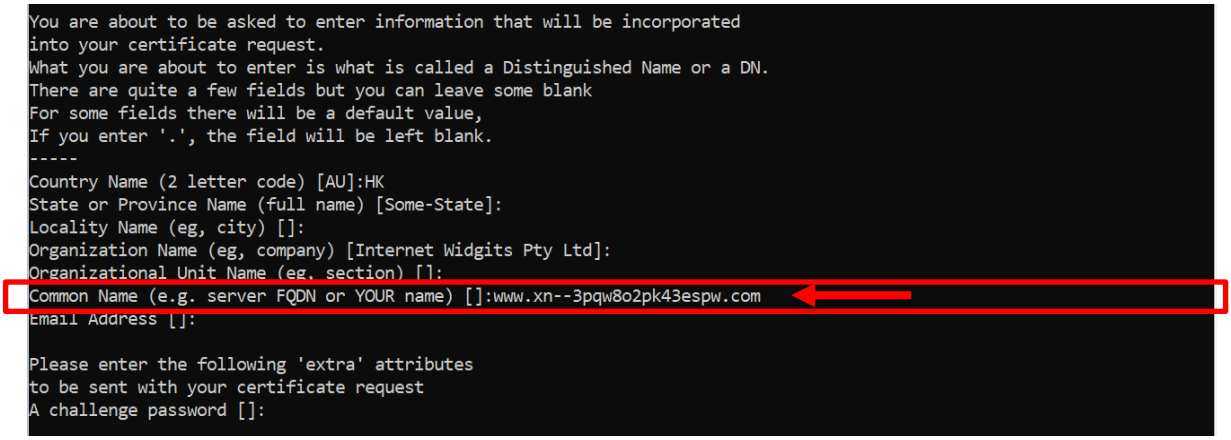
For application of e-Cert (Server) with "Wildcard" feature, *please input the "Common Name" field with "Server Name with Wildcard" (including the wildcard component, i.e. the asterisk '*', in the left-most component of the server name), e.g. *.myserver.com, being filled in the application form.*

```
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 []:
```

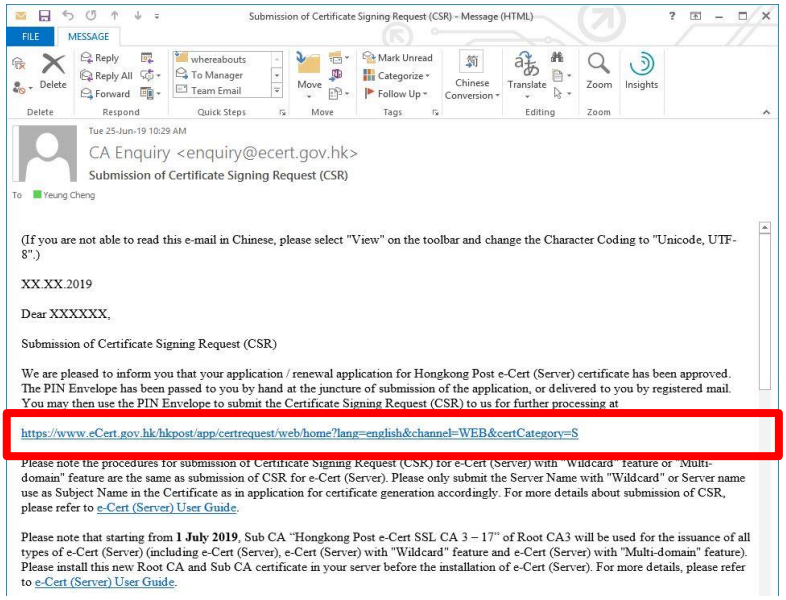
Note: To generate Certificate Signing Request (CSR) with Chinese Domain Name, use IDN conversion tool to convert Chinese Domain Name into ASCII characters and input the converted name in the "Common Name" field.

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



C. Submitting Certificate Signing Request (CSR)

1. Click on the hyperlink in the e-mail with subject "Submission of Certificate Signing Request (CSR)" sent from Hongkong Post Certification Authority to access the Hongkong Post CA web site.



2. Type the "Server Name", the "Reference Number" (9-digit) as shown on the cover of the PIN Envelope and the "e-Cert PIN" (16-digit) as shown inside the PIN Envelope, and then click "Submit".

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

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)

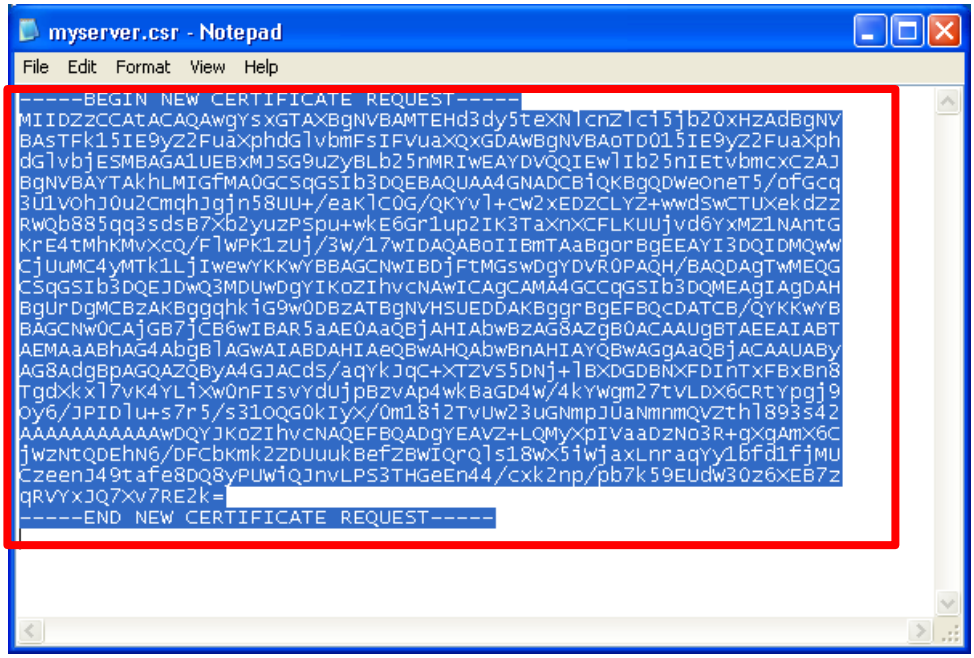
This page is to confirm the application data. If the above information is correct, please click "Confirm" to proceed
You may opt to get the e-Cert (Server) containing the organisation name and branch name in *Chinese by clicking "Confirm Opt with Chinese" button to proceed

Confirm | Reject | Back | Confirm Opt with Chinese

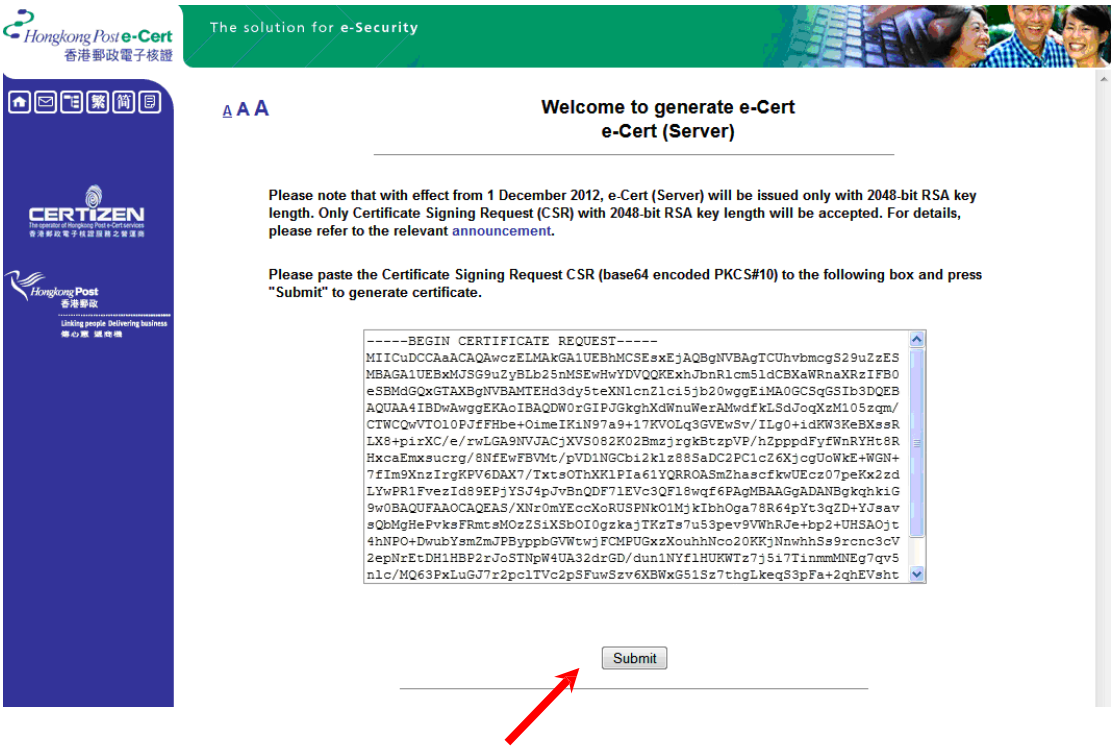
*For Chinese domain application, please make sure the Chinese characters are correct.

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 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-----".



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



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

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

Note:

1. *You can also download your e-Cert (Server) from the Search and Download Certificate web page.*
   https://www.ecert.gov.hk/en/sc/index.html
2. *For all types of e-Cert (Server):*
   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 (Cross certificate 2022)". Click the following link to download:
   http://www1.ecert.gov.hk/root/root_ca_3_x_gsca_r3_pem.crt
3. *For all types of EV e-Cert (Server):*
   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 (Cross certificate 2022)". 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 nginx 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"**:

   /etc/nginx/ssl.key/myserver.key
   /etc/nginx/ssl.crt/cert0000812104.cer
   /etc/nginx/ssl.crt/ecert_ssl_ca_3-17_pem.crt
   /etc/nginx/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"**:

   /etc/nginx/ssl.key/myserver.key
   /etc/nginx/ssl.crt/cert0000812104.cer
   /etc/nginx/ssl.crt/ecert_ev_ssl_ca_3-17_pem.crt
   /etc/nginx/ssl.crt/root_ca_3_x_gsca_r3_pem.crt

2. Change to the nginx directory containing the certificate files (e.g. /etc/nginx/ssl.crt/), and then type the following command at the prompt to create a certificate chain file (myserver_hkpostca.crt) containing the server certificate, 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 cert0000812104.cer ecert_ssl_ca_3-17_pem.crt
   root_ca_3_x_gsca_r3_pem.crt > myserver_hkpostca.crt

   b) For installation of **EV e-Cert(Server)** issued by **"Hongkong Post e-Cert EV SSL CA 3 – 17"**:

   cat cert0000812104.cer ecert_ev_ssl_ca_3-17_pem.crt
   root_ca_3_x_gsca_r3_pem.crt > myserver_hkpostca.crt

3. Open the nginx configuration file (e.g. /etc/nginx/nginx.conf) with a text editor.

4. Locate your HTTPS server configuration section, and then modify the following directives within the section. Please add them if they are not present.

```
# HTTPS server
server {
    listen       443 ssl;
    server_name  myserver.com;

    ssl_certificate      ssl.crt/myserver_hkpostca.crt;
    ssl_certificate_key  ssl.crt/myserver.key;

    ...
}
```

5. Save the changes and exit the editor.

6. Restart your nginx server. For example:

```
systemctl stop nginx

systemctl start nginx
```