



e-Cert (Server) User Guide

For Nginx HTTP Server

Contents

| | | |
|----|---|----|
| A. | Guidelines for e-Cert (Server) Applicant..... | 2 |
| B. | Generating Certificate Signing Request (CSR)..... | 3 |
| C. | Submitting Certificate Signing Request (CSR)..... | 6 |
| D. | Installing Server Certificate | 12 |

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 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 nginx 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.

| BeforeConversion | After Conversion |
|------------------|------------------------------|
| www.我的伺服器.com | www.xn--3pinq8o2pk43espw.com |

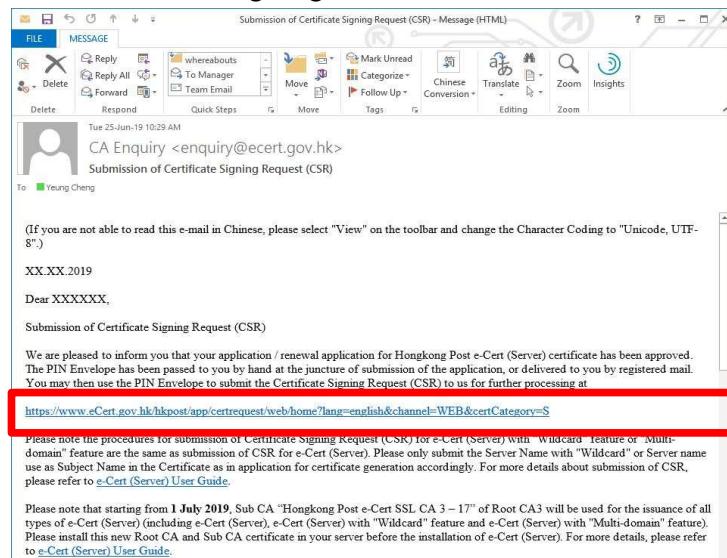
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', 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) []:
 ←
Email Address []:

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

C. Submitting Certificate Signing Request (CSR)

- 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.



- 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.)

The solution for e-Security

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
Branch Name : HKPO-Business Development Branch

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

Confirm | Reject | Back | Confirm Opt with Chinese

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

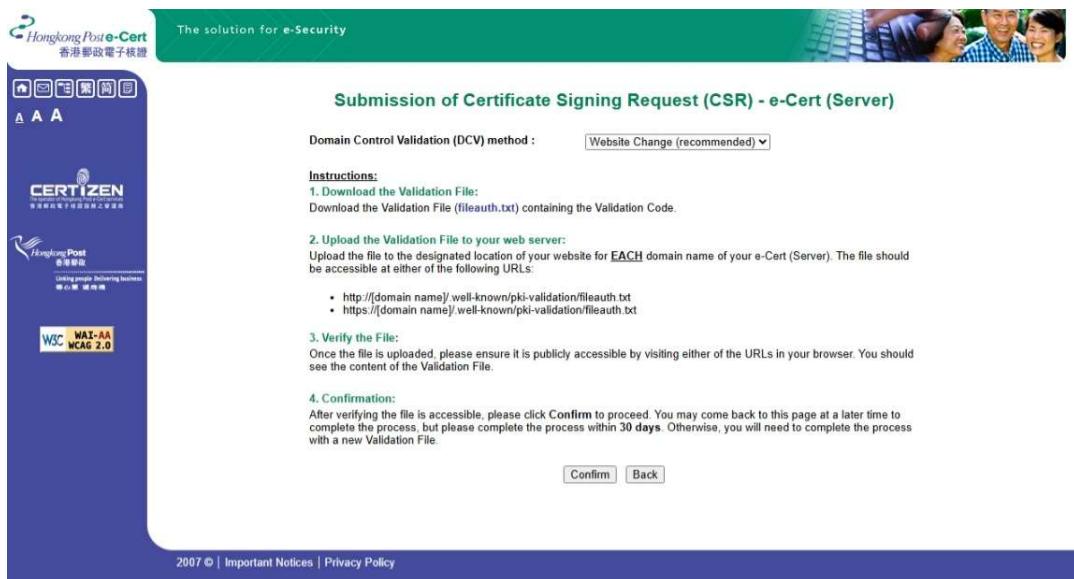
2007 © | [Important Notices](#) | [Privacy Policy](#)

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

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

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

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



B. For “DNS Change” DCV method, add a DNS TXT record that includes the Validation Code for EACH domain name of your e-Cert (Server). Once the record(s) is/are added and publicly resolvable, click “Confirm” to proceed.

The screenshot shows the Hongkong Post e-Cert CSR submission interface. At the top, it says "Submission of Certificate Signing Request (CSR) - e-Cert (Server)". The validation method is set to "DNS Change (recommended)". The instructions state: "1. Add a DNS record: Add a DNS TXT record for EACH domain name of your e-Cert (Server)". The record details are: Type: TXT, Host: [domain name], Value: [Validation Code] (with a "Copy Validation Code" button), and TTL: 3600. The confirmation section says: "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." There are "Confirm" and "Back" buttons at the bottom. The page footer includes links to "Important Notices" and "Privacy Policy".

C. For “Constructed E-mail” DCV method, choose one of the designated e-mail addresses and click “Send Validation Code”. Once you have received the e-mail, enter the Validation Code in the web page and click “Confirm” to proceed. **Please note that this method is NOT applicable to e-Cert (Server) with "Multi-domain" feature.**

The screenshot shows the Hongkong Post e-Cert CSR submission interface. At the top, it says "Submission of Certificate Signing Request (CSR) - e-Cert (Server)". The validation method is set to "Constructed E-mail". The instructions state: "1. Receive the Validation Code: Select a designated e-mail address to receive the Validation Code." The email entry field shows "admin @ [domain name]". The confirmation section says: "2. Confirmation: Validation Code: [] Enter the Validation Code, then click Confirm to proceed." There are "Confirm" and "Back" buttons at the bottom. The page footer includes links to "Important Notices" and "Privacy Policy".

5. Open the Certificate Signing Request (CSR) that you previously generated in Part B Step 2 with a text editor (e.g. Notepad) and copy the entire content including the lines "-----BEGIN NEW CERTIFICATE REQUEST-----" and "-----END NEW CERTIFICATE REQUEST-----". Paste the content to the text box, and then click "Submit".

The solution for e-Security

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-----
MIICrjCCAZYCAQAwKDElMAkGA1UEBhMCSEwGTAKBgNVBAMMEHd3dy5LY2VydC5n
b3YuaGwggE1MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDm-FkQ0tM0Wboc
9s0su1D/GwubM2NEk4z26uJbAPU1GhwxCJ+HREB/hJFxtCJAjvtzJUU93cAx1
1Lb7FCb+alw+pgiavACNif4uEhOL81FDiwiLidHemb74u2YVekKyWzdIP0gRiz2x3
Bv61s6yK5NWhvRx42yuf2NFlnJXLyc6dcVpbjCQ80mLM51iyIE2eW335KV
86qwy42uQmBpbiKnUEPCK2cm0FkchP+t6zfZ6y3YB08qFKvDHTC85Z1zpThMF
OcU2Aea7InpR4Y64urndngKoGe12EM8mbpazXdemvV/YA357z61cnXFg1oIHLO
A5ST8iHVAgMBAgGQTA/BgkqhkiG9w0BCQ4xMjAwMC4GA1UdEQQnMCWCEHd3dy51
Y2VydC5nb3YuuaGuCExD3d2eU2WH1nqzu2921lhrHA0GCSqS1b3DQEBCwUAA1B
AQDk8+MjQ4x1hgP24lGGrw81sAb2Pmd9eSbvr7ODuvTj9i5AlaxWrVcaQx4i1
fJjgPKu/2TWEUBf2FBsH2CJbW9/zHb1Q13LW+8Rhf5JeJm6Ku+wseGoGVzs
:0x8cLaxt0Lp0sJr1szlxrQDFKlpFr4R901UJ1U17QZFW+IBq9uBYItJex2Xx4vC
:3VeKd1wXNWhPhekhU/Z9rAXCmH0lxsCjTer4zrDmaND9M57PpJE/7JAIXXyb
C33UfMUTEBK1+v+561SD2hWEQm/yf2df+EylBCs167uacXJ1cjbrwapSqv039
```

Submit Back

2007 © | Important Notices | Privacy Policy

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

The solution for e-Security

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

The following is the information of this certificate:-

Subscriber Details

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

The following is the system generated information

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

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

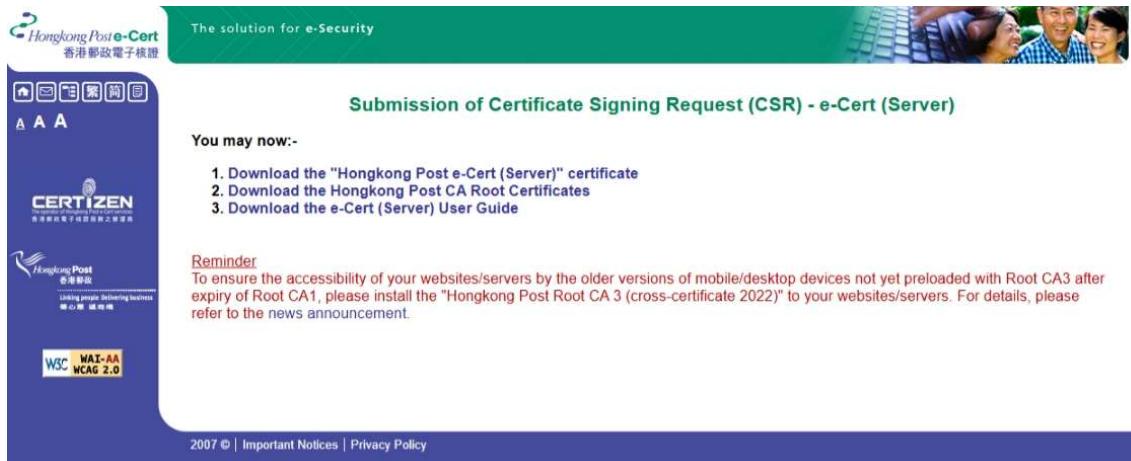
Please click "Accept" to confirm acceptance of this certificate. Otherwise, please click "Reject" and state the reasons for rejecting the certificate.

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

Accept Reject

2007 © | Important Notices | Privacy Policy

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. 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 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
```